

Parallels[®] Panel

Administrator's Guide

Parallels Plesk Panel 11.5

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>.

Microsoft, Windows, Windows Server, Windows NT, Windows Vista, and MS-DOS are registered trademarks of Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

Mac is a registered trademark of Apple, Inc.

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

Contents

After Upgrading to Panel 11.5	10
Upgrade from Earlier Panel Versions.....	11
Upgrade from Small Business Panel.....	14
Differences between SBP and Panel 11.....	14
About Parallels Plesk Panel	18
About Panel Users.....	19
The Panel GUI.....	20
Interface Views.....	24
Customizing Power User View.....	25
Web Servers	27
Apache Web Server (Linux).....	28
Apache with nginx.....	30
Adjusting Apache Settings for Virtual Hosts.....	34
Adjusting nginx Settings for Virtual Hosts.....	35
Optimizing Apache Web Server.....	38
IIS Web Server (Windows).....	41
Adjusting IIS Settings for Websites.....	42
IIS Application Pool.....	42
Web Hosting	44
Website Directory Structure.....	44
Defining a Custom Virtual Host Template.....	45
Virtual Host Structure (Linux).....	45
Virtual Host Structure (Windows).....	47
Website Preview.....	50
PHP Configuration.....	50
PHP Handlers.....	52
Custom PHP Configuration.....	54
Multiple PHP Versions.....	58
Configuring ASP.NET (Windows).....	60
DNS	63
Server-Wide DNS Template.....	64
Adjusting DNS Template.....	65
Applying DNS Template Changes (Linux).....	68
DNS Zones for Subdomains.....	69
Configuring the Recursive DNS.....	70
Restricting DNS Zones Transfer.....	71
Restricting Users' Access to Other Users' DNS Zones.....	71
Using BIND Instead of Microsoft DNS (Windows).....	72
Switching Off the DNS Service.....	72
Using External DNS Servers.....	72
Panel Without a DNS Server.....	74

Mail 75

Configuring Server-Wide Mail Settings	77
Using Panel Without the Mail Server.....	79
Removing Mail Functionality from the Control Panel	81
Using Other Mail Server Software	82
Antispam Tools.....	83
SpamAssassin Spam Filter	85
DomainKeys Protection.....	88
DNS Blackhole Lists.....	90
Server-wide Black and White Lists.....	90
Sender Policy Framework System (Linux).....	92
Greylisting (Linux)	93
Outbound Spam Protection	94
Installing Parallels Premium Outbound Antispam	95
Configuring Protection.....	96
Antivirus Software.....	100
Webmail Software	102
Mailing Lists (Linux).....	103
Preventing Mass Email Sending (Linux)	104
Mail Queue (Linux)	104
Mass Email Notifications	105
Creating, Editing and Removing Message Templates.....	106
Sending E-mail Notices.....	108
Configuring Email Notifications	109

Database Servers 112

Adding and Removing Database Servers	114
Configuring Backup Settings for Remote SQL Servers	116
Changing Database Administrator's Credentials.....	117
Database Hosting Preferences	118
Database Management Tools	119
Connecting to External Databases (Windows).....	120

Server Administration 121

IP Pool	122
Scheduling Tasks	126
Scheduling Tasks on Linux-based Servers.....	127
Scheduling Tasks on Windows-based Servers.....	129
Server Settings	131
System Services	132
System Date and Time	134
Firewall	135
The Panel Firewall (Linux)	135
The Panel Firewall (Windows)	136

Panel Administration 138

Panel Licensing	139
Installing a Panel License Key	140
Installing Additional License Keys for Panel Add-ons.....	141
Upgrading Your License Key	142
Rolling Back to Your Previously Used License Key.....	142
Securing Panel	142
Restricting Administrative Access.....	143

Restricting Remote Access via API RPC	144
Setting Up the Minimum Password Strength	144
Turning On the Enhanced Security Mode	145
Using Secure FTP	146
SSL Protection	146
Panel and Network Environments	151
Ports Used by Panel	152
Running Panel Behind a Router with NAT	153
Configuring Port Range for Passive FTP Mode (Windows)	154
Setting Up Help Desk	155
Trial (Try and Buy) Mode for Presence Builder	157
Configuring the Try and Buy for Existing Customers	160
Configuring the Try and Buy for Potential Customers	161
Customizing Trial Mode Notifications	162
Offering the Try and Buy with Alternative Billing Solutions	165
Changing Your Password and Contact Information	168
If Your Panel Works with Parallels Customer and Business Manager	169
Appearance and Branding	170
Appearance	170
Branding and Themes	176
Panel Components	176
Web Applications	177
How Apps Become Available to Your Customers	181
Application Vault	183
Session Preferences	187
Managing Panel from Mobile Devices	188
Panel Inside Parallels Virtuozzo Containers	192
Remote Access (Windows)	194
Additional Administrator Accounts	195
Creating Additional Administrator Accounts	196
Modifying Additional Administrator Accounts	196
Suspending and Activating Additional Administrator Accounts	197
Removing Additional Administrator Accounts	197
Event Tracking	198
Adding Event Handlers (Linux)	199
Adding Event Handlers (Windows)	200
Removing Event Handlers	201
Migration from Other Hosting Platforms	202
Data Transfer from Another Panel	202
Panel Extensions (Linux)	203
Counter-Strike Game Server Extension	204
File Server Extension	215
Firewall Extension	223
Watchdog (System Monitoring) Extension	230
VPN Extension	242

Panel Updates and Upgrades **248**

Panel Updates	249
Panel Upgrades	251
Changing the Updates/Upgrades Source	253
Reporting Upgrade Problems	254

Statistics and Monitoring **255**

Action Logs	256
Setting Up Action Logging	257
Downloading the Action Log	257
Clearing the Action Log	258

Viewing Statistics.....	259
Automating Report Generation and Delivery by E-mail	260
Viewing Virus and Spam Protection Statistics (Windows)	261
About Disk Space Usage Calculation	262
Server Health Monitor	266
Installing Health Monitor.....	266
Tracking Server Health	266
Accuracy of Health Monitor Values	268
Configuring Alarms, Trends, and E-mail Notifications	268
Updating Health Parameters After Hardware Change.....	268
Monitoring Connections to Panel	269
Monitoring User Sessions	269
Monitoring FTP Users Sessions.....	270
Monitoring Terminal Connections (Windows)	271

Backup and Restoration **272**

Configuring Global Backup Settings.....	274
Configuring Panel for Using FTP Repository	275
Backing Up the Entire Server	276
Backing Up Individual Accounts and Sites	276
Scheduling Backups	277
Restoring Data from Backup Archives	279
Downloading Backup Files from Server	281
Uploading Backup Files to Server	281
Removing Backup Files from Server.....	282
Backup Logs.....	282

Shared Files and Folders **283**

File Sharing Settings	284
Sharing and Protecting Files	285
Sharing Files with Other Users Within the Organization.....	286
Publishing Files for Partners	287
Publishing Files for Your Customers.....	289
Uploading Your Files to a Private Directory on the Server	290
Transferring Large Files that Cannot Be Sent by E-mail	291
Accessing and Working with Files.....	292

Customers and Resellers **303**

Hosting Plans and Subscriptions.....	305
Relationship Between Plans and Subscriptions.....	306
Setting Up Hosting Plans	308
Setting Up Add-on Plans	311
Subscribing Customers to Plans	312
Managing Customers	314
Managing Subscriptions	317
Serving Non-Technical Customers	321
Reseller Plans	322
Setting Up Reseller Plans	323
Subscribing Resellers to Plans	323

Website Management **324**

Quick Start with Parallels Panel	326
Set Up Your First Website.....	327
Set Up Mail Accounts	331

View Site Visit Statistics	350
Customer Account Administration	350
Changing Your Password and Contact Information	354
Viewing Subscription Summary	355
Managing Account Balance and Invoices	362
Ordering More Resources	366
Viewing Statistics	368
(Advanced) Managing Auxiliary User Accounts	370
Websites and Domains	377
Domains and DNS	378
Hosting Settings	395
Website Content	413
(Advanced) Restricting Access to Content	418
Previewing Websites	420
Web Applications	421
(Advanced) Website Security	429
(Advanced) Extended Website Management	435
Creating Sites with Presence Builder	467
Getting Familiar With Presence Builder	470
Creating a Website	472
Importing Sites from SiteBuilder 4.5	473
Editing Websites	474
Saving and Loading Copies of a Website	513
Publishing a Website to the Internet	515
Publishing a Website Copy to Facebook	516
Viewing Site Visits Statistics, Comments, and New Orders on the Dashboard	518
Deleting Websites	520
FTP Access to Your Websites	521
Changing FTP Access Credentials	521
Adding FTP Accounts	522
Setting Up Anonymous FTP Access	524
Mail Accounts	526
Adding Mail Accounts	527
Configuring Mail Account	528
(Advanced) Configuring Global Mail Settings	535
Using Mailing Lists	536
Scheduling Tasks	537
Scheduling Tasks (Linux)	538
Scheduling Tasks (Windows)	540
Website Databases	542
Creating Databases	543
Accessing Databases	543
Copying Databases	544
Exporting and Importing Databases	544
Managing Database User Accounts	545
Accessing Databases with ODBC (Windows)	546
Backing Up and Recovering Websites	547
Backing Up Data	548
Managing Backup Files	554
Restoring Data	556

Appendix A: Properties of Hosting Plans and Subscriptions **558**

Visibility of Hosting Features in the Control Panel	560
Resources	561
Permissions	564
Hosting Parameters	568
PHP Settings	571
Web Server (Apache)	571
Mail	572

DNS	573
Performance	573
Logs & Statistics	574
Applications	574
Additional Services	574

Appendix B: Properties of Reseller Plans and Subscriptions 575

Resources	576
Permissions	577
IP Addresses	577
Applications	578

Appendix C: Event Parameters Passed by Event Handlers 579

Administrator information updated	581
Service stopped	581
Service started	581
Service restarted	581
IP address created	581
IP address updated	581
IP address deleted	581
Session settings updated	582
Customer account created	582
Customer account updated	582
Customer account deleted	582
Customer account status updated	583
Customer's interface preferences updated	583
Customer GUID updated	583
Reseller account created	583
Reseller account updated	584
Reseller account deleted	584
Reseller account status updated	584
Reseller's interface preferences updated	584
Reseller's IP pool updated	584
Disk space limit for reseller account reached	584
Traffic limit for reseller account reached	584
Disk space limit for subscription reached	585
Traffic limit for subscription reached	585
Default domain (the first domain added to a subscription/webpace) created	585
Default domain (the first domain added to a subscription/webpace) updated	586
Default domain (the first domain added to a subscription/webpace) deleted	586
Subscription owner changed	586
Default domain, status updated	586
Default domain, DNS zone updated	586
Default domain, GUID updated	586
Subdomain of a default domain created	586
Subdomain of a default domain updated	587
Subdomain of a default domain deleted	587
Default domain, alias created	587
Default domain, alias updated	588
Default domain, alias deleted	588
Default domain, alias DNS zone updated	589
Reseller account limits updated	589
Subscription limits updated	589
Panel user logged in	589
Panel user logged out	589
Panel user failed to log in	589

Panel user failed to log in through API	589
<hr/>	
Mail account created	590
Mail account updated	590
Mail account deleted.....	590
Mailing list created	590
Mailing list deleted	591
Hosting settings created	591
Standard or frame forwarding hosting created	592
Hosting settings updated	593
Hosting settings deleted	593
Standard or frame forwarding hosting updated	593
Standard or frame forwarding hosting deleted	593
Web user account created	593
Web user account updated	594
Web user account deleted.....	594
Web application installed.....	594
Web application reconfigured	595
Web application uninstalled.....	595
Web application upgraded.....	595
License key updated	595
License key expired.....	595
Database server created	596
Database server updated	596
Database server deleted	596
Database created	596
Database deleted	596
Database user account created	597
Database user account updated	597
Database user account deleted.....	597
Parallels Plesk Panel component updated or added	598
Reseller plan created	598
Reseller plan updated	598
Reseller plan deleted.....	598
Service plan of reseller created	598
Service plan of reseller updated	598
Service plan of reseller deleted	599
Service plan of administrator created.....	599
Service plan of administrator updated.....	599
Service plan of administrator deleted	599
 Additional FTP account created	 600
<hr/>	
Additional FTP account updated	600
<hr/>	
Additional FTP account deleted	600
<hr/>	
Server health status changed.....	601
Update available.....	601
Update installed.....	601

After Upgrading to Panel 11.5

This chapter is intended to the users who switched to Panel 11.5 either from Plesk Panel 9 and earlier or from Parallels Small Business Panel. The chapter describes the main changes in the business model of Panel 11.5 comparing to these products.

In this chapter:

Upgrade from Earlier Panel Versions	11
Upgrade from Small Business Panel	14

Upgrade from Earlier Panel Versions

Compared to the previous versions of Plesk software (Plesk 9 and earlier), Parallels Plesk Panel 10 introduces the following changes:

- **User accounts.** In Panel 11, there are no client accounts and domain administrator accounts. For users who need to resell hosting services and host their own websites, you will set up *reseller accounts*. For users who do not need to resell hosting services, but only host their own websites, you will set up *customer accounts*.
Customers can create user accounts in the Panel if they want to allow other users to access the Panel for managing websites, installed applications, or use e-mail services. In 11, customers can create any number of users for access to their Panel, and set up multiple additional FTP accounts for access to the webspace.
- **Service plans.** In Panel 11, there are no reseller, client, or domain templates. Instead, there are *service plans* that you create according to your service offerings: *Reseller plans* for signing up resellers, and *hosting plans*, for signing up customers who do not need to resell services. After plans are created, you create reseller or customer accounts and subscribe them to the plans - and the users are provisioned with the necessary resources and authorized to perform operations in the Panel.
The most important change brought in by service plans is that, unlike old Plesk templates, they are not applied only once, during the initial resources provisioning, but remain connected to them, so that modifications of a plan change the provisioned resources and privileges.
In addition to hosting plans, there are also *add-on plans*. You can use them to allocate more resources and services to customers.
- **Subscriptions.** Multi-domain hosting subscriptions replace domains. Instead of creating domains for your customers, you *subscribe* them to a hosting plan, or, in other words, you create a *subscription* for the customer. Actually, not only customers can be subscribed to hosting services and host their websites and mail, the Panel administrator and resellers can have their own subscriptions as well, which they may use for their own purposes.
Subscriptions can be created based on service plans or configured manually.
When subscribing a new customer to your services in Panel 11, you specify a domain name at the first step. A customer's subscription is always linked to a domain, which is identified by such attributes as domain name, IP address and system user account. All subscriptions are named after the domains to which they are linked. This link is permanent and cannot be broken in any way, so moving a domain from one subscription to another is impossible. However, you can still rename domains.
You can host a number of websites under a single subscription, and you can create several subscriptions for a single customer account.
- **Allocation of resources.** In previous versions of Plesk, resources were allocated to reseller accounts, client accounts, and domains. In Panel 11, resources are allocated to resellers and hosting service subscriptions. Customer accounts in Panel 11 do not get any resource allocations directly, so they cannot redistribute them among subscriptions that they purchase. All resources allocated to a single subscription are shared among all websites hosted in the webspace associated with the subscription.

- **Two separate panels: Server Administration Panel and Control Panel.** System administration, and customer and reseller account management tasks are performed in *Server Administration Panel*. All operations related to managing websites, hosting features, and mail accounts are performed in *Control Panel*. Server Administration Panel provides links for access to Control Panel: You can use them to log in to Control Panel and manage websites on behalf of your resellers and customers.
- **Changes in organization of subdomain-related directories.** Due to safety reasons, Panel now stores content and configuration of hosted subdomains in separate directories:
 - `/<VHOST>/<subdomain_name>`, the directory that contains HTTP/HTTPS documents (unlike the earlier versions that separated HTTP and HTTPS documents).
 - `/<VHOST>/<subdomains>/<subdomain_name>`, the service directory that keeps subdomain configuration. *We strongly recommend that you do not change the content of this directory.*

What Happens When You Upgrade or Migrate to Panel 11

When you upgrade or migrate to Panel 11, accounts, domains, users, and domain templates are transformed according to the following schemes:

- Reseller accounts are transferred without changes, and resources are allocated to them by means of custom subscription, which are not bound to plans.
- Client accounts become customer accounts, and after upgrade or migration is finished, you need to perform either of the following operations to make sure that the accounts fit in the new business model:
 - Redistribute former clients' resources among the subscriptions belonging to them.
 - Convert customers to resellers and assign the existing subscriptions to them. This can be done if the customer accounts did not belong to a reseller before upgrade or migration.
- Domains are converted to individual subscriptions. The subscriptions are assigned to the administrator, resellers, or customers, depending on whom the former domains belonged to.
- Domain administrator accounts are converted to user accounts, which are assigned to the customers who own the corresponding domains.
- Domain templates belonging to the server administrator and resellers are converted to hosting plans.
- Reseller templates are converted to reseller plans.

The following table summarizes the conversion of business objects.

Objects in previous versions of Plesk	Objects in Panel 11
Reseller account	Reseller account

Client account	Customer account
Domain	Subscription (Custom)
Domain administrator account	User account
Reseller template	Reseller plan
Domain template	Hosting plan

Upgrade from Small Business Panel

This chapter is intended for users who have migrated from Parallels Small Business Panel (SBP) to Parallels Plesk Panel and want to know about changes in management operations, as well as about new product possibilities. If you want to learn more about the migration procedure, refer to **Installation, Upgrade, and Migration Guide**, section **Migrating from Parallels Small Business Panel**.

Migration to Panel is almost seamless as Panel allows you to perform the majority of tasks you did in SBP. The main difference you may find is that some functions are now available in new locations or have a slightly different effect. Moreover, Panel provides you with a number of features unavailable in SBP, such as enhanced user role permissions, the Presence Builder tool, or access to new web apps. Learn more about product differences in the section **Differences between SBP and Panel 11** (on page 14).

After the migration, you will use Panel in Power User view - a replacement of the SBP interface. Power User view is almost identical to the SBP user interface. Panel in this view is, in essence, Control Panel with server management capabilities. For more information on Power User view, refer to the section **The Panel GUI** (on page 20).

Next in this section:

Differences between SBP and Panel 11 14

Differences between SBP and Panel 11

User interfaces of SBP and Panel in Power User view are almost identical. Therefore, here we will discuss only the most important changes to the way you work with Panel.

Next in this section:

Extended User Role Permissions 15
 Presence Builder Tool 16
 SSL Protection 16
 Web Apps..... 17
 Extended Mail Management 17
 Other Panel Features 17

Extended User Role Permissions

Panel, comparing to SBP, allows more accurate adjustment of user role privileges due to a larger number of available permissions. For example, Panel allows dividing users on those who can manage mail accounts and those who can manage company mailing lists. As Panel has the extended list of permissions, some of SBP permissions can migrate into a number of related Panel permissions. For better understanding how permissions are migrated, refer to the table below.

SBP permission	Panel permission	Migration result comments
Manage users Manage roles	Manage users and roles	The permission is granted, if one of the SBP permissions is granted.
Manage websites and domains	Create and manage sites Configure log rotation Configure anonymous FTP service Create and manage scheduled tasks Create and manage databases Configure and perform data backup and restoration View statistics Design sites in Presence Builder Create and manage additional FTP accounts Manage DNS settings Install and manage Java applications	
Change server settings	-	The permission is not migrated, as Panel allows changing server settings to users with the Administrator role only.
Manage mail	Create and manage mail accounts Create and manage mailing lists	
Update personal information	-	The permission is not migrated, as Panel allows changing personal information to all users.
-	Upload and manage files	By default, this permission is denied after migration.
-	Configure spam filter	By default, this permission is denied after migration.
-	Configure antivirus	By default, this permission is denied after migration.

For more information on user role properties, refer to the section **User Roles** (on page 371).

Presence Builder Tool

While using SBP, you could easily create your own websites with the Site Editor tool. For the same purposes, Panel provides you with the much more powerful tool, Presence Builder. Comparing to Site Editor, Presence Builder offers:

- New intuitive interface that allows creating websites in less number of steps.
- About 100 website templates filled with content that you can use as a basis for your sites.
- Additional components that can be easily integrated with your site, such as the online store or the embedded video.
- Integration of your website with Facebook and much more.

For more information on Presence Builder, refer to the section **Building Websites with Presence Builder** (on page 467).

Note that websites created in Site Editor are not compatible with Presence Builder. Nevertheless, if Site Editor is installed in Panel, you can edit such websites with it. In that case, websites in **Websites & Domains** list will contain the additional button **Edit in SiteBuilder 4 or Site Editor**.

SSL Protection

Panel allows you to secure connections to your websites the same way as you did in SBP. That means you can obtain SSL certificates in **Server > Tools & Settings > SSL Certificates** and assign them to IP addresses in **Server > Tools & Settings > IP Addresses**. As in SBP, you can assign only one certificate per IP address. Thus, if your hosting resources include one shared IP address, you can secure only one website. Panel provides enhanced SSL protection features that allow you to resolve this problem:

- *Separate SSL certificates for websites.*
If you use Panel on a Linux operating system with the SNI technology support, it is possible to use authentic SSL certificates for sites hosted on shared IP addresses. In other words, Panel allows using separate SSL certificate for each website. Learn more about separate SSL certificates in the section **SSL and Shared IP Addresses (Linux)** (on page 150).
- *Shared SSL certificate for a number of websites.*
If you use Panel on a Windows operating system, it is possible to use one shared SSL certificate to secure connections to all sites. In that case, certificate is assigned to a domain that shares it with others. That domain is called master SSL domain. In other words, all websites will use common SSL certificate, despite of the fact it is issued to only one of your websites. Learn more about shared SSL certificates in the section **SSL and Shared IP Addresses (Windows)** (on page 150).

The process of assigning an SSL certificate to a website is covered in the section **Securing Connections with SSL Certificates** (on page 430).

Web Apps

Comparing to SBP, the app management in Panel has little or no changes. As in SBP, the list of available web apps is accessed through the **Applications** tab. For more information on app management, refer to the section **Using Website Applications** (on page 421).

Note that the uploading of your own app packages is now performed by means of Application Vault. Vault is the local Panel repository of web apps. Besides of extending the list of available apps, it allows you to update apps, configure their server-wide settings, and carry out some other operations. For more information on Application Vault, refer to the section **Web Applications** (on page 177).

Extended Mail Management

Mail management in Panel slightly varies from those in SBP. General mail settings are now available in **Mail > Change Settings**, while other settings are located in **Server > Settings > Mail**.

Comparing to SBP mail functionality, Panel provides a number of additional mail features:

- *Enhanced spam protection:*
 - Server black and white lists.
Use these lists to always reject or always receive mail from selected servers. Learn more on black and white mail lists in the section **Server-wide Black and White Lists** (on page 90).
 - Extended SpamAssassin settings.
Panel allows you to configure SpamAssassin more accurately. For example, you have access to such settings as spam filter sensitivity or SpamAssassin's black and white lists. Moreover, you can configure spam filter individually for each mail account. Learn more in the **Protecting from Spam** (on page 530) section.
- *Monitoring mail server message queue (on Linux platforms).*
This can be helpful when your mail server is overloaded and cannot cope with the amount of received messages. You can find out the reason that caused the overload using the mail queue. Learn more about message queue in the section **Mail Congestion and Message Queue (Linux)** (on page 104).

Other Panel Features

On top of main changes described above, Panel contains a number of features unavailable in SBP at all. These are event management, server health monitoring, custom branding themes and many more. The scope of this chapter does not allow to cover all of them. For the detailed information on other server management operations, refer to certain sections of this guide.

About Parallels Plesk Panel

Parallels Plesk Panel is designed to help IT specialists manage web, DNS, mail and other services through a comprehensive and user-friendly GUI. It is a hosting control panel, an intermediary between system services and users. For example, when a user creates a website through the Panel GUI, Panel propagates this request to a web server, either Apache or IIS, and the latter adds a new virtual host to the system. This method of administering all system services from a single web interface reduces maintenance costs and gives administrators more flexibility and control.

How Can I Use Panel?

Panel is an essential instrument for hosting service providers (HSPs) - companies that sell shared and dedicated hosting accounts. Being installed on a server, Panel enables HSPs to organize server resources into packages and offer these packages to their customers. The customers are companies and individuals who need web presence but do not have the necessary IT infrastructure. Learn more about the Panel intended audience in the section **About Panel Users** (on page 19).

Can I Customize Panel to Address My Needs?

Each Panel user group is provided with their own GUI that is customized to fully meet their needs. Thus, HSPs get tools for offering hosting services, including an integrated billing solution that automates their business. By contrast, companies that use Panel to manage their own web infrastructure do not have hosting selling capabilities in their GUI. Instead, they can perform server management operations (such as system recovery, web server configuration, and so on). Learn more about the Panel interface in the section **The Panel GUI** (on page 20).

Next in this chapter we explain how different user groups should use Panel to gain all its benefits.

In this chapter:

About Panel Users	19
The Panel GUI	20

About Panel Users

Panel is a web hosting panel that targets four user groups:

- *Power users.*
These are companies that buy VPS hosting with preinstalled Panel or deploy it by themselves on their IT infrastructure. Panel allows such customers not only to manage various aspects of their web presence but also to have full control over server management operations, such as server backup, configuration of PHP settings, and so on. For example, web design studios use Panel as a platform for web development. Panel allows them to test created websites and present the results to clients.
- *Hosting service providers (HSPs).*
HSPs use Panel for two main purposes. First, as an easy tool for services configuration. Thus, providers do not need to separately configure web or FTP server - everything is done in the Panel GUI. Once services are configured, HSPs can combine them with server resources (like disk space or traffic) into hosting packages (service plans). For example, one package can contain a website, mail accounts, and a number of web applications. These packages are then sold to HSPs' clients - hosting customers and resellers.
- *Resellers.*
These are companies that resell hosting services provided by HSPs. They use Panel to buy hosting resources in bulk, and then split the resources into smaller packages, and sell them to their customers. All server management is performed by HSPs, allowing resellers to reduce their costs and concentrate on offering services to end-users.
- *Customers.*
These are the end-users of Panel. By subscribing to one of the hosting plans offered by an HSP or a reseller, they get access to Panel and manage the services they have bought. They can create sites, fill them with content, add mail accounts, and so on.

The Panel GUI

For convenience, Panel tools for performing server and account management tasks are divided between two web interfaces called *panels*: *Server Administration Panel* and *Control Panel*. In earlier Panel versions, each panel had its own unique responsibilities:

- *The Control Panel* focused on web hosting operations and had all means to create and manage websites, mailboxes, and so on.
- *The Server Administration Panel* was in charge of server maintenance and accounts management.

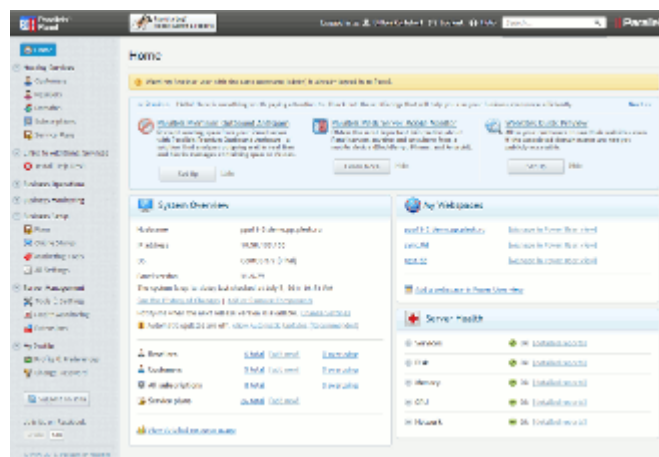
If administrators needed to perform a web hosting management task, for example, add a mailbox under a certain customer's account, they located the account in the Server Administration Panel and then opened the account in the Control Panel. As Panel evolved over time, the border between the panels has become subtle. Now, the only significant difference between the two panels is that *tools for serving customers and resellers are available only in the Server Administration Panel*. As for the other functions, the panels are quite similar: Both of them allow you to maintain a server and manage web hosting. If you do not use Panel for selling hosting services, you can choose any of these two panels.

The brief description of each panel is provided below, but before we go into details, we would like to acquaint you with Panel views because views and panels are tightly connected.

Panel Views

Each Panel user group has its own Panel usage scenarios. The GUI can be configured to better meet the needs of a certain group by rearranging tools between different web interfaces and hiding odd tools. For example, power users may prefer to use only the Control Panel with tools for server management, whereas hosting service providers use both panels with all available tools; shared hosting customers use the Control Panel without server management facilities. Such a user-targeted combination of available panels and tools is called *view*. Learn more about the views in the section **Interface Views** (on page 24).

Server Administration Panel



The Server Administration Panel is the main instrument of hosting providers that allows them to serve their customers and maintain a server. Here, for example, the administrator creates new hosting plans and customer accounts, configures server-wide settings of system services, and so on. In addition, the administrator can set up Panel to manage web hosting right from the Server Administration Panel (create websites and mail accounts for their customers, install web apps, and so on). Learn more in the section **Interface Views** (on page 24).

Control Panel



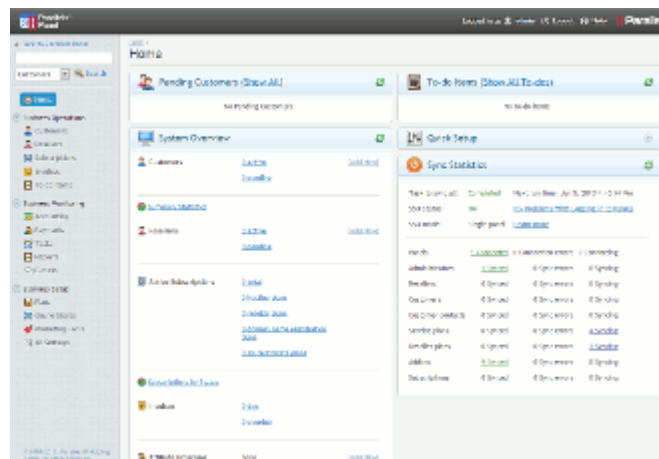
The main task of the Control Panel is managing hosting services. Customers use this panel to add domains and mailboxes, manage website content and so on. The administrator can use this panel to create their own hosting accounts - *webspaces* or access customer accounts. Learn more about webspaces and hosting management in the chapter **Web Hosting Management** (on page 324).

Power users also use the Control Panel but in *Power User view*. In this view, the Control Panel gets additional capabilities for server administration. Thus, power users can not only maintain their websites but control various server parameters, for example, switch off unused Apache modules or perform Panel update. Learn more about interface views in the section **Interface Views** (on page 24).

Parallels Plesk Panel Suite Components

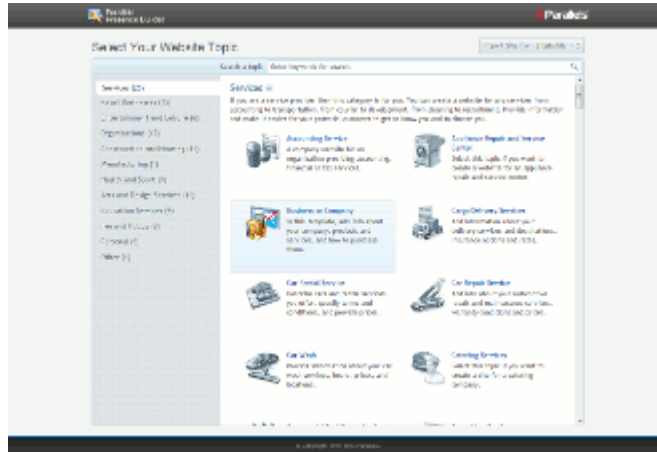
In addition to the standard Panel functionality, Parallels Plesk Panel suite offers two optional components that significantly increase Panel capabilities: *Customer & Business Manager* and *Presence Builder*. These components are tightly integrated with Panel and have their own user interfaces.

- *Customer & Business Manager*.



Customer and Business Manager (hereafter referred to as Business Manager) is an optional solution that automates all business operations, for example, charging customers and generating invoices. Note that Customer and Business Manager is an optional component and you may decide to use another solution or perform business operations manually. Learn more about Business Manager in the **Administrator's Guide to Parallels Customer and Business Manager**.

- *Presence Builder.*



Presence Builder is a site building tool that helps customers create polished, professional-looking web sites in record time based on more than 100 site templates. Learn more about the tool in the section **Building Websites with Presence Builder** (on page 467).

Next in this section:

Interface Views.....	24
Customizing Power User View	25

Interface Views

As mentioned earlier, each Panel user group carries out their own set of tasks through Panel. To better meet user needs, Panel offers two interface views: *Service Provider* and *Power User*. These views define what panels you use, what tools are present in these panels, and how the tools are organized.

- *Service Provider view.*
This view is convenient for HSPs as it is intended for selling hosting services. It has all the features required to create and manage customer accounts, subscriptions, and service plans. This view includes the Server Administration Panel and the Control Panel.
- *Power User view.*
This view is the best for power users - those who use Panel solely for personal needs, such as for maintaining a company portal or a mail server. In this view, both server administration and hosting services management take place in the Control Panel. As this view does not assume a reselling service to others is needed, it does not provide facilities for managing hosting plans, subscriptions, resellers, and customers. Also, as the server administration functions are included in the Control Panel in this view, the Server Administration Panel becomes unavailable.

This view can be tailored to needs of an administrator if you select *Custom view* in the view selector. For details on how to do the customization, read **Customizing Power User View** (see page 25).

You can change the Panel view any time from **Tools & Settings > Interface Management**.

Hosting Operations in Server Administration Panel

By default, when you want to perform an operation in a certain hosting account (for example, create a mailbox), you open this account with the link on the **Domains** or **Subscriptions** pages. The account is opened in a new window.

Since Panel 10.4, there has been no need to open hosting accounts in separate windows. This may be convenient when you want to perform a series of hosting operations on a group of accounts or you are just accustomed to carrying out all hosting tasks from a single GUI as in previous Panel versions. You can set Panel to perform all *hosting operations in the Server Administration Panel* on the **Tools & Settings > Interface Management** page. Once you activate the option, Panel will open hosting accounts in the interface that is similar to the Control Panel but shown on the current page of the Server Administration Panel.

Customizing Power User View

Power User view has a subtype, *Custom View* (available in **Tools & Settings > Interface Management**), which serves two main purposes:

- *To simplify the user experience of administrators who use managed hosting.*
Some administrators carry out only basic administration tasks (monitoring system services, administering user accounts, and so on) leaving more complex tasks, usually server and services configuration, to the support service of a service provider. This user group wants to have only tools they really need and hide the other tools.
- *Make Panel safer and more comfortable.*
Administrators can voluntarily revoke some of their permissions to hide the tools they do not need in everyday operations and return to the full-featured Power User view only if they need some system tuning (for example, to turn on server backups).

If you go to the **Tools & Settings > Custom View Settings** page (the **Administrative Tools** tab), you can select the tools the administrator will see in this view. The view settings may be unavailable if the service provider who gave you access to Panel has decided to lock Custom view.

Locking Custom View and Hiding Custom View Settings

To *lock* Custom view means to limit the selection of Panel features available to the administrator and disallow any changes to the features list. Thus, when Custom view is locked, it is impossible to switch to any other view from the GUI (or API RPC) or change the Custom view settings. Generally, if you are a service provider, you can make some tools unavailable to administrators, and, thus, separate Panel administration into two parts:

- **Day-by-day operations.** These operations are performed by the Panel administrator, the person who purchased the web hosting.
- **Complex configuration and maintenance.** These operations are accomplished by your support team. Such operations may include configuration of a network, DNS, web server and so on.

If a Panel administrator needs a certain feature and is unable to find it, your support team turns this feature on by unlocking Custom view, modifying the view settings, and locking the view again.

Custom view is locked *only* through a command-line call of the `poweruser` utility:

```
poweruser --on -simple true -lock true
```

The lock is removed by calling `poweruser --on -lock false`.

Custom View and Webspaces

The peculiarity of Custom view is that you can instantly adjust permissions, hosting parameters, PHP settings, and other webspace parameters *of all webspaces you have created in this view*. This is possible because each webspace you create in this view derives from the artificial *Custom* service plan that is not visible in the plans list. The settings of this plan are available in **Tools & Settings > Custom View Settings**. When you change the settings, the changes (if possible) are automatically applied to all webspaces under the Custom plan.

Another point that deserves attention is that the Custom plan has a special permission, *Ability to create, remove, and switch among webspaces*. If this permission is cleared in the GUI, it is not possible to create webspaces in Custom view.

If you need to adjust custom view settings through the command-line, use the `admin` utility. Learn more about the utility options in **Parallels Plesk Panel 11.5 for Linux (Windows): Reference for Command Line Utilities**.

CHAPTER 3

Web Servers

In this chapter:

Apache Web Server (Linux)	28
IIS Web Server (Windows)	41

Apache Web Server (Linux)

Parallels Plesk Panel for Linux uses the *Apache HTTP Server* (<http://httpd.apache.org/>) for hosting websites. Apache itself does not operate with websites; it manages virtual hosts - web resources identified either by an IP address or a host name. When you create a site, Panel adds a new virtual host to Apache so that the site becomes available through the web server.

By default, to achieve better performance when delivering web content, Apache is supplemented with another web server - *nginx*. For the details about how Apache is integrated with *nginx* in Panel and how to make Apache a standalone server, see [Apache with nginx](#) (on page 30).

Default Web Server Configuration

The file `/etc/httpd/conf/httpd.conf` defines Apache configuration for all virtual hosts in the system. The configuration files for virtual hosts are on the lowest level of the configuration files hierarchy. They are included into the Apache configuration file (`last_httpd.conf`) through several levels of inclusion using the `include` directive. The *nginx* web server is configured similarly: the `/etc/nginx/nginx.conf` file includes the configuration files of all virtual hosts through several levels of inclusion. To learn about the hierarchy of configuration files, see [Web Server Configuration Files](#) in the *Advanced Administration Guide*.

Each virtual host in the system has two files - `last_httpd.conf` and `last_nginx.conf` - that define default Apache and *nginx* configuration for this virtual host correspondingly. These files (located in `/var/www/vhosts/system/<domain_name>/conf/`) are generated automatically based on so-called configuration templates. Therefore, if you want to change the default web server configuration, you should adjust these template files. Learn how to do this in the [Changing Virtual Hosts Settings Using Configuration Templates](#) in the *Advanced Administration Guide*.

Custom Web Server Configuration

Website owners may need custom web server capabilities that are not provided by the default configuration. For example, unusual types of index files or the restricted access to the site by IP address. This can be done by overriding the default configuration for specific customers.

The default web server configuration can be overridden on the following levels:

- *Service plan*
The configuration defined on the service plan level overrides the *default* configuration. You can set any Apache and *nginx* directives for a particular service plan. These settings are stored in Panel database and will be applied to all customers' (plan subscribers') websites by default. See [Web Server \(Apache\)](#) (on page 571).

- **Website (virtual host)**
The custom *virtual host (website)* configuration overrides the configuration defined in its service plan. When you set Apache and nginx directives for a particular website, your directives are saved in the `vhost.conf`, `vhost_ssl.conf` and `vhost_nginx.conf` files (located in `/var/www/vhosts/system/<domain_name>/conf/`).

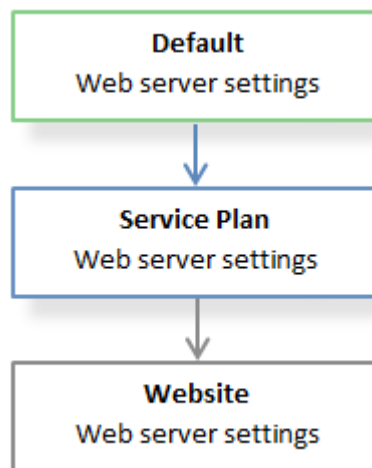
You can configure web server settings for a website (virtual host) in two ways:

- By specifying your settings in the Control Panel. When you save your changes, Panel creates corresponding directives in the virtual host configuration files. For details, see **Adjusting Apache Settings for Virtual Hosts** (on page 34) and **Adjusting nginx Settings for Virtual Hosts** (on page 35).
- By editing configuration files manually. For details, refer to the Advanced Administration Guide, **Virtual Host Configuration Files**.

Note: Only the Linux user `root` can add or modify custom Apache and nginx configuration files manually.

Note that website settings work only for the selected website and are used instead of the default settings and the service plan level settings.

See the hierarchy of web server settings on the diagram below.



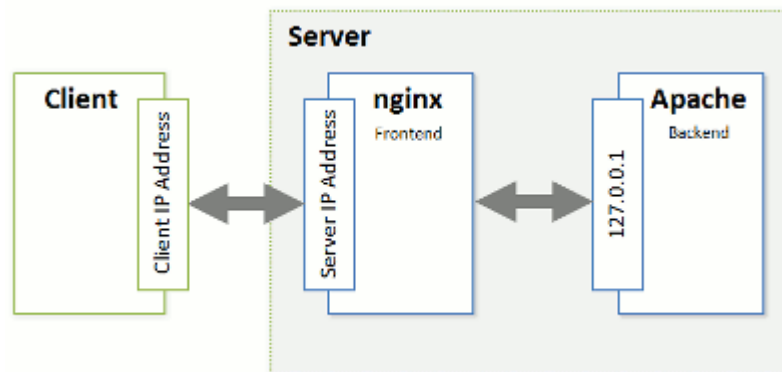
Next in this section:

Apache with nginx	30
Adjusting Apache Settings for Virtual Hosts.....	34
Adjusting nginx Settings for Virtual Hosts	35
Optimizing Apache Web Server.....	38

Apache with nginx

You can improve the work of the web server which hosts customer websites by installing *nginx*, a supplementary high-performance web server which is typically used as a reverse proxy server. This web server was specifically designed for delivering large amounts of static content (such as images, video, css, xml, and so on). As opposed to Apache, nginx is much more efficient when it comes to handling a large number of concurrent connections. Another advantage of this web server compared with Apache is that nginx has a significantly smaller memory footprint per client connection.

To leverage all the benefits of nginx, Panel configures it as a *reverse proxy server* that stands between the Internet and Apache (see the diagram below). This means that nginx becomes a frontend web server that processes all incoming requests from site visitors. The requests are sent to Apache which, in turn, distinguishes requests for static and dynamic content. If a request is for a static file (such as jpg, css, html, and so on), Apache passes the request through all registered handlers (applies `.htaccess` directory-level configuration, rewrites a URL, and so on) and returns to nginx a response which contains only the location of the requested file on the file system. nginx locates the file and sends it to the client. If the request is for a dynamic file (such as a PHP script), Apache executes the file and sends the response to nginx, which delivers it to the client.



Such a combination of nginx and Apache gives the following advantages:

- The maximum number of concurrent connections to a website increases.
- The consumption of server CPU and memory resources decreases. The maximum effect will be achieved for websites with a large amount of static content (such as photo galleries, video streaming sites, and so on).
- The efficiency of serving visitors who have a slow connection speed (GPRS, EDGE, 3G, and so on) improves. For example, a client with a 10 KB/s connection requests a PHP script, which generates a 100 KB response. If there is no nginx on the server, the response is delivered by Apache. During the 10 seconds required to deliver the response, Apache and PHP continue to consume full system resources for this open connection. If nginx is installed, Apache forwards the response to nginx (the nginx-to-Apache connection is very fast as both of them are located on the same server) and releases system resources. As nginx has a smaller memory footprint, the overall load on the system decreases. If you have a large number of such slow connections, use of nginx will significantly improve website performance.

The technical details on how Panel processes HTTP requests with the help of nginx are provided next in this section. For information on how to turn on the support for nginx in Panel, refer to the section **Installing nginx** (on page 34). If you do not want to use nginx, make Apache your frontend web server following the instructions in the section **Turning off nginx** (on page 34).

How Panel with nginx Processes HTTP Requests

To seamlessly integrate nginx with Apache, Panel uses two additional Apache modules:

- *mod_aclr2*. This module sets up a handler which runs after handlers of all other Apache modules (`mod_rewrite`, `.htaccess` related modules, `mod_php`, and so on). Therefore, if the request is for dynamic content, `mod_aclr2` will never get it as the request will be served by upper-level handlers of certain Apache modules (`mod_php`, `mod_perl`, `mod_cgi`, and so on). The only exceptions are SSI requests: once they reach `mod_aclr2`, it redirects them to proper handlers. If the request is for a static file, `mod_aclr2` searches for the exact file location on the file system and sends the location to nginx.
- *mod_rpaf*. From the point of view of Apache, all of its clients have the same IP address - the address of the nginx server (see the diagram above). This causes problems for websites and web apps that use client IP addresses for authentication, statistic purposes, and so on. `mod_rpaf` solves the problem by replacing the IP address of the nginx server in all requests with client IP addresses. In more detail, the module uses the special X-Forwarded-For header in which nginx puts the IP address of a client.

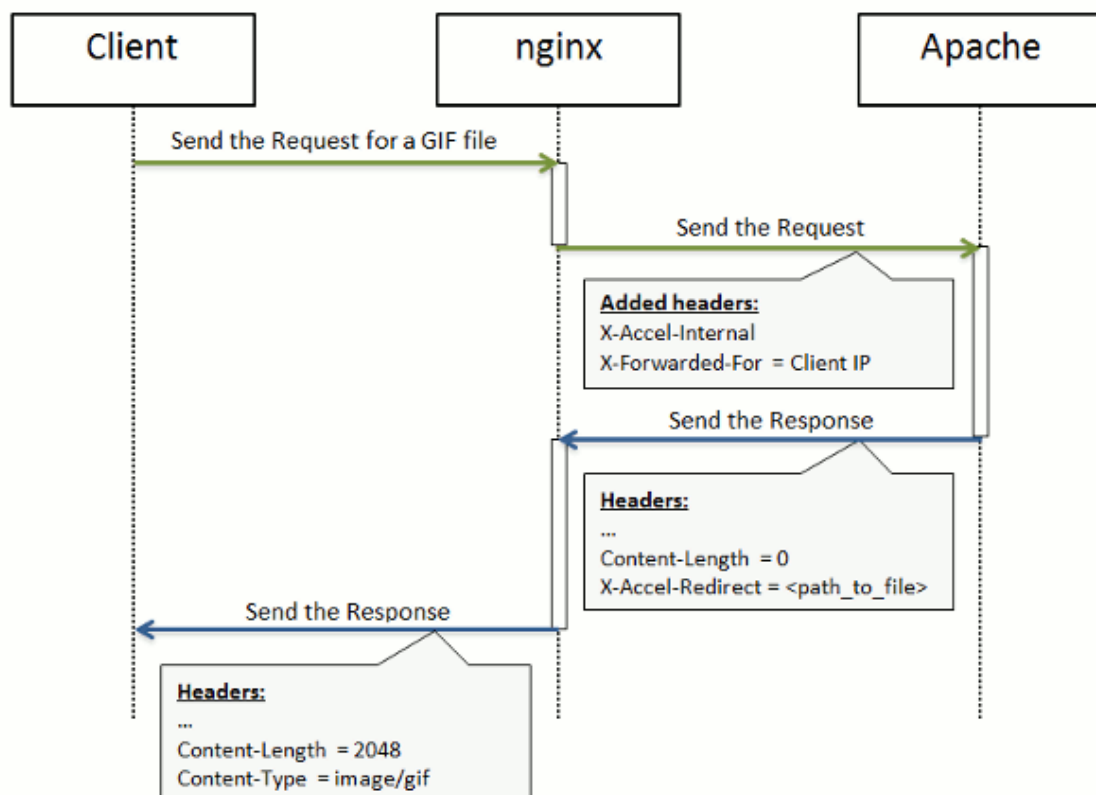
Let us take a closer look at how Panel processes requests for static and dynamic content with the help of these modules.

The sequence of processing an HTTP request for a static file is as follows (see the diagram):

1. A client sends a request to a web server.
2. nginx adds the *X-Accel-Internal* (used by `mod_aclr2`) and *X-Forwarded-For* (which contains the IP address of the client) headers to the request and sends the request to Apache.
3. Apache receives the request and starts to process it by registered handlers (applies `.htaccess` configuration, rewrites URL, and so on). In this step, `mod_rpaf` replaces the IP address of the nginx server in the `REMOTE_ADDR` Apache variable with the client's address from the *X-Forwarded-For* header.
4. After the request is processed by all registered handlers, it reaches `mod_aclr2`. The handler checks for the *X-Accel-Internal* header presence. If the header is present, the module sends to nginx a response with zero content length and the *X-Accel-Redirect* header. This header contains the exact location of the file as determined by `mod_aclr2`.
5. Once nginx receives the response, it locates the file and delivers it to the client.

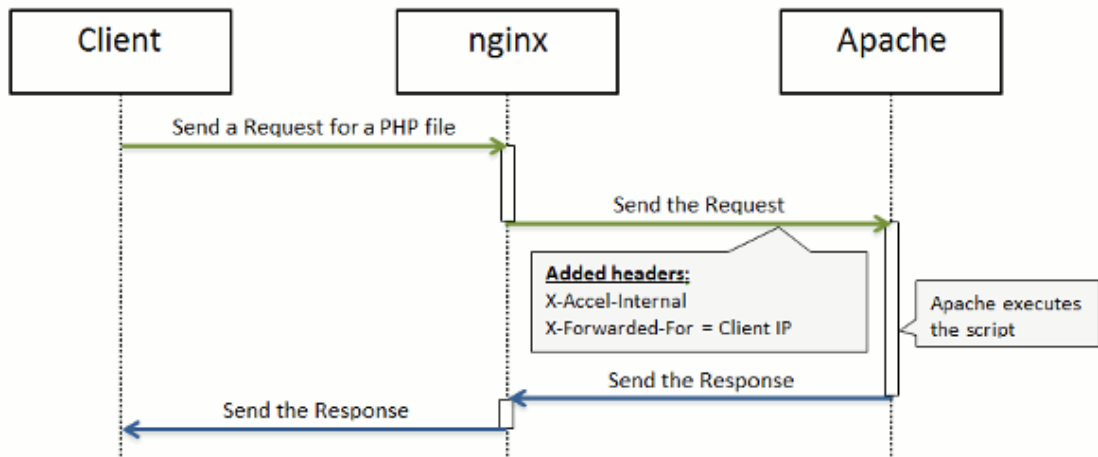
The diagram below is an example of how Panel handles a request for a 2 KB GIF file.

The Request for Static Content



In the case of processing requests for dynamic content, the steps from 1 to 3 are the same. Then the request passes to the handler of the appropriate Apache module (*mod_php*, *mod_perl*, *mod_cgi*, and so on). The request never reaches *mod_aclr2* (except for SSI requests). The handler generates a response and sends it to nginx, which, in turn, delivers the response to the client. The diagram below illustrates how Panel processes a request for a PHP file.

The Request for Dynamic Content



Next in this section:

Installing nginx 34
 Turning off nginx 34

Installing nginx

If you perform a clean installation of Panel 11, nginx will be turned on by default. If you upgrade from earlier versions, you can add the nginx component at any time after the upgrade in **Tools & Settings > Updates & Upgrades > Add Components**. Once the component is added, you should run the **Reverse Proxy Server (nginx)** service in **Tools & Settings > Services Management**.

You can view the version of the installed nginx server in **Tools & Settings > Server Components**.

Turning off nginx

To return to the configuration with a single Apache web server, stop the **Reverse Proxy Server (nginx)** service in **Tools & Settings > Services Management**.

To make nginx the frontend web server again, start the **Reverse Proxy Server (nginx)** service.

Note: The start and stop operations for the **Reverse Proxy Server (nginx)** service do not only start and stop nginx, they actually switch the web server configuration (nginx and Apache combination or just Apache as a frontend web server). The restart operation works in the same way as for all other services: the nginx service is restarted.

Adjusting Apache Settings for Virtual Hosts

You can customize Apache configuration for a particular website in the Control Panel on the **Websites & Domains > <domain_name> > Web Server Settings** page.

Adjusting Common Apache Settings

The section **Common Apache settings** contains the settings that website owners typically want to adjust. For example, to add custom index files or restrict access to the site by IP address. For each parameter, you can either type a custom value, or use the default Apache configuration (by selecting the **Default** value).

Note: As opposed to other web server settings, the **Deny access to the site** parameter does not override but supplements the list of IP addresses provided in the default configuration. In case of a conflict (for example, when you allow the address that is denied in the default configuration), your values will be used.

Adjusting Additional Apache Directives

To add Apache directives for a website that are not available in the **Common Apache settings**, use the **Additional directives for HTTP** and **Additional directives for HTTPS** fields. When editing the fields, use the syntax as in `httpd.conf`. For example, if you want to set a custom error page, add the line:

```
ErrorDocument 401 /my_error_page.html
```

Important: Your customers cannot view and edit these fields.

Adjusting nginx Settings for Virtual Hosts

By default, the Apache web server is working in conjunction with nginx. The benefits are that web pages load faster and server resources are saved. To learn how Apache and nginx collaborate by default, see **Apache with nginx** (on page 30).

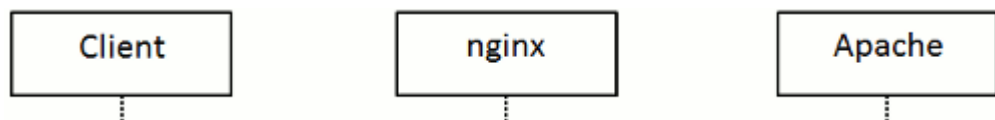
For any website, you can change the default way of Apache and nginx collaboration. More exactly, you can specify which web content (static or dynamic) should be processed by each of the servers. This can help optimize the performance of highly loaded web applications that have a lot of dynamic content (PHP files) or a lot of static content. The corresponding settings are available in the Control Panel on the **Websites & Domains > <domain_name> > Web Server Settings** page.

Note: nginx-related settings are available only if nginx is turned on.

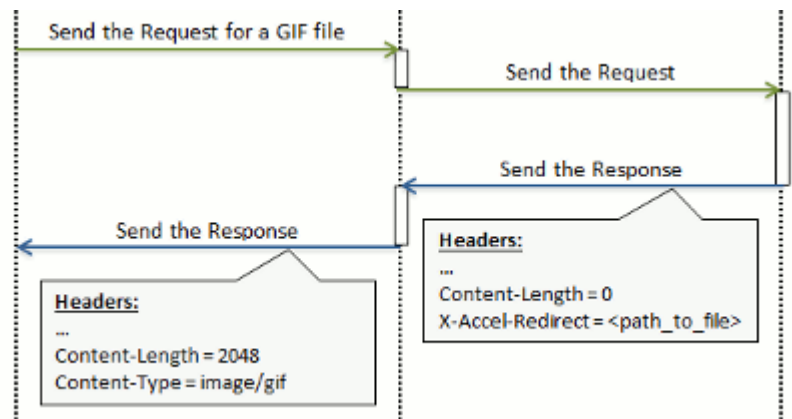
The diagrams below show all the possible configurations and provide comments on pros and cons of each configuration.

Processing Static Content

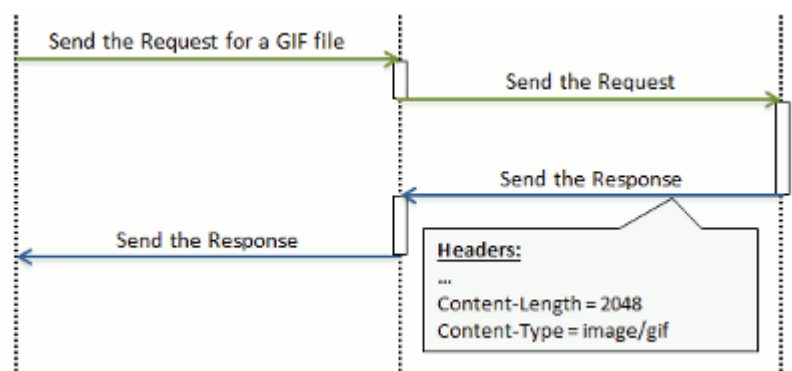
The following table shows how Panel will handle the request for a 2KB GIF image file depending on the nginx configuration.



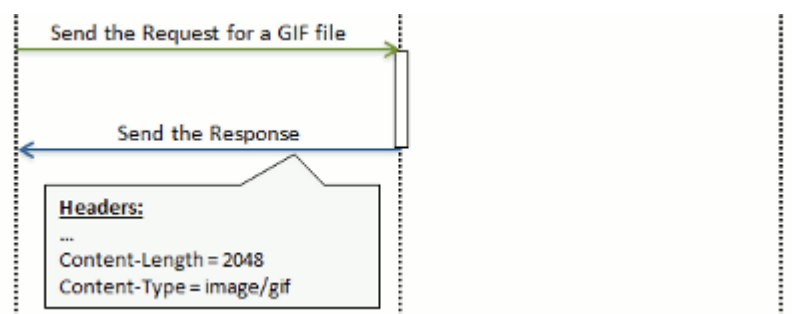
Smart static files processing is turned on



Smart static files processing is turned off

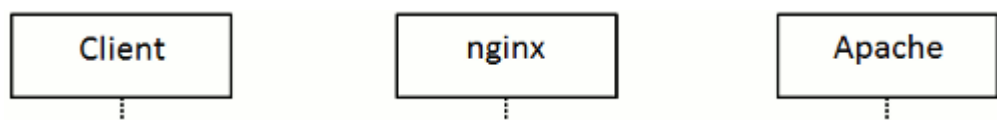


The GIF file extension is included into **Serve static files directly by nginx**

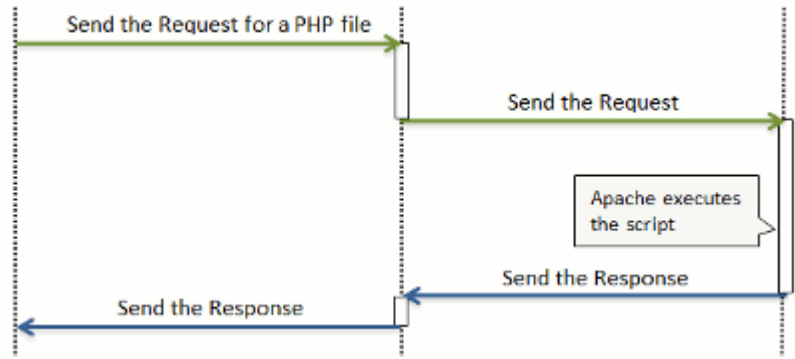


Processing Dynamic Content

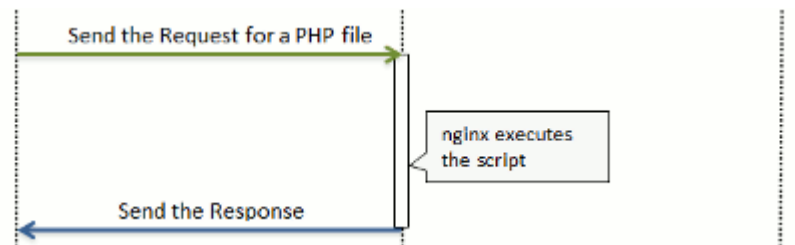
The following table shows how Panel will handle the request for a PHP file depending on the nginx configuration.



Process PHP by nginx is turned off



Process PHP by nginx is turned on



Important: To make the option **Process PHP by nginx** available, you should install PHP-FPM support for nginx. For details on installing PHP-FPM support, refer to the section **PHP Handlers** (on page 52).

Setting Up Additional nginx Directives

To add custom nginx directives for a website, use the **Additional nginx directives** field. When editing the field, use the syntax as in `nginx.conf`. For example, if you want to pack all the proxied requests with gzip, add the line:

```
gzip_proxied any;
```

Note that your customers cannot view and edit the **Additional nginx directives** field.

Optimizing Apache Web Server

To increase the performance of your Apache web server, you can employ the following practices:

- *Switching on and off Apache modules* allows decreasing the server resource consumption by using only Apache modules that you really need for proper functioning of websites on your server.
- *Running Apache with piped logs* increases the website density on the server.
- *Setting up the Apache restart interval* allows you to decrease the number of Apache restarts.

Next in this section:

Switching On and Off Apache Modules.....	39
Running Apache with Piped Logs	40
Setting Up the Apache Restart Interval	41

Switching On and Off Apache Modules

You can switch off the Apache web server modules that are not critical to hosting services in **Tools & Settings > Apache Web Server**. This will allow you to reduce server resources consumption (for example, get the smaller RAM footprint that is critical to VPS) and, as a result, provide for more hosting customers on a server.

Note that some modules are interdependent and can be switched off (on) only when the modules they depend on are off (on). For example, the *cache* module depends on *disk_cache*, *file_cache*, and *mem_cache* modules. This means that you cannot switch off the *cache* until its three dependent modules are off.

Caution: This feature is for advanced users only. Toggle modules only if you completely understand the consequences of your actions. Note that some modifications may reduce Apache performance or even lead to it becoming inoperable. In addition, these changes may affect certain Panel functions. For example, if you turn off *mod_perl* or *mod_php*, the Perl and PHP scripts (including webmail) will stop working on websites. This may cause a situation in which you offer a feature that does not work in a service plan.

Depending on your operating system, the following Apache modules are always enabled:

Debian or Ubuntu:

- *env*
- *auth_digest*
- *authn_file*
- *authz_host*
- *authz_user*
- *actions*
- *alias*
- *dav*
- *dav_fs*
- *mime*
- *ssl*

Redhat or CentOS:

- *env*
- *auth_digest*
- *authn_file*
- *authz_host*
- *authz_user*
- *actions*
- *alias*
- *autoindex*

- *dav*
- *dir*
- *log_config*
- *mime*
- *negotiation*
- *setenvif*
- *ssl*

SUSE:

- *env*
- *auth_digest*
- *authn_file*
- *authz_host*
- *authz_user*
- *actions*
- *alias*
- *dav*
- *dir*
- *log_config*

Running Apache with Piped Logs

If you are going to host more than 300 domains or web sites on your server, we recommend that you switch on the support for *piped logs* in the Apache web server. By default, Apache restarts when it needs to process log files, for example, rotate them. When the number of websites on your server is about 300 or more, this will slow down the server because of frequent Apache restarts. If you switch on the support for piped logs, Apache will write error and access logs through a pipe to another process instead of direct writing to log files. This lets Apache work without restarting every time it processes the logs.

You can switch on the support for piped logs using the **Tools & Settings > Apache Web Server > Piped Logs** option.

Note: If the number of websites you plan to host on your server exceeds 900, you should recompile Apache with more file descriptors as described in the section **Recompiling Apache with More File Descriptors** of the **Advanced Administration Guide**.

Setting Up the Apache Restart Interval

When users perform operations with domains and subdomains (such as creating, removing, or changing their configurations), the changes take effect only after the restart of Apache.

If you want to avoid too many Apache restarts, you can set a fixed interval of time in which Panel should restart Apache. Note that if the interval is 0 seconds, Apache restarts immediately after each change. It is recommended to always set this interval to more than 0 seconds, especially if users perform a lot of operations with domains and subdomains through Panel.

If during the specified interval of time no changes were made with domains, Apache will not restart.

IIS Web Server (Windows)

Parallels Plesk Panel for Windows uses the *IIS HTTP Server* (<http://www.iis.net/>) for hosting and managing websites.

IIS manages websites - web resources identified either by an IP address or a host name. When you create a site, Panel adds a new virtual host to IIS so that the site becomes available for browsers through the web server.

Default Web Server Configuration

The *default IIS configuration* is defined by the hosting provider using IIS tools such as IIS Manager. The default configuration is applied to all websites on the server. However, a number of configuration parameters can be changed for individual websites right in the Panel UI.

Custom Web Server Configuration

Website owners may need custom web server capabilities that are not provided by the default configuration. For example, unusual types of index files or the restricted access to the site by IP address.

You or site owners can configure web server settings for a website by specifying IIS settings in the Control Panel. The *custom website configuration* overrides the default configuration. For details about custom IIS configuration, see **Adjusting IIS Settings for Websites** (on page 42).

Next in this section:

Adjusting IIS Settings for Websites.....	42
IIS Application Pool	42

Adjusting IIS Settings for Websites

You or site owners can customize IIS configuration for a particular website in the Control Panel in **Websites & Domains** > select a domain > **Web Server Settings**. All the settings are divided into three groups:

- **Common Settings**
The section **Common settings** contains the settings that website owners typically want to adjust. For example, to add custom index files or allow directory browsing. For each parameter, you can either type a custom value, or use the default IIS configuration (by selecting the **Default** value).
- **Directory Security Settings**
The settings in the section **Directory security settings** allow you to enforce HTTPS connections and to prohibit anonymous access to the site.
- **Access Restriction Settings**
The settings in the section **Access restriction settings** allow you to control access to the website by IP addresses.

Note: As opposed to other web server settings, the **Deny access to the site** parameter does not override but supplements the list of IP addresses provided in the default configuration. In case of a conflict (for example, when you allow the address that is denied in the default configuration), your values will be used.

IIS Application Pool

IIS application pool serves websites and web applications hosted on your server. Dedicated IIS application pool allows your customers to have a level of isolation between websites. Since each dedicated application pool runs independently, errors in one application pool belonging to one user will not affect the applications running in other application pools dedicated to other users.

By default, Parallels Plesk Panel offers a shared application pool for all users. However, users can use dedicated application pools if this option is provided by the hosting package.

IIS application pool can work in the following two modes:

- **Shared pool** - one pool is used for all users and websites by default.
- **Dedicated pool** - separate pool for every customer is provided. It is also possible to allocate per-package pools within the customer's pool, that will isolate running websites hosted under a particular package from other customer's websites.

➤ ***To change the IIS application pool working mode:***

1. Go to **Tools & Settings** > **IIS Application Pool**.
2. Select the **Global Settings** tab.
3. Select the required mode and click **OK**.

➤ ***To limit the amount of CPU resources that the IIS application pool can use:***

1. Go to **Tools & Settings > IIS Application Pool**.
2. Select the **Switch on CPU monitoring** checkbox and provide a number (in percents) in the **Maximum CPU use (%)** field.
3. Click **OK**.

➤ ***To stop all applications running in the server application pool:***

1. Go to **Tools & Settings > IIS Application Pool**.
2. Click **Stop**.

➤ ***To start all applications in the application pool:***

1. Go to **Tools & Settings > IIS Application Pool**.
2. Click **Start**.

➤ ***To restart all applications running in the application pool:***

1. Go to **Tools & Settings > IIS Application Pool**.
2. Click **Recycle**. This can be handy if some applications are known to have memory leaks or become unstable after working for a long time.

Web Hosting

Web hosting configuration implies adjustment of a number of web server settings and settings of other related services. Thus, on Panel for Linux, you can switch off unused Apache modules; for IIS server, you can configure its application pool.

In this chapter:

Website Directory Structure.....	44
Website Preview	50
PHP Configuration.....	50
Multiple PHP Versions.....	58
Configuring ASP.NET (Windows).....	60

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 45) and **Virtual Host Structure (Windows)** (on page 47) 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:

Defining a Custom Virtual Host Template.....	45
Virtual Host Structure (Linux)	45
Virtual Host Structure (Windows).....	47

Defining a Custom Virtual Host Template

➤ *To define a custom virtual host template:*

1. On your local file system, create the following directories:
 - `cgi-bin` if you want to include custom scripts in the template.
 - `httpdocs` if you want to include custom documents such as web pages or images.
 - `error_docs` if you want to include custom error messages.
2. Place the files you need in the corresponding directories.
You can use the default files stored in the `/var/www/vhosts/.skel/0` on Linux or `C:\inetpub\vhosts\.skel\0` on Windows.
3. Pack the directories into an archive in `tgz`, `tar`, `tar.gz`, or `zip` format.
Make sure that the directories are in the root of the archive file and not in a subdirectory. If you include other directories or files in the root of the archive, Panel will not add them to the template.
4. Upload the archive to Panel on the **Tools & Settings > Virtual Host Template** page.

To switch back to the default virtual host template, go to **Tools & Settings > Virtual Host Template** and click the **Default** button.

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>	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	psadm	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`

Virtual Host Structure (Windows)

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 their first web user.

Directories Tree	User Permissions	Description	Created
<code>\<VHOST></code>	None		
<code>\plesk</code>	List contents		Always
<code>\statistics\<domain_name></code>	List contents	Statistics directory	Always
<code>\anon_ftpstat</code>	List contents	Anonymous FTP statistics	Always

\ftpstat	List contents	FTP user statistics	Always
\webstat	List contents	HTTP user statistics	Always
\.security	Read	Security settings	Always
\.web.<user>.security	Read		On demand
\anon_ftp	List contents	Anonymous FTP files	On demand
\cgi-bin	List contents	CGI scripts	On demand
\error_docs	List contents	Error message files	Always
<doc>.html	Read, write		
\httpdocs	Full control	HTTP documents	Always
\logs	List contents	Virtual host logs	Always
\web_users	None	Web users' directory	On demand
\<web_user>	None		
\<subdomain>	Full control	HTTP and HTTPS documents of a subdomain	On demand
\<domain>	Full control	HTTP and HTTPS documents of an additional domain	On demand

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 have different locations:

Old Location	New Location	Comment
\statistics	\.plesk\statistics	Statistics directory
\statistics\logs	\logs	Virtual host logs
\.security	\.plesk\.security	Security settings

<code>\.web.<user>.security</code>	<code>\.plesk\.security</code>	
--	--------------------------------	--

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

Website Preview

Your customers can preview their websites during domain name propagation. The two preview modes are available: *Quick Preview* and *Limited Preview*.

- *Quick Preview*, the recommended option, presents *customers' sites as subdomains of one of your domains*. For example, *customer-site.tld* will be available for preview as *customer-site.tld.192-0-2-12.your-domain.tld*. Here *192-0-2-12* is the site's IP where dots are replaced with dashes. Note that if you do not specify a preview domain, the site preview function will be unavailable to your customers.
- (Default) *Limited Preview* is used in earlier Panel versions; it presents customers' sites as directories on the Panel server. For example, *server-host-name:8443/sitepreview/http/your-domain.tld/*. This mode has two major drawbacks: Only authorized users can view such websites and some scripts and Flash animation might not work well on them. We recommend to use this mode only before the Quick Preview is configured.

Note that both these options do not work properly for password-protected directories.

The preview selector and the form to configure the preview domain name is located in **Tools & Settings > Website Preview Settings**.

Note: Customers also could preview their sites prior to Panel 10.4, but the preview feature had a number of limitations due to different implementation methods. The major difference is that since 10.4 customers can share the preview link with anybody, whereas previously they could only view the domain themselves. In addition, sites in the earlier preview mode would not work with complex CGI scripts or Flash content.

PHP Configuration

PHP is one of the most popular scripting languages for creating dynamic web pages. The majority of today's websites and web applications are based on PHP scripts. Thus, site administrators should clearly understand how they can control the execution of PHP scripts.

There are three main factors that define how PHP scripts will be executed for a certain website:

1. *PHP handler*.

When a visitor accesses a site based on PHP scripts, a web server interprets site scripts to generate a page that will be shown to the visitor. The PHP handler calls PHP libraries needed for this interpretation.

You can select a PHP handler for a service plan or a website correspondingly in:

- service plan settings (**Hosting Parameters** tab > **Scripting** > **Run PHP as**).
- website settings (**Control Panel** > **Websites & Domains** > select a domain > **General** tab > **Web Scripting and Statistics** > **Run PHP as**).

You can choose from a number of PHP handlers: ISAPI (Windows), Apache module (Linux), FastCGI, CGI, or PHP-FPM (Linux). What PHP handler to choose depends on factors such as security considerations, script execution speed, and memory consumption.

Learn about PHP handler features in the section **PHP Handlers** (on page 52).

2. *PHP version.*

Panel supports different versions of PHP. For each available handler, one or more PHP versions can be selected. For details, see **Multiple PHP Versions** (on page 58).

3. *PHP settings.*

PHP behavior is defined by a number of configuration settings. These settings specify various aspects of script execution, such as performance (for example, the amount of memory a script can use), security (for example, access to the file system and services), and so on. Administrators may adjust these settings for a number of reasons: to prevent a memory leak caused by poorly written scripts, to protect data from malicious scripts, to meet the requirements of a certain web app, and so on.

Learn about the PHP settings hierarchy and about how to adjust the settings in the section **Custom PHP Configuration** (on page 54).

Next in this section:

PHP Handlers	52
Custom PHP Configuration	54

PHP Handlers

The list of PHP handlers available in the Panel UI depends on the operating system and the web server that is processing PHP files. One of the handlers, PHP-FPM, additionally needs to be installed with the Parallels Installer.

You can choose one of the following PHP handlers at **Hosting Parameters > Scripting > Run PHP as** taking into consideration the resources consumption and security aspects of each option:

Run PHP as	Performance	Memory Usage	Security
Apache module (Linux only)	High. Runs as a part of the Apache web server.	Low	<p>This handler (also known as mod_php) is the <i>least secure option</i> as all PHP scripts are executed on behalf of the <code>apache</code> user. This means that all files created by PHP scripts <i>of any plan subscriber</i> have the same owner (<code>apache</code>) and the same permission set. Thus, it is theoretically possible for a user to affect the files of another user or some important system files.</p> <p>Note: You can avoid some security issues by turning the PHP <code>safe_mode</code> option on. This disables a number of PHP functions that have potential security risks. Note that this may lead to inoperability of some web apps. The <code>safe_mode</code> option is considered to be obsolete and has been removed since PHP 5.3.</p>
ISAPI extension (Windows only, <i>not supported since PHP 5.3</i>)	High. Runs as a part of the IIS web server.	Low	<p>The ISAPI extension can provide site isolation if a dedicated IIS application pool is switched on for subscriptions. Site isolation means that the sites of different customers run their scripts independently. Thus, an error in one PHP script does not affect the work of other scripts. In addition, PHP scripts run on behalf of a system user associated with a hosting account. Learn how to configure the IIS application pool in the section Configuring IIS Application Pool (Windows) (on page 42).</p> <p>Note: The ISAPI extension handler is not supported starting from PHP 5.3.</p>
CGI application	Low. Creates a new process for each request and closes it once the request is processed.	Low	<p>The CGI handler provides PHP script execution on behalf of a system user associated with a hosting account. On Linux, this behavior is possible only when the suEXEC module of the Apache web server is on (default option). In other cases, all PHP scripts are executed on behalf of the <code>apache</code> user.</p> <p>We recommend that you use the CGI handler only as a fallback.</p>

<p>FastCGI application</p>	<p>High (close to Apache module and ISAPI extension). Keeps the processes running to handle further incoming requests.</p>	<p>High</p>	<p>The FastCGI handler runs PHP scripts on behalf of a system user associated with a hosting account.</p>
<p>PHP-FPM application (Linux only)</p>	<p>High</p>	<p>Low</p>	<p>The PHP-FPM is an advanced version of FastCGI which offers significant benefits for highly loaded web applications. Unlike other handlers, PHP-FPM cannot be selected for all websites at once in service plan settings; you can use this handler only for individual websites.</p> <p>To be able to use this handler, install the support for PHP-FPM through Tools & Settings > Updates and Upgrades > Add/Remove components > Plesk hosting features > nginx web server and reverse proxy support > PHP-FPM support for nginx.</p> <hr/> <p>Important: Depending on your operating system, you may need to add third-party repositories to install PHP-FPM. Parallels Installer shows information about required repositories beside the component's name.</p> <hr/> <p>To use the PHP-FPM handler for a website:</p> <ol style="list-style-type: none"> 1. Go to Subscriptions > <domain_name> > Manage hosting or open the subscription in the Control Panel. 2. Go to Websites & Domains > <domain_name> > Web Server Settings page and turn on the option Process PHP by nginx. <p>Note that other PHP handlers are not available for selection if the option Process PHP by nginx is turned on.</p>

Note: Switching PHP from **Apache module** to **FastCGI application** may impair the functionality of existing PHP scripts. Switching to **PHP-FPM** by selecting **Process PHP by nginx** in the website's web server settings may do the same.

Adjusting the List of PHP Handlers Available to Customers

You can limit the list of PHP handlers available for customers using the `site_isolation_settings.ini` file. This file is available on both Windows and Linux Panel servers. For details, see **Configuring Site Isolation Settings** in the Advanced Administration Guide.

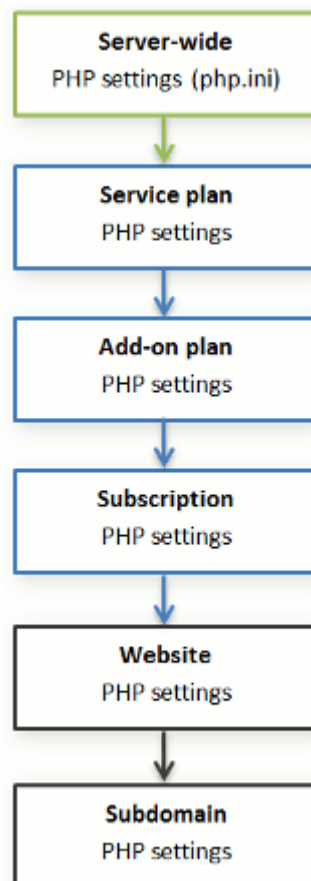
Custom PHP Configuration

Custom PHP Settings in Panel

Generally, PHP settings are defined by the server-wide configuration file. For Linux it is, typically, `/etc/php.ini` and for Windows - `%plesk_dir%\Additional\PleskPHP5\php.ini`. This file defines the PHP configuration for all websites hosted on your server.

Note: In Panel for Linux, you can add custom PHP handlers that can have their own `php.ini` located in some other directory.

Since Panel 10.4, *PHP settings are visible in the Panel GUI and you can adjust them individually for each hosting plan or subscription*. Moreover, your customers (if allowed) can adjust your PHP settings and preset them individually for each of their websites and subdomains. See the PHP settings hierarchy on the diagram below.



You can set the custom PHP configuration on the **PHP Settings** tab of a certain service plan, add-on plan, or subscription. Custom PHP settings for a website or subdomain can be set in the Control Panel, **Websites & Domains** > select a website or subdomain > **PHP Settings**. *PHP settings from a higher level act as a preset for a lower level, thus each lower level overrides them.* For example, you can purposely apply some PHP limitations to a service plan and then offer your customers the add-on plan that removes the limitations. PHP settings of the add-on plan will override the settings defined in the main service plan.

If customers have the corresponding permissions, they can specify the PHP configuration that is unique for each website (or subdomain) in their subscription.

Groups of PHP Settings

For convenience, all PHP settings in Panel are categorized into three groups:

- **Performance settings.**
These settings define how scripts work with system resources. For example: Use the `memory_limit` parameter to limit the amount of memory for a script and, as a consequence, to prevent memory leaks; or set `max_execution_time` to limit the maximum time a script is allowed to run, and thus prevent scripts from tying up the server.

Note: The typical default limit for PHP scripts is 60 seconds. Increasing the `max_execution_time` can affect limitations on the virtual host level. If you or your customers set a custom `max_execution_time` of PHP scripts on a site, and this value is greater than the web server's time limits on script execution (in Apache, nginx, and FastCGI settings), then the web server's time limits for this site will be set to the same value as PHP scripts' `max_execution_time`.

- **Common settings.**
This group contains other commonly used PHP settings. Generally, these are: Security settings (such as the PHP safe mode toggle or the permission to register global variables), error reporting settings (such as the directive to log errors), and so on.
- **Additional directives.**
If you cannot find particular parameters among performance or common settings, add them in the **PHP Settings > Additional configuration directives** field. All directives from that field will be included in the final PHP configuration. For example, if you want PHP to log errors to your own file, add the line:
`error_log=/tmp/my_file.log`. The entire list of PHP directives is available at <http://php.net/manual/en/ini.list.php>. As additional directives, you can add directives that have the `PHP_INI_USER` and `PHP_INI_ALL` modes.
Note that additional directives are available *only* to the Panel administrator. Your customers do not have a corresponding field in Control Panel.

Important: If you use Panel for Windows or Panel for Linux where PHP *does not* run as an Apache module, your customers can override some PHP settings regardless of any permissions in force. They can use the `ini_set()` function in their scripts to change the values of the following parameters: `memory_limit`, `max_execution_time`, and those of your additional directives that PHP allows to set anywhere (PHP_INI_ALL directives; learn more at <http://php.net/manual/en/ini.list.php>).

The Default Values of PHP Parameters

You can set the value of each parameter in **PHP Settings** 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*. The only exceptions are add-on plans: the value set to **Default** on the add-on's **PHP Settings** tab will keep the parameter's value from the main service plan.

It is possible to use three placeholders in parameter values:

- `{DOCROOT}` for the document root directory of a domain that gets custom PHP configuration.
- `{WEBSPACEROOT}` for the root directory of a subscription (webpace).
- `{TMP}` for the directory which stores temporary files.

Note: Default values of PHP settings in Panel differ from the ones suggested by the official PHP documentation at <http://php.net/manual/en/ini.list.php>.

Allowing Customers to Change PHP Settings

You can allow your customers to override subscription PHP settings with their own *per-website* and *per-subdomain* PHP configuration. For this purpose, you should use the following permissions on the **Permissions** tab of a certain service plan or subscription:

- **Hosting performance settings management.**
Along with management of some other settings, this permission grants customers access to PHP settings from the *performance settings* group.
- **Common PHP settings management.**
If granted, allows customers to adjust PHP settings from the *common settings* group.

Note that you can toggle these permissions for a plan (subscription) only if it has the granted **Hosting settings management** permission.

Even if your customers do not have permissions to adjust PHP settings, you (as the administrator) can always perform such per-website (subdomain) PHP configuration. To do this, open a hosting account from the Server Administration Panel and apply changes on the **PHP Settings** tab of the particular website (subdomain) you wish to change. The **Additional configuration directives** field will also be available to you.

Location of Website-Level PHP Settings in Panel for Windows

After you apply all the necessary modifications, you can view the modified `php.ini` for a certain website. The paths to the ini files are kept in the Windows registry, under *HKEY_LOCAL_MACHINE\SOFTWARE\PHP\Per Directory Values*. For example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\PHP\Per Directory  
Values\C\inetpub\vhosts\<DOMAIN NAME>\httpdocs
```

where *<DOMAIN NAME>* stands for a certain domain name.

Learn more about PHP settings in Windows registry at <http://php.net/manual/en/configuration.changes.php>.

Multiple PHP Versions

Most PHP versions are not backward-compatible. For example, 5 is not compatible with 4, 5.2 with 5.1, and so on. Therefore, a web app that requires PHP 4 might not work with PHP 5.3 supplied with Panel 11.5. To avoid this, you can install any PHP version on the server in addition to the supplied one. After registering this version in Panel, you can set it as default for certain service plans or any website in Panel. Customers granted the **Hosting settings management** permission will be able to specify the PHP version for a particular website.

Using Multiple PHP Versions in Panel on Linux

On Linux systems, you can install any PHP version you need and then make it available in Panel by registering it with the `php_handler` command-line utility.

➤ **To add the support for an arbitrary PHP version in Panel:**

1. Install the desired PHP version on your server. For installation guidelines, refer to the official PHP documentation available at <http://php.net/manual/en/install.php>. In brief, the installation includes the following main steps.

Warning: These steps are provided for demonstration purposes only. Depending on your operating system and the desired configuration, installation steps can differ significantly. When you install an additional PHP version on your server, read the official PHP documentation on installation.

1. Log in to your server as `root`.
2. Obtain the PHP source you need from the official website (<http://php.net/downloads.php>) and unpack it:

```
gunzip php-NN.tar.gz
tar -xf php-NN.tar
```

3. Configure and build PHP. This is when you can customize PHP with various options, such as specifying which extensions will be enabled. Run `./configure --help` for a list of available options.

```
cd ../php-NN
./configure --prefix /usr/local/phpNN
make
make install
```

4. Set up your `php.ini`:

```
cp php.ini-development /usr/local/lib/php.ini
```

You may edit your `.ini` file to set PHP options. If you prefer having `php.ini` in another location, run the `configure` utility with the option `--with-config-file-path=/some/path` in step 3.

2. Register the new PHP version in Panel:

```
/usr/local/psa/bin/php_handler --add -displayname <NN> -path  
<path to php cgi> -phpini <path to php.ini> -type <php handler> -id <NN-custom>
```

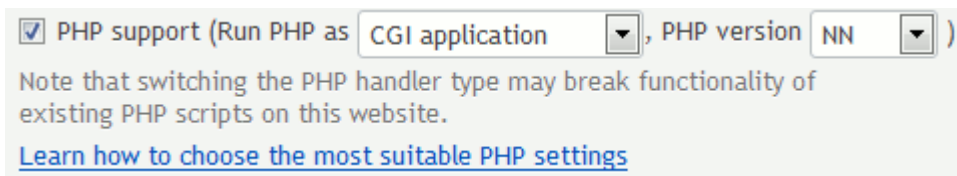
where

- `-displayname <NN>` is the PHP version name that will be shown in the Panel UI. We recommend that you include the version number in the `displayname`, for example, you can name the version "5.3.3-custom".
- `-path <path to php cgi>` is the location of the PHP CGI binary file. You can find this in the output of the command `make install` in the line *Installing PHP CGI binary*. For example, if you see the line *Installing PHP CGI binary: /usr/local/bin/*, the location you need to specify is */usr/local/bin/php-cgi*. Learn more at <http://php.net/manual/en/install.unix.commandline.php>.
- `-phpini <path to php.ini>` is the location of the `php.ini` file, for example, `/some/path/php.ini`.
- `-type <php handler>` is the type of the PHP handler associated with this version. Learn more about PHP handlers in the section **PHP Handlers** (on page 52).

Important: You can set either the *CGI* or *FastCGI* PHP handler. *mod_php* is not supported.

- (Optional) `-id <NN-custom>` is the identifier that you will use for referring to this PHP version when adjusting or removing it.

After you register the PHP version in Panel, it will be available for selection in service plan settings and in the hosting settings of a particular website. See the picture below.



Using Multiple PHP Versions in Panel on Windows

All up-to-date and commonly used versions of PHP are shipped with Panel and can be installed through **Tools & Settings > Updates and Upgrades > Add/Remove Components**.

You can specify a certain PHP version for a service plan and for a website in their hosting settings, in **PHP support > PHP version**:

- Version 4.x is outdated, use it only if you need to host old PHP application versions.
- Version 5.x is current and its use is recommended.




Configuring ASP.NET (Windows)

ASP.NET is a flexible set of tools and web development technologies that allows you to employ a number of applications based on ASP.NET framework. Parallels Plesk Panel supports 1.1.x, 2.0.x and 4.0.x versions of the .NET framework and allows configuring most of its settings. Most ASP.NET configuration settings that commonly need to be customized in order for ASP.NET applications to function in a desirable way can be edited through Parallels Plesk Panel.


➤ **To configure the server-wide ASP.NET settings:**

1. Go to **Tools & Settings > ASP.NET Settings** (in the Applications group). The settings for ASP.NET 1.1.x, ASP.NET 2.0.x and ASP.NET 4.0.x are located under the corresponding tabs.
2. Set up the strings that determine database connection data for ASP.NET applications which use databases. This option is available only for ASP.NET 2.0.x.

When you open the ASP.NET configuration page for the first time, sample connection parameters with common constructions are displayed. You can delete them and specify your own strings.

- To add a string, enter the required data into the **Name** and **Connection Parameters** input fields and click  next to them.
 - To remove a string, click  next to it.
3. Set up custom error messages that will be returned by ASP.NET applications in the **Custom Error Settings** field:
 - To set the custom error messages mode, select an appropriate option from the **Custom error mode** menu:
 - **On** - custom error messages are enabled.
 - **Off** - custom error messages are disabled and detailed errors are to be shown.
 - **RemoteOnly** - custom error messages are displayed only to remote clients, and ASP.NET errors are shown to the local host.
 - To add a new custom error message (which will be applied unless the **Off** mode was selected), enter the values in the **Status Code** and **Redirect URL** fields, and click .
 - **Status Code** defines the HTTP status code resulting in redirection to the error page.
 - **Redirect URL** defines the web address of the error page presenting information about the error to the client.

Due to possible conflicts, you cannot add a new custom error message with an error code that already exists, but you can redefine the URL for the existing code.

- To remove a custom error message from the list, click  next to it.
4. Configure compilation settings in the **Compilation and Debugging** field:
- To determine the programming language to be used as default in dynamic compilation files, choose an entry from **Page default language** list.
 - To enable compiling retail binaries, leave the **Enable debugging** checkbox empty.
 - To enable compiling debug binaries, select the **Enable debugging** checkbox. In this case, the source code fragments containing error will be shown in a diagnostic page message.

Note: When running applications in debug mode, a memory and/or performance overhead occurs. It is recommended to use debugging when testing an application and to disable it before deploying the application into production scenario.

5. Configure encoding settings for ASP.NET applications in the **Globalization Settings** section:
- To set an adopted encoding of all incoming requests, enter an encoding value into the **Request encoding** field (default is utf-8).
 - To set an adopted encoding of all responses, enter an encoding value into the **Response encoding** field (default is utf-8).
 - To set an encoding which must be used by default for parsing of `.aspx`, `.asmx`, and `.asax` files, enter an encoding value into the **File encoding** field (default is Windows-1252).
 - To set a culture which must be used by default for processing incoming web requests, select an appropriate item from the **Culture** list.
 - To set a culture which must be used by default when processing searches for a locale-dependent resource, select an appropriate item from the **UI Culture** list.
6. Set a code access security trust level for ASP.NET applications in the **Code Access Security** field.

CAS trust level is a set of restrictions applied to an app. For example, the Low level restricts app's network capabilities (like sending mail) while the Full trust level removes any restrictions.

- To allow changing the CAS trust level for websites, select the checkbox **Allow changing the CAS trust level for individual websites**. If you do not select this checkbox, websites will use the server-wide setting. Otherwise, each website will be able to have its own CAS trust level specified in the website's hosting settings.

Important: When an assembly is assigned a trust level that is too low, it does not function correctly. For more information on the permissions levels see http://msdn.microsoft.com/library/en-us/dnnetsec/html/THCMCh09.asp?frame=true#c09618429_010.

7. Set client session parameters in the **Session Settings** field:

- To set up the default authentication mode for applications, select an appropriate item from the **Authentication mode** list. **Windows** authentication mode should be selected if any form of IIS authentication is used.
- To set up time that a session can remain idle before it is abandoned, enter the appropriate number of minutes into the **Session timeout** field.

8. Click **OK** to apply all changes.

Note: Parallels Plesk Panel supports separate configurations for different versions of the .NET framework (1.1.x, 2.0.x and 4.0.x).

DNS

Your Parallels Plesk Panel works in cooperation with a DNS server which enables you to run the DNS service on the same machine where you host websites. Particularly, this server is *BIND* on Linux and *Microsoft DNS* or *BIND* on Windows. For instructions on switching between these two DNS servers on Windows, see **Using BIND Instead of Microsoft DNS (Windows)** (on page 72).

How Panel Creates DNS Zones

Setup of DNS zones for newly added domains is automated: When you add a new domain name to the Control Panel, a zone file is automatically generated for it and registered in the name server's database, and name server is instructed to act as a primary (master) DNS server for the zone. Subscribers can manage DNS zones of their domains through the Control Panel if their subscriptions provide the corresponding permissions. Additionally, subscribers can choose whether they want to use Panel DNS server as a master or a slave DNS server, or switch off the DNS service for their domains. To learn how to manage DNS zones of domains within a subscription, refer to the section **(Advanced) Configuring DNS for a Domain** (on page 386).

Panel creates DNS zones for domains in accordance with the *server-wide DNS template*. The template defines the structure of DNS zones for all domains in Panel. To learn how to edit the DNS template and apply its changes to existing zones, refer to the section **Server-Wide DNS Template** (on page 64).

Switching Off the DNS Service for Hosted Domains

Panel allows you to switch off the DNS service for all or certain domains hosted on your server. To learn how to do this, see the section **Switching Off the DNS Service** (on page 72).

External DNS Servers

If you do not want to run the DNS service on your Panel server, you can use an external DNS for domains hosted on your server. Learn more in the section **Using External DNS Servers** (on page 72).

Using Panel Without a DNS Server

You can exclude the DNS server component from your Panel installation. If you do this, Panel does not provide the DNS service for websites hosted on it until you install a DNS server or connect an external DNS service. To learn what happens when the DNS service is not configured in your Panel, see the section **Panel Without a DNS Server** (on page 74).

Next in this chapter, we will provide details on how to configure various aspects of the DNS service for domains hosted on your server.

In this chapter:

Server-Wide DNS Template	64
DNS Zones for Subdomains	69
Configuring the Recursive DNS	70
Restricting DNS Zones Transfer	71
Restricting Users' Access to Other Users' DNS Zones	71
Using BIND Instead of Microsoft DNS (Windows)	72
Switching Off the DNS Service	72
Using External DNS Servers	72
Panel Without a DNS Server	74

Server-Wide DNS Template

In Panel, DNS zones are built from the server-wide DNS template that is available in **Tools & Settings > DNS Template**. The DNS template defines which records Panel will create in DNS zones of hosted domains. For example, the `<domain>. A <ip.web>` record in the template may transform into something like `example.com. A 10.52.0.1` in the DNS zone file.

To learn how to define the DNS template, see the section **Adjusting DNS Template** (on page 65).

One of the main benefits the DNS template gives you is adjusting all DNS zones at once. In other words, it allows adding, modifying, or removing DNS records from all or a large amount of zones. To learn how Panel applies the server-wide DNS template changes to DNS zones, refer to the section **Applying DNS Template Changes** (on page 68).

Next in this section:

Adjusting DNS Template	65
Applying DNS Template Changes (Linux)	68

Adjusting DNS Template

Viewing the Default Records in the Server-Wide DNS Template

➤ **To view the default records in the server-wide DNS template:**

Go to **Tools & Settings > DNS Template**. All resource record templates will be displayed. The *<ip>* and *<domain>* templates are automatically replaced in the generated zone with real IP addresses and domain names.

Adding Resource Records to the Server-Wide DNS Template

➤ **To add a new resource record to the server-wide DNS template:**

1. Go to **Tools & Settings > DNS Template**.
2. Click **Add DNS Record**.
3. Select the resource record type and specify the record properties as desired.

Note that you can use *<ip>* and *<domain>* templates that will be replaced in the generated zone with real IP addresses and domain names. You can use a wildcard symbol (*) to specify any part of the domain name, and you can specify the exact values you need.

4. Click **OK**.

Removing Resource Records from the Server-Wide DNS Template

➤ **To remove a resource record from the server-wide DNS template:**

1. Go to **Tools & Settings > DNS Template**.
2. Select a checkbox corresponding to the record template you wish to remove, and click **Remove**.
3. Confirm removal and click **OK**.

Restoring the Default Configuration of the Server-Wide DNS Template

Panel provides you with the option to return the DNS template to the state in which it was right after Panel installation.

➤ ***To restore the original configuration of server-wide DNS template:***

1. Go to **Tools & Settings > DNS Template**.
2. Click **Restore Defaults**.

Editing the Start of Authority (SOA) Record

The Panel updates automatically the zone name, host name, administrator's e-mail address, and serial number, and writes the default values for the rest of Start of Authority record parameters to the zone files it maintains. If you are not satisfied with the default values, you can change them through the control panel.

➤ ***To change the Start of Authority (SOA) record settings in the server-wide DNS template:***

1. Go to **Tools & Settings > DNS Template**.
2. Click **SOA Records Template**.
3. Specify the desired values:
 - **TTL**. This is the amount of time that other DNS servers should store the record in a cache. The Panel sets the default value of one day.
 - **Refresh**. This is how often the secondary name servers check with the primary name server to see if any changes have been made to the domain's zone file. The Panel sets the default value of three hours.
 - **Retry**. This is the time a secondary server waits before retrying a failed zone transfer. This time is typically less than the refresh interval. The Panel sets the default value of one hour.
 - **Expire**. This is the time before a secondary server stops responding to queries, after a lapsed refresh interval where the zone was not refreshed or updated. The Panel sets the default value of one week.
 - **Minimum**. This is the time a secondary server should cache a negative response. The Panel sets the default value of three hours.
4. Click **OK**. The new SOA record parameters will be set for the newly created domains.

Usage of serial number format recommended by IETF and RIPE is mandatory for many domains registered in some high-level DNS zones, mostly European ones. If your domain is registered in one of these zones and your registrar refuses your SOA serial number, using serial number format recommended by IETF and RIPE should resolve this issue.

Parallels Plesk Panel servers use UNIX timestamp syntax for configuring DNS zones. UNIX timestamp is the number of seconds since January 1, 1970 (Unix Epoch). The 32-bit timestamp will overflow by July 8, 2038.

RIPE recommends using YYYYMMDDNN format, where YYYY is year (four digits), MM is month (two digits), DD is day of month (two digits) and NN is version per day (two digits). The YYYYMMDDNN format will not overflow until the year 4294.

➤ ***To change the Start of Authority (SOA) serial number format to YYYYMMDDNN for the server-wide DNS template:***

1. Go to **Tools & Settings > DNS Template**.
2. Click **SOA Records Template**.
3. Select the **Use serial number format recommended by IETF and RIPE** checkbox.

Note: See the sample of SOA serial number generated with the selected format. If the resulting number is less, than the current zone number, the modification may cause temporary malfunction of DNS for this domain. Zone updates may be invisible to Internet users for some time.

4. Click **OK**.

➤ ***To restore the default Start of Authority (SOA) serial number format (UNIX timestamp) for the server-wide DNS template:***

1. Go to **Tools & Settings > DNS Template**.
2. Click **SOA Records Template**.
3. Clear the **Use serial number format recommended by IETF and RIPE** checkbox.

Note: See the sample of SOA serial number generated with the selected format. If the resulting number is less, than the current zone number, the modification may cause temporary malfunction of DNS for this domain. Zone updates may be invisible to Internet users for some time.

4. Click **OK**.

Applying DNS Template Changes (Linux)

Once you change the structure of the server-wide DNS template, you can apply changes to existing zones in Panel for Linux by clicking **Apply DNS Template Changes**. The following options become available after clicking **Apply DNS Template Changes**:

- *Apply changes to unaltered zones.*
Use this option if you desire to obtain more control and apply changes only to direct template copies leaving user-modified zones for manual review and per-zone application.
- *Apply changes to all zones.*
Use this option to deliver changes to all zones at once.

To apply changes to a particular zone, open the related subscription in the Control Panel, and go to **Websites & Domains > <domain_name> > DNS Settings** and select the zone. You should see the corresponding button in the toolbar.

Note: If you apply changes to all zones, the zones become *unaltered* and will remain in this status until somebody modifies them. The same goes for a user-modified zone if you apply the changes directly to it.

In Panel for Windows, the changes in the server-wide DNS template are applied only to newly created zones.

The template changes are applied using the following rules:

- User-modified records *always* remain intact (are not modified or removed under any circumstances).
- Records added to the template are added to the zone.
- Records removed from the template are removed from the zone (if they were not changed by users before that).
- Records modified in the template are modified in the zone (if they were not changed by users before that).

Note: After restoration, migration, or upgrade, *all zones* are treated as user-modified by default, so no changes will be applied if you update something in the DNS template and forward the changes only to unaltered zones. If you wish to perform DNS zone changes in bulk after upgrade, apply the changes to *all zones* at the first time.

DNS Zones for Subdomains

Panel allows each subdomain to have its own DNS zone. These subdomain zones are useful if you wish to specify a custom name server for a particular subdomain or shorten the number of domain DNS records by rearranging them to subordinate zones. Generally speaking, subdomain DNS zones bring all domain DNS features to the subdomain level.

By default, Panel does not create separate DNS zones for subdomains. However, if you wish to try out this feature, use the following command-line call:

```
server_pref -u -subdomain-dns-zone own
```

To turn this feature off, use:

```
server_pref -u -subdomain-dns-zone parent
```

Learn more about running Panel utilities at

- (Linux) <http://download1.parallels.com/Plesk/PP11/11.5/Doc/en-US/online/plesk-unix-cli/37894.htm>
- (Windows) <http://download1.parallels.com/Plesk/PP11/11.5/Doc/en-US/online/plesk-win-cli/44076.htm>

Note: The default behavior in 10.4 versions before MU#9 was to create subdomain DNS zones. If you apply Update #9 to 10.4, the feature will remain active. Otherwise, the default behavior will be not to create the separate zones.

When subdomain zones are off, customers modify the parent domain's DNS zone by toggling Panel control over a particular subdomain zone. In fact, when they go to **Websites & Domains > <domain_name> > DNS Settings > Switch On/Off the DNS Service** and clicks **Manage** next to a subdomain name, the following situations are possible.

ON	Has no effect on the DNS zone of a parent domain.	
OFF	A new DNS zone is created for the subdomain, and all DNS records corresponding to this subdomain are removed from the parent domain's DNS zone.	Only A and AAAA records corresponding to this subdomain are added to the parent domain's DNS zone.

Configuring the Recursive DNS

Panel allows you to configure its DNS server to provide the *recursive service* for queries. With recursive service allowed, your DNS server, when queried, performs all the lookup procedures required to find the destination IP address for the requester. When recursive service is not allowed, your DNS server performs minimal number of queries only to find a server that knows where the requested resource resides and to redirect the requester to that server. Therefore, recursive service consumes more server resources and makes your server susceptible to denial-of-service attacks, especially when the server is set to serve recursive queries from clients outside your network.

After your install Parallels Plesk Panel, the built-in DNS server serves recursive queries only from your own server and from other servers located in your network. This is the optimal setting. If you upgraded from earlier versions of Parallels Plesk Panel, your DNS server may be configured to serve recursive queries from any host.

➤ ***If you want to change the settings for recursive domain name service:***

1. Go to **Tools & Settings > DNS Template > DNS Recursion**.
2. Select the option you need:
 - To allow recursive queries from all hosts, select **Any host**.
 - To allow recursive queries from your own server and hosts from your network, select **Localnets**.
 - To allow recursive queries only from your own server, select **Localhost**.
3. Click **OK**.

Restricting DNS Zones Transfer

By default, transfer of DNS zones is allowed only for name servers designated by NS records contained within each zone. If your domain name registrar requires that you allow transfer for all zones you serve, adjust the restrictions on DNS zones transfer as described below.

➤ ***To define hosts to which DNS zone transfers are allowed:***

1. Go to **Tools & Settings > DNS Template**.
2. Click **Transfer Restrictions Template**. A screen will show all hosts to which DNS zone transfers for all zones are allowed.
3. Click **Add New Address**.
4. Specify the registrar's IP or network address and click **OK**.

Restricting Users' Access to Other Users' DNS Zones

By default, users can create new subdomains and domain aliases in the DNS zones belonging to other users. This means that they can set up websites and e-mail accounts which could be used for spamming, phishing or identity theft.

➤ ***To prevent users from setting up domains and domain aliases in the DNS zones belonging to other users:***

1. Go to **Tools & Settings > Server Settings**.
2. Select the **Forbid users to create DNS subzones in other users' DNS superzones** checkbox.
3. Click **OK**.

Using BIND Instead of Microsoft DNS (Windows)

On Windows, there are two DNS servers available as Panel components: *Microsoft DNS* and *BIND*. The default Panel installation includes only *Microsoft DNS*. However, you can install the BIND DNS server and switch to it at any time.

➤ **To switch from Microsoft DNS to BIND:**

1. Go to **Tools & Settings > Updates and Upgrades** and install the BIND DNS server using the Parallels Installer.
2. Go to **Tools & Settings > Server Components** and click **DNS Server**.
3. Select **BIND DNS Server** and click **OK**.

When you have both DNS servers installed on your server, you can switch between them at any time on the page **Tools & Settings > Server Components > DNS Server**.

Switching Off the DNS Service

By default, Panel server acts as a primary name server for all hosted domains. However, if you do not want to provide the DNS service, you can switch it off by clicking **Switch Off** in the **Tools & Settings > DNS Template**. Note that this will switch off the DNS only for domains created after you click the button. Additionally, subscribers of service plans that include the permission **DNS zone management** will still be able to switch on the DNS for their domains through the Control Panel.

Using External DNS Servers

Although Panel provides all the instruments to run DNS on your server, you also can host the DNS zones on an external DNS server. This may be your own separate server or a third-party DNS service such as *Amazon Route 53* (<http://aws.amazon.com/route53/>) or *DynECT* (<http://dyn.com/dns/dynect-managed-dns/>).

By default, Panel is unable to automatically manage DNS zones on external DNS servers. To make this possible, you should write an integration script. The script should communicate with the DNS server's backend (like API) and apply all DNS zones changes occurred in Panel. To learn how to prepare such a script, refer to the document **Developing Extensions for Parallels Plesk Panel 11.5**, section **Integration with Third-Party DNS Services**.

Note: If you perform clean Panel installation and plan to use an external DNS server, you can exclude the DNS server component as described in the section **3. Choose Panel Components** of the **Installation, Upgrade, Migration, and Transfer Guide**. To learn how Panel behaves when it is not connected to an external DNS service and does not have a local DNS server, see the section **Panel Without a DNS Server** (on page 74).

With external DNS, all Panel features related to DNS are supported and work as usual, namely:

- DNS template, zones, and records management by means of the Panel UI, command-line utilities, and API requests.
- APS applications that use the DNS aspect.
- Other services that use DNS, for example, DomainKeys spam protection and Sender Policy Framework. To learn more, see the sections **Antispam Tools** (on page 83).

Integration with Amazon Route 53

An example of the script that integrates Panel with *Amazon Route 53* is available in the `/examples/route53-dns.zip` file from the `plesk-extensions-sdk.zip` archive available at <http://download1.parallels.com/Plesk/Doc/en-US/zip/plesk-extensions-sdk.zip>.

➤ **To integrate your Panel with Amazon Route 53:**

1. Download the file <http://download1.parallels.com/Plesk/Doc/en-US/zip/plesk-extensions-sdk.zip>.
2. Copy the file `route53.php` from the archive `/examples/route53-dns.zip` file to any location on your Panel server.
3. Specify your Amazon security credentials in the script (lines 23 and 24):

```
'client' => array(
    'key' => '<key>',
    'secret' => '<secret>',
),
```

4. Make the script `route53.php` readable by the user `psaadm`. Run:


```
chown psaadm /usr/share/route53.php
chmod 400 /usr/share/route53.php
```
5. Download the library for working with Amazon Web Services in PHP - `aws.phar` from <http://aws.amazon.com/sdkforphp/> and place it in the same directory with the script.
6. Run the following command line utility:

```
plesk bin server_dns --enable-custom-backend '/usr/bin/php
/<path_to_route53>/route53.php
```

Subscription Transferring Issue

If you transfer subscriptions from Panel with a local DNS service to Panel with an external DNS service, the DNS zones of the domains *are not transferred* to the external nameservers automatically. You should create the zones on the nameservers manually.

Panel Without a DNS Server

If you exclude a DNS server from your Panel installation (as described in the section **3. Choose Panel Components** of the **Installation, Upgrade, Migration, and Transfer Guide**) and do not connect an external DNS service, Panel does not provide the DNS service for websites hosted on it. Additionally, the following changes in Panel behavior take place:

- The **DNS Template** link is not displayed on the **Tools & Settings** page of the Server Administration Panel.
- In the Control Panel, the link **DNS Settings** in **Websites & Domains > <domain_name>** is replaced with the link **Whois Information** that opens a page with the information about the domain name registration.
- Panel users are unable to install web applications that require DNS zone management permission (or *DNS aspect*).
- Panel returns errors on attempts to manage its DNS server or DNS zones by means of the command line utility `dns` or API RPC requests with `<dns>` nodes.

Important: If you already have domains on your Panel server and then install a DNS server or connect an external DNS service, you should configure DNS zones of these domains manually. DNS zones for domains created after you configure DNS service in your Panel will be created automatically in accordance with the server-wide DNS template.

Mail

By default, your Parallels Plesk Panel works in cooperation with a mail server, which enables you to run the mail services on the same machine where you host websites.

The mail server settings are available in **Tools & Settings** > the **Mail** group. For details, see **Configuring Server-Wide Mail Settings** (on page 77).

Mail Server Software

By default, the *Postfix* mail server is installed on Parallels Plesk Panel for Linux, and *MailEnable* on Parallels Plesk Panel for Windows.

Other supported software is *Qmail* on Linux (shipped with Panel), and *IceWarp* or *SmarterMail* on Windows (need to be installed separately). For details, see **Using Other Mail Server Software** (on page 82).

Using Panel Without the Mail Server

Using the mail server in Panel is optional. Parallels Plesk Panel for Linux allows you to switch off or not install the mail service for all domains hosted on your server. On Windows, you cannot uninstall the default mail server, but you can change the server's configuration to prohibit outgoing mail.

Learn the aspects of using Panel without the mail server in **Using Panel Without the Mail Server** (on page 79).

Removing Mail Functionality from the Control Panel

You may want to prohibit your users from operating mail services, without uninstalling the mail server. In this case, you can hide some mail-related UI elements. For details, see **Removing Mail Functionality from the Control Panel** (on page 81).

Next in this chapter, we will provide details on how to configure various aspects of the mail service for domains hosted on your server.

In this chapter:

Configuring Server-Wide Mail Settings	77
Using Panel Without the Mail Server	79
Removing Mail Functionality from the Control Panel	81
Using Other Mail Server Software	82
Antispam Tools	83
Outbound Spam Protection	94

Antivirus Software	100
Webmail Software	102
Mailing Lists (Linux).....	103
Preventing Mass Email Sending (Linux).....	103
Mail Queue (Linux).....	104
Mass Email Notifications	105
Configuring Email Notifications.....	109

Configuring Server-Wide Mail Settings

By default, Panel works in cooperation with mail server software, which provides email services for mailboxes and mailing lists. After installation, the mail server is configured automatically and is ready to serve. However, we recommend that you review the default settings to make sure that they satisfy your needs.

➤ **To view or configure the mail service settings:**

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group). The server-wide mail preferences screen will open on the **Settings** tab.
2. Leave the **Enable mail management functions in Panel** checkbox selected if you want to allow your users to create mail accounts through Control Panel and use the mail services provided by the Panel-managed mail server. If you are using an external mail server, clear this checkbox.
3. If you want to limit the size of an email message that can be sent through your server, type the desired value in kilobytes into the **Maximum message size** box. Otherwise, leave this field blank.
4. To protect your server against unauthorized mail relaying or injection of unsolicited bulk mail, select the **Enable message submission** checkbox to allow your customers to send email messages through the port 587.



Also notify your customers that they need to specify in their email programs' settings the port 587 for outgoing SMTP connections, and be sure to allow connections to this port in your firewall settings.

5. Select the mail relay mode.

With closed relay the mail server will accept only mail addressed to the users who have mailboxes on this server. Your customers will not be able to send any mail through your outgoing SMTP server, therefore, we do not recommend closing mail relay.

With relay after authorization, only your customers will be able to receive and send email through your mail server. We recommend that you leave the **authorization is required** option selected, and specify allowed authentication methods:

- **POP3 lock time.** With POP3 authorization, once a user has successfully authenticated to the POP server, he or she is permitted to receive and send email through the mail server for the specified period of time.
- **SMTP.** With SMTP authorization, your mail server requires authorization if the email message must be sent to an external address.

Note for Windows hosting users: If you do not wish to use relay restrictions for networks that you trust, specify the network IP and mask in the **Use no relay restrictions for the following networks:** field (e.g., 123.123.123.123/16) and click the  icon. To remove a network from the list, click the  icon corresponding to the network you wish to remove.

The relay hosts on the networks in the list are considered not to be potentially operated by spammers, open relays, or open proxies. A trusted host could conceivably relay spam, but will not originate it, and will not forge header data. DNS blacklist checks will never query for hosts on these networks.

There is also an option to allow open relay without authorization, which, by default, is hidden from the user interface. Opening mail relay without authorization is not recommended because it allows spammers to send unsolicited mail through your server. If you want to set the open relay, log in to the server's file system, locate the file `root.controls.lock` in your Parallels Plesk Panel installation directory (`PRODUCT_ROOT_D/var/root.controls.lock` on Unix and `PRODUCT_DATA_D/var/root.controls.lock` on Windows platforms) and remove the line `/server/mail.php3:relay_open` from this file. The open relay option will show in your control panel.

6. Select the antivirus program that should be used on the server. For details, see **Antivirus Software** (on page 100).
7. Select the spam protection options that should be used on the server.

Note: If you wish to set up spam protection systems, such as SpamAssassin spam filter, or protection systems based on DomainKeys, DNS blackhole lists or Sender Policy Framework (SPF), proceed to the section **Antispam Tools** (on page 83).

8. If you are using Qmail mail server, you can also select the mail account format.

Selecting the **Use of short and full names is allowed** option will allow users to log in to their mail accounts by specifying only the left part of e-mail address before the @ sign (for example, `username`), or by specifying the full email address (for example, `username@your-domain.com`).

To avoid possible authorization problems for email users who reside in different domains but have identical user names and passwords, we highly recommend that you choose the **Only use of full mail account names is allowed** option.

Once you have set your mail server to support only full mail account names, you will not be able to switch back to supporting short account names until you make sure there are no encrypted passwords for mailboxes and user accounts with coinciding user names and passwords residing in different domains.

9. Click **OK** to submit the changes.

Using Panel Without the Mail Server

Using the mail server in Panel is optional. Parallels Plesk Panel for Linux allows you to switch off (uninstall) the mail service for all domains hosted on your server. On the Windows hosting, you cannot switch off the default mail server, but you can change its configuration to prohibit outgoing mail. Also, you can exclude the mail server from the installed components during Panel installation.

However, when the mail server is not installed or prohibited from sending outgoing mail, you face the problem: Panel still needs to send notifications, and customers' scripts may need to send emails. To solve this problem, Panel can send outgoing mail through an arbitrary external SMTP server.

Using an External SMTP Server for Outgoing Mail (Linux)

When the Panel-managed mail server is not installed, Panel uses the built-in SMTP client to send mail through the specified external SMTP server. By default, the client is not installed, and the link **External SMTP Server** is not available in **Tools & Settings > the Mail group**. Panel allows you to install the client only *instead of* the Panel-managed mail server.

To use the external SMTP server:

1. Uninstall the Panel mail server and install the SMTP client: In **Tools & Settings > Updates and Upgrades > Add/Remove Components > Mail hosting features** select **MSMTP relay only mail server (SMTP client)** instead of the selected mail server.
After you have uninstalled the Panel mail server, customers cannot use mail services. For details, see **Control Panel Functionality Without the Mail Server** below on this page.
2. Set the SMTP server in **Tools & Settings > External SMTP Server** (in the **Mail group**) and select at least one of the options:
 - **Allow Panel to send email notifications through this SMTP server**
 - **Allow users' scripts to send mail through this SMTP server** Other ways to set up the external SMTP server settings:
 - By the command line utility `mailserver` (the `--update-smtp-settings` command)
 - By API RPC requests with the `server` operator (`set.prefs` operation)
3. If the SMTP server requires authentication, you need to notify site owners about the credentials (**Username** and **Password**) that they should use in their scripts to enable the scripts to send mail.

Panel will send notifications and mail generated by scripts through the specified external SMTP server. Note that if you do not specify the external SMTP server settings, no mail services will be available.

After you install the client, only one link - **External SMTP Server** - will be found in **Tools & Settings > the Mail group**.

Note: If you exclude the mail server from the list of components during Panel installation, the SMTP client is automatically installed instead of mail server software. In this case, you will be prompted to provide the SMTP client settings during Panel installation.

Using an External SMTP Server for Outgoing Mail (Windows)

Panel has a built-in SMTP client that sends outgoing mail to the SMTP server specified in **Tools & Settings > External SMTP Server** (in the **Mail** group). By default, the Panel mail server is specified there, so that Panel sends all outgoing mail (including notification and mail generated by scripts) through the Panel mail server.

When you prohibit any outgoing mail from Panel mail server, you should specify another SMTP server in **Tools & Settings > External SMTP Server** (in the **Mail** group) and select at least one of the options:

- **Allow Panel to send email notifications through this SMTP server**
- **Allow users' scripts to send mail through this SMTP server.**

If the SMTP server requires authentication, you need to notify site owners about the credentials (**Username** and **Password**) that they should use in their scripts to enable the scripts to send mail.

Panel will send notifications and mail generated by scripts through the specified external SMTP server.

If you do not set the external SMTP server, no outgoing mail services will be available.

Control Panel Functionality Without the Mail Server

With the mail server uninstalled, Panel does not provide mail-related functionality for your subscribers. The **Mail** tab and UI elements related to mailboxes are not available. In addition, other changes take place when no mail server is installed:

- Webmail is not available.
- Users cannot install APS applications that require mail service.

Note that all the files and folders containing mail data of your subscribers remain on Panel server.

Important: When you perform transfer of domains from Panel with a mail service to Panel without the mail service, all the data that concerns domains' mailboxes *is not transferred*.

Removing Mail Functionality from the Control Panel

If you want to use a mail server running on a separate machine, or want to prohibit your users from operating mail services, you can remove controls related to managing email services and adding new mail accounts from the Panel UI. To do this, turn off the **Enable mail management functions in Panel** option. This option does not actually switch off the Panel-managed mail server, but only removes some UI elements from the Control Panel. These elements will be hidden from hosting service customers and their users. The following items are removed:

- The **Mail** tab.
- **Users** tab > *user name* > **Change Settings** > **Create an e-mail address under your account** option.

➤ ***To hide the user interface elements related to mail services from the Control Panel:***

1. In the Server Administration Panel, go to **Tools & Settings** > **Mail Server Settings** (in the **Mail** group).
2. Turn off the **Enable mail management functions in Panel** option and click **OK**.

Alternatively, you can hide mail-related functionality and corresponding permissions using the `/usr/local/psa/admin/conf/panel.ini` file. To do so, add the following line:

```
services.withoutMailService = true
```

Using Other Mail Server Software

Using Other Mail Server Software (Linux)

Panel for Linux is shipped with the *Postfix* and *Qmail* mail servers. You can switch between the two servers in **Tools & Settings > Updates and Upgrades > Add/Remove Components > Mail hosting features**.

Panel will start using the new mail server without any need for server restart. You can select another mail server at any time later.

Using Other Mail Server Software (Windows)

Apart from the default mail server (*MailEnable*), Panel for Windows supports *IceWarp* (*Merak*) and *SmarterMail*, which are not shipped with Panel but should be installed separately. To use IceWarp or SmarterMail, do the following:

1. Download and install the mail server software according to the instructions provided by the mail server manufacturer.
2. Log in to Panel and go to **Tools & Settings > Server Components > the Mail Server** link.

The mail server you have installed should now be displayed in the list of available mail servers.

3. Select the mail server you need and click **OK**.

Panel will start using the new mail server without any need for server restart. You can select another mail server at any time later.

Antispam Tools

To protect your users from spam, you can use the following tools with your Panel:

- **SpamAssassin spam filter.** It is a powerful spam filter that uses a wide variety of local and network tests to identify spam signatures.
You can configure the spam filter so as to either delete suspicious messages when they come to your mail server, or change the subject line and add "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers to the messages. The latter can be useful for users who prefer to filter mail with mail filtering programs installed on their own computers.
To learn more about SpamAssassin, visit <http://spamassassin.apache.org>.
To configure and switch on the SpamAssassin filter, proceed to the section **SpamAssassin Spam Filter** (on page 85).
- **DomainKeys.** DomainKeys is a spam protection system based on sender authentication. When an e-mail claims to originate from a certain domain, DomainKeys provides a mechanism by which the recipient system can credibly determine that the e-mail did in fact originate from a person or system authorized to send e-mail for that domain. If the sender verification fails, the recipient system discards such e-mail messages. To configure the DomainKeys system on your server, refer to the section **DomainKeys Protection** (on page 88).
- **DNS blackhole lists.** This spam prevention system is based on DNS queries made by your mail server to a database, which contains known and documented sources of spam, as well as an extensive listing of dynamic IP addresses. Any positive response from this database should result in your mail server returning a '550' error, or rejection of the requested connection.
To configure your mail server for working with DNSBL databases, proceed to the section **DNS Blackhole Lists** (on page 90).
- **Sender Policy Framework** (available only for Linux hosting). This spam prevention system is also DNS query-based. It is designed to reduce the amount of spam sent from forged e-mail addresses. With SPF, an Internet domain owner can specify the addresses of machines that are authorized to send e-mail for users of his or her domain. Receivers that implement SPF then treat as suspect any e-mail that claims to come from that domain but fails to come from locations that domain authorizes.
To learn more about SPF, visit <http://www.openspf.org/howworks.html>.
To enable filtering based on SPF, proceed to the section **Sender Policy Framework System (Linux)** (on page 92).
- **Server-wide black and white lists.** Black and white lists are standard mail server facilities. You can use black and white lists to block or receive mail from specific servers. Your mail server retrieves domain names and IP addresses of servers which attempt to establish connection with it. If a domain name is matched against black list entries, your server refuses the connection. Thus, the potential spam message will be never received. If an IP address is matched against white list entries, your server receives a message from the sender without using the spam protection systems such as sender authentication, greylisting, or DNSBL.
To set up server-wide black and white lists, proceed to the section **Server-wide Black and White Lists** (on page 90).

- **Greylisting** (available only for Linux hosting). Greylisting is a spam protection system which works as follows: For every e-mail message that comes to the server, sender's and receiver's e-mail addresses are recorded in a database. When a message comes for the first time, its sender and receiver addresses are not listed in the database yet, and the server temporarily rejects the message with an SMTP error code. If the mail is legitimate and the sending server is properly configured, it will try sending e-mail again and the message will be accepted. If the message is sent by a spammer, then mail sending will not be retried: spammers usually send mail in bulk to thousands of recipients and do not bother with resending.

The greylisting protection system also takes into account the server-wide and per-user black and white lists of e-mail senders: e-mail from the white-listed senders is accepted without passing through the greylisting check, and mail from the black-listed senders is always rejected.

When the greylisting support components are installed on the server, then greylisting is automatically switched on for all domains. You can switch off and on greylisting protection for all domains at once (at **Tools & Settings > Spam Filter Settings**), or for individual subscriptions (in **Control Panel > Mail tab > Change Settings**).

Next in this section:

SpamAssassin Spam Filter	85
DomainKeys Protection	88
DNS Blackhole Lists	90
Server-wide Black and White Lists.....	90
Sender Policy Framework System (Linux)	92
Greylisting (Linux).....	93

SpamAssassin Spam Filter

The SpamAssassin spam filter identifies spam messages among emails sent to mailboxes hosted on your Panel server. To achieve the desired level of spam protection, Panel lets you configure a number of SpamAssassin settings, namely:

- *Spam filter sensitivity*

To identify spam messages, SpamAssassin performs a number of different tests on contents and subject line of each message. As a result, each message scores a number of points. The higher the number, the more likely a message is spam. For example, a message containing the text string “BUY VIAGRA AT LOW PRICE!!!” in Subject line and message body scores 8.3 points. By default, the filter sensitivity is set so that all messages that score 7 or more points are classified as spam. If your users still receive spam messages with the default sensitivity, increase it by setting a lesser value, for example, 6. If SpamAssassin marks valid messages as spam, decrease the sensitivity by setting a higher value.

- *Spam marks*

At the server level, you cannot set the server-wide spam filter to automatically delete spam: you can do it only on a per-mailbox basis. So, for the server-wide policy, you can choose only marking messages as spam: `X-Spam-Flag: YES` and `X-Spam-Status: Yes` headers are added to the message source by default. If you want, the spam filter will additionally include a specific text string to the beginning of the messages' subject line (by default, this string is `*****SPAM*****`).

Though you cannot configure SpamAssassin to delete all spam messages, you can let each mailbox owner configure their own spam protection settings. This includes, for example, setting their spam filters to automatically delete messages marked by SpamAssassin, or setting up their personal black and white lists. For details on adjusting spam filtering settings for a specific mailbox, refer to the section **Protecting from Spam** (on page 530).

- *Maximum size of messages to check*

Analyzing a huge number of emails can heavily increase the load on your server. To avoid this, you can set the maximum size of the message that the spam filter will test.

- *Number of SpamAssassin processes*

Another way to limit the server loading by SpamAssassin is defining the maximum number of SpamAssassin processes (on Linux) or threads (on Windows) running simultaneously on the server.

- *Trusted languages and locales (only on Windows)*

You can define the language characteristics of mail that should always pass the filter by specifying trusted languages and locales. Letters written in the specified languages and with the defined character sets will not be marked as spam.

- *Black and white lists*

SpamAssassin lets you include certain senders into its *black* and *white* lists:

- If you do not want your users to receive e-mail from specific domains or individual senders, add the respective entries to the spam filter's black list.
- If you want to be sure that you and your users will not miss e-mail from specific senders, add e-mail addresses or entire domains to the spam filter's white list.

These settings are available to you on the **Tools & Settings > Spam Filter Settings** page.

Note: Panel exposes only basic SpamAssassin functionality. If you want to create complex antispam rules, edit SpamAssassin configuration files. For more information on advanced SpamAssassin configuration, refer to the **Advanced Administration Guide, Spam Protection** for both Linux and Windows and other respective documentation at http://spamassassin.apache.org/doc/Mail_SpamAssassin_Conf.html.

Next in this section:

Switching on SpamAssassin	86
Defining the Maximum Mail Size for SpamAssassin (Linux)	87
Configuring Black and White Lists	87

Switching on SpamAssassin

➤ *To switch on SpamAssassin:*

1. Go to **Tools & Settings > Spam Filter Settings** (in the **Mail** group).
2. Select the option **Switch on server-wide SpamAssassin spam filtering**.
3. To let your users set their own spam filtering preferences on a per-mailbox basis, select the option **Apply individual settings to spam filtering**.
4. Specify the maximum number of SpamAssassin processes in the field **Maximum number of worker spamd processes to run (1-5)**. We recommend that you use the default value.
5. Adjust the spam filter's sensitivity by typing the desired value in the field **The number of points a message must score to qualify as spam**.
6. On Windows, define the maximum size of messages that SpamAssassin will process by selecting the option **Do not filter if mail size exceeds specified size** and providing the desired value. On Linux, this parameter is unavailable in Panel. For details on editing the maximum mail size on Linux, see **Defining the Maximum Mail Size for SpamAssassin (Linux)** (on page 87).
7. Specify how to mark messages recognized as spam in the field **Add the following text to the beginning of subject of each message recognized as spam**. If you do not want the spam filter to modify message subject, leave this box blank. If you want to include into the subject line the number of points that messages score, type `_SCORE_` in this box.
8. On Windows, specify trusted languages and locales using the lists **Trusted languages** and **Trusted locales**.
9. Click **OK**.

Defining the Maximum Mail Size for SpamAssassin (Linux)

To decrease the load on your server caused by SpamAssassin, you can limit the maximum size of emails that SpamAssassin should analyze. All messages exceeding this size will be delivered to their recipients without checking.

➤ ***To define the maximum size of messages that SpamAssassin will process:***

1. Open for editing the configuration file `/etc/psa/psa.conf`
2. Specify the desired value in bytes for the parameter `SA_MAX_MAIL_SIZE`.

By default, the maximum email size is 256000 bytes. We recommend that you limit the maximum mail size to 150 - 250 Kbytes, which is usual for mail messages in HTML format with images. The size of the mail is considered critical for filter and server overload if it exceeds 500 Kbytes, which is usual for mail messages containing attachments.

Configuring Black and White Lists

➤ ***To add entries to the black or white list:***

1. Go to the corresponding tab of the **Tools & Settings > Spam Filter Settings** page.
2. Click **Add Addresses**.
3. Provide the list of entries you want to add to the list.

Separate addresses with a comma, a colon, or a white space. You can use an asterisk (*) as a substitute for a number of letters, and question mark (?) as a substitute for a single letter. For example: `address@spammers.net`, `user?@spammers.net`, `*@spammers.net`. Specifying `*@spammers.net` will block the entire mail domain `spammers.net`. If you use a Windows-based server, also specify what to do with messages coming from the specified addresses.

4. Click **OK**.

➤ ***To remove entries from the black or white list:***

Select the entries on the corresponding tab and click **Remove**.

Prohibiting Relaying Spam Through Panel Server on Windows

In Panel for Windows, the white list contains localhost (127.0.0.1) by default. This means that SpamAssassin does not check incoming messages sent from addresses hosted on your server. Spam senders may use this for relaying spam messages through your server.

➤ **To prohibit relaying mail for unauthenticated SMTP connections:**

Remove 127.0.0.1 from the white list.

DomainKeys Protection

➤ **To switch on spam protection based on DomainKeys:**

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group).
2. Under the **DomainKeys spam protection** group, select the following options:
 - **Allow signing outgoing mail.** Selecting this option allows you and your customers to switch on support for DomainKeys e-mail signing on a per-subscription basis through the Control Panel (**Control Panel > Mail tab > Change Settings**). It does not automatically switch on signing of outgoing e-mail messages.
 - **Verify incoming mail.** Selecting this option will configure the DomainKeys system to check all e-mail messages coming to e-mail users under all domains hosted on the server.
3. Click **OK**.

Now your mail server will check all incoming e-mail messages to ensure that they come from the claimed senders. All messages, sent from the domains that use DomainKeys to sign e-mail, which fail verification will receive the header *DomainKey-Status: 'bad'*. All messages, sent from the domains that do not participate in the DomainKeys program and do not sign e-mail, will be accepted without verifying.

➤ **To switch on signing outgoing e-mail messages for all domains in a subscription:**

1. Go to **Control Panel > Mail tab > Change Settings**.
2. Select the **Use DomainKeys spam protection system to sign outgoing e-mail messages** checkbox.
3. Click **OK**.

Now, the following will happen for the selected domains:

- Private keys are generated and placed in the server's database.
- Public keys are generated and placed in the TXT resource records created in the domains' DNS zones.
- The sender's policy advertised in the DNS TXT resource records is set to "all e-mail messages sent from this domain must be cryptographically signed; if someone receives an e-mail message claiming to originate from this domain, which is not signed, then this e-mail must be discarded."
- Outgoing e-mail messages are digitally signed: the "DomainKeys-Signature" header containing a signature based on a private key is added to the message headers.

DNS Blackhole Lists

You can use free and paid subscription blackhole lists with your server.

➤ ***To switch on spam protection based on DNSBL:***

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group).
2. Select the **Switch on spam protection based on DNS blackhole lists** checkbox.
3. In the **DNS zones for DNSBL service** input box, specify the host name that your mail server should query, for example: `sbl.spamhaus.org`.
4. Click **OK**.

Now, e-mail messages from known spammers should be rejected with an error code 550 (connection refused).

Important: If you use the Qmail mail server and switch on DNSBL, senders with IP addresses from the blackhole list will not be able to send email even if they pass SMTP authentication. To avoid this problem, switch on the message submission as described in the section **Configuring Server-Wide Mail Settings** (on page 77).

Server-wide Black and White Lists

➤ ***To reject connections from specific mail servers:***

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group).
2. Click the **Black List** tab.
3. Click **Add Domain**.
4. Specify the name of the domain from which you do not want to receive e-mail. For example, 'evilspammers.net'.
5. Click **OK**.
6. Repeat steps from 3 to 5 to add as many domains as required.

➤ ***To assure mail reception from specific servers or networks:***

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group).
2. Click the **White List** tab.
3. Click **Add Network**.
4. Specify an IP address or range of IP addresses from which mail must always be accepted.

5. Click **OK**.
6. Repeat steps from 3 to 5 to add as many addresses as required.

Sender Policy Framework System (Linux)

➤ *To set up support for Sender Policy Framework on your Linux-based server:*

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group). The server-wide mail preferences screen will open on the **Settings** tab.
2. Select the **Switch on SPF spam protection** checkbox and specify how to deal with e-mail:
 - To accept all incoming messages regardless of SPF check results, select the **Create only Received SPF-headers, never block** option from the **SPF checking mode** drop-down box. This option is recommended.
 - To accept all incoming messages regardless of SPF check results, even if SPF check failed due to DNS lookup problems, select the **In case of DNS lookup problems, generate temporary errors** option from the **SPF checking mode** drop-down box.
 - To reject messages from senders who are not authorized to use the domain in question, select the option **Reject mail if SPF resolves to fail** from the **SPF checking mode** drop-down box.
 - To reject the messages that are most likely from senders who are not authorized to use the domain in question, select the option **Reject mail if SPF resolves to softfail** from the **SPF checking mode** drop-down box.
 - To reject the messages from senders who cannot be identified by SPF system as authorized or not authorized because the domain has no SPF records published, select the option **Reject mail if SPF resolves to neutral** from the **SPF checking mode** drop-down box.
 - To reject the messages that do not pass SPF check for any reason (for example, when sender's domain does not implement SPF and SPF checking returns the "unknown" status), select the option **Reject mail if SPF does not resolve to pass** from the **SPF checking mode** drop-down box.
3. To specify additional rules that are applied by the spam filter before the SPF check is actually done by the mail server, type the rules you need in the **SPF local rules** box.

We recommend that you add a rule for checking messages against the open database of trusted senders, for example, 'include:spf.trusted-forwarder.org'. For more information on SPF rules, visit <http://tools.ietf.org/html/rfc4408>.

4. To specify the rules that are applied to domains that do not publish SPF records, type the rules into the **SPF guess rules** box.

For example: `v=spf1 +a/24 +mx/24 +ptr ?all`

5. To specify an arbitrary error notice that is returned to the SMTP sender when a message is rejected, type it into the **SPF explanation text** box.

If no value is specified, the default text will be used as a notification.

6. To complete the setup, click **OK**.

Greylisting (Linux)

When the greylisting support components are installed on the server, greylisting protection is automatically switched on for all domains. Therefore, no additional actions are required. If you do not want to use greylisting protection, you can switch it off.

➤ ***To switch off greylisting protection for all domains:***

1. Go to **Tools & Settings > Spam Filter Settings** (in the **Mail** group).
2. Clear the **Switch on server-wide greylisting spam protection** checkbox.
3. Click **OK**.

➤ ***To switch on greylisting protection for all domains:***

1. Go to **Tools & Settings > Spam Filter Settings** (in the **Mail** group).
2. Select the **Switch on server-wide greylisting spam protection** checkbox.
3. Click **OK**.

➤ ***To switch off greylisting protection for all domains in a subscription:***

1. Go to **Control Panel > Mail tab > Change Settings**.
2. Clear the **Switch on greylisting spam protection for all mail accounts under this domain** checkbox.
3. Click **OK**.

➤ ***To switch on greylisting protection for all domains in a subscription:***

1. Go to **Control Panel > Mail tab > Change Settings**.
2. Select the **Switch on greylisting spam protection for all mail accounts under this domain** checkbox.
3. Click **OK**.

Outbound Spam Protection

If your hosting offerings include mail services, keep in mind that your mail server can be used for malicious purposes. For example, spammers can use compromised accounts for sending mass e-mails containing spam or viruses, compromised computers (also called zombies) could relay spam through your server, and so on. This may cause an increased load on the server, spam or malware complaints from recipients, or your server's IP addresses may be added to public black lists.

To prevent sending spam and other malicious messages from your server, we offer *Parallels Premium Outbound Antispam* (hereafter referred to as Outbound Antispam). This is an additional Panel component that analyzes all outgoing mail and blocks sending of undesired messages. To learn how to install Outbound Antispam, see the section **Installing Parallels Premium Outbound Antispam**. (on page 95)

To detect outgoing spam and virus messages, the component uses the external Parallels Premium Outbound Antispam service that identifies outbreaks of spam and email-borne malware over the Internet in real time. Every email outbreak can be identified by one or more recurrent patterns, even if messages within the attack differ from each other. The Parallels Premium Outbound Antispam service detects such outbreaks using constantly updated global service repositories where all spam and virus patterns are stored. When your mail server (qmail or Postfix) is requested to send a message, the local Outbound Antispam component extracts the message patterns and compares them to its local cache or sends to the service repository to identify whether they were seen in global spam or virus attacks. All messages which patterns were identified as malicious are blocked. An even more important benefit of using Outbound Antispam is that it allows you to identify spammers who use your server within the first few messages they send out, allowing you to prevent them from issuing the attack. In addition, the component counts mail from each unique sender notifying you when a sender exceeds a certain message threshold.

To learn how to turn on and configure protection from outbound spam on your server, see the section **Configuring Protection** (on page 96).

Mail Classification

Outbound Antispam uses the following mail classification.

Type	Description
Confirmed spam	Spam messages that contain patterns seen in global spam attacks. For example, these messages are sent from compromised computers (zombies).
Bulk spam	Spam messages sent in bulk quantities from sources that were not yet identified as spammers. The patterns of such messages were seen in global spam attacks.

Suspected spam	Messages that are sent in bulk quantities but not yet confirmed as spam. This can be sending of legitimate mass e-mails as well as spam messages in the first few seconds of the attack.
Virus messages	Messages that either contain characteristics of confirmed malware or with high likelihood pose a malware threat.
Valid mail	Legitimate messages for which Outbound Antispam does not have any incriminating information.
Non spam	Messages that are confirmed, without doubt, as coming from trusted sources. This classification is very rarely used.

Next in this section:

Installing Parallels Premium Outbound Antispam	95
Configuring Protection	96

Installing Parallels Premium Outbound Antispam

To start using Parallels Premium Outbound Antispam, perform the following steps:

1. *Install the component.* This is done from the **Tools & Settings > Updates & Upgrades**. After the installation is completed, you will find the component on the **Tools & Settings > Outbound Spam Filter** page.
2. *Activate the component.* Parallels Premium Outbound Antispam requires a separate license key. You can purchase such a key from your service provider or directly from Parallels. Once you have obtained a key, install it to Panel using the **Tool & Settings > License Management > Additional License Keys** page.

Configuring Protection

Setting up outbound spam protection with Parallels Premium Outbound Antispam includes configuration of the following aspects:

1. *Connection settings* (on page 97). To let the Parallels Premium Outbound Antispam component installed on your Panel communicate with the external part of the antispam system (the repositories), you should configure the component's connection settings.
2. *Sender identification policy* (on page 98). To effectively fight sending of spam, the outbound antispam solution includes a mechanism that allows you to identify the actual e-mail senders even if they send spam from multiple e-mail addresses. You should define how the system will identify senders.
3. *Saving of message samples* (on page 98). To track suspicious activities of senders on your server, you can configure Parallels Premium Outbound Antispam to save message samples in a specified directory to let you analyze them later.
4. *Protection policy* (on page 98). To define how the system will handle spam and malware messages, configure the *protection policy*. For example, you can prohibit sending of spam messages or limit the total number of messages from a single sender. Additionally, if you are sure that a certain sender is not a spammer, you can add them to the *white list* or *bulk senders list*. The system will send mail from these senders bypassing some of the antispam checks.

Next in this section:

Connection Settings	97
Sender Identification Policy	98
Saving Message Samples	98
Protection Policy.....	98

Connection Settings

To detect malicious messages, Parallels Premium Outbound Antispam uses the external Parallels Premium Outbound Antispam service that checks patterns of outgoing mail. As Parallels Premium Outbound Antispam requires a permanent connection to the service, the default policy prohibits sending *any* messages when the service is unavailable. This could happen, for example, if your Parallels Premium Outbound Antispam license key has expired or due to network connection problems.

To let users send e-mails when the service is unavailable, select the checkbox **Skip scanning when the service is unavailable** in **Tools & Settings > Outbound Spam Protection > Server Configuration** tab.

Note: The Parallels Premium Outbound Antispam service address is specified in the corresponding field on the **Server Configuration** tab of the Parallels Premium Outbound Antispam page. Normally, you should not change the default value `resolver@d.plesk.ctmail.com`. The only exception is when you experience connectivity problems and want to troubleshoot them.

Sender Identification Policy

An important aspect of outbound spam protection is identification of mail senders. The sender identification allows you to know the problematic users or accounts on your server and take actions to prevent them from sending more spam or doing other actions related to mail sending.

To let you effectively recognize unique senders, Parallels Premium Outbound Antispam offers you the following ways of identification:

- *SMTP authentication username*. If your Panel server uses SMTP authentication, Parallels Premium Outbound Antispam will identify users by usernames provided during the SMTP authentication. To switch on the SMTP authentication in Panel, go to **Tools & Settings > Mail Server Settings > Relay options**.
- *IP address* from which a sender connects to your server.
- *SMTP authentication username if available; otherwise, IP address*.
- *Custom mail header*. This may be any string of text included in the message header.

For example, if you choose *IP address*, the system will identify all users that connect to your server from this IP address as a single sender even if they use different e-mail addresses. To choose a way to identify unique senders, select the corresponding option in the **Tools & Settings > Outbound Spam Protection > Unique Sender Identifier** tab.

Saving Message Samples

To keep track of suspicious activities of e-mail senders and identify potential spammers, you can configure Parallels Premium Outbound Antispam to save samples of outgoing messages to a specific directory. To do this, select the corresponding checkbox in the **Tools & Settings > Outbound Spam Protection > Unique Sender Identifier** tab, specify the directory, and enter the *thresholds* for different message types: *spam*, *suspected spam*, and *virus messages* (see the classification in **Protecting from Outbound Spam** (on page 94)). When a number of messages of a certain type from a sender reaches the corresponding threshold, the system adds the last of these messages to the specified directory to let you analyze the message's content later. Then the system starts counting messages again from zero. For example, if you set the threshold for suspected messages to *10*, the system will save each tenth suspected message.

Note: The thresholds do not limit the number of messages that each sender can send.

Protection Policy

The *protection policy* settings located on the **Tools & Settings > Outbound Spam Protection > Protection Policy** tab define what types of messages according to the Parallels Premium Outbound Antispam classifications the system will block.

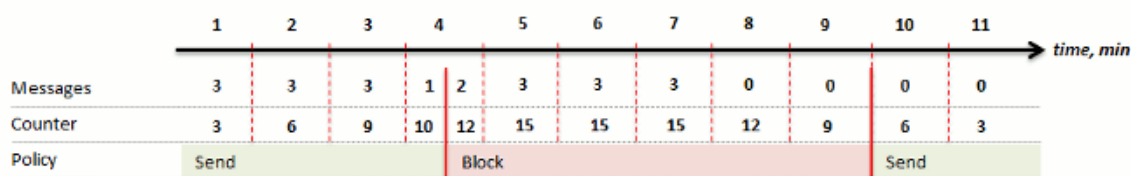
As described in the section **Protecting from Outbound Spam** (on page 94), protection works in the following way: When the Panel mail server receives a request to send a message, the Outbound Antispam component extracts message patterns and sends them to the external service. The latter, in its turn, identifies a message type (spam, valid mail, and so on) and sends the result back to the component. If the message type is selected in **Block message sending**, a server will refuse the SMTP transaction with the 5xx PERMFAIL reply code. For a sender, this means that a message could not be sent under any circumstances. If the sender is another mail server, it is discouraged from retrying to send the message. If the sender is a mail client (like Microsoft Outlook or Mozilla Thunderbird), the message will bounce back to it.

Additional Protection Settings

Outbound Antispam allows you not only to reject messages of a certain type, but to identify their senders by means of **Thresholds for blocking senders** that you can set for each message type. The system keeps statistics (available at the **Dashboard** tab) on unique senders who exceed these thresholds. Outbound Antispam counts all messages of the selected type within the *5 minute window*. If a counter value exceeds a threshold, your mail server refuses the SMTP transactions for all messages until the counter value does not become lower than the threshold again (this will mean that a sender stopped trying to send messages of that type). You can specify how the server should reject messages:

- **Delay sending.** In this case, the system will refuse SMTP transactions with the 4xx TEMPFAIL reply code. For the sending server this means that it could try to resend this message. For the users of mail clients (like Microsoft Outlook or Mozilla Thunderbird) this means that the message will stay unsent in their outbox.
- **Block sending.** In this case, the system will refuse SMTP transactions with the 5xx PERMFAIL reply code. As described above, this means that a message could not be sent under any circumstances.

Let us take a look at how the blocking thresholds work. For example, we set the threshold for blocking spam to 10 and some sender tries to send 3 spam messages per minute through our server. See the timeline below. On the 4th minute, the counter reaches 10 and Outbound Antispam starts to block all spam messages from the sender. Note that the 5 minute counting window has a 1 minute shift, thus on the 6-th minute, the counter's value will be equal to the sum of messages sent from 2-nd to 6-th minute, and so on. On the 8-th minute, the sender stops trying to send spam, but the counter's value still exceeds the threshold. Starting from the 10-th minute (when the counter's value is equal to 9), Outbound Antispam will begin to accept messages from the sender again.



Such temporary blocking can help you to identify compromised accounts and spammers who use them. If they are unable to send messages from a certain account, they will probably stop trying to use this account.

Note that temporary blocking does not override the **Block message sending** settings but supplements them. For example, if you choose to block spam in **Block message sending** and then set the threshold for blocking spam, all spam messages will be *always* blocked regardless of the message counter value. In this case, this threshold will just help you to identify who is permanently trying to send spam through your server.

Another benefit of using thresholds is that you can limit the overall messages sending rate (the **Total messages** parameter).

Allowing Certain Users to Send All Kinds of E-mail

If you are sure that a certain sender is not a spammer, you can make the system send their mail without scanning. To do this, add the identifiers of these senders to the *white list* or *bulk senders list*. These lists are located in **Tools & Settings > Outbound Spam Protection > White List** and **Tools & Settings > Outbound Spam Protection > Bulk Senders List** tabs respectively. The difference between the lists is in the following:

- Users from the white list can send any number of messages including messages considered as spam. Parallels Premium Outbound Antispam does not check messages from the senders in the white list.
- Users from the bulk senders list can send any number of *suspected spam* - mass e-mails that Parallels Premium Outbound Antispam does not consider spam. Spam and virus messages sent by senders from this list will be blocked.

For example, if you know that your customer sends mass non-spam e-mails such as newsletters, you should add their identifier to the bulk senders list to protect them from blocking by the Parallels Premium Outbound Antispam. However, note that if the system detects these newsletters as spam, it will block sending anyway.

Antivirus Software


To provide your e-mail users with anti-virus protection, you can use either the Parallels Premium Antivirus or Kaspersky Antivirus solutions. Both solutions can scan server's mail traffic in real time, however, only Kaspersky Antivirus allows fine tuning and filtering of specific file types from attachments.

The both programs require an additional license key with annual renewal. Check the current prices with your provider or visit Parallels site.

➤ **To install Parallels Premium Antivirus or Kaspersky Antivirus:**

1. Go to **Tools & Settings > Updates**. Updater will open in a new window or tab.
2. Click **Cancel updating**.
3. Click **Add Components**.

4. In the list of components, expand the **Additional mail services** group, and select either **Parallels Premium antivirus** or **Kaspersky antivirus extension**.
5. Click **Continue**.

After the installation is completed, obtain and install a license key for the selected antivirus program, as described in the following steps.
6. Go to **Tools & Settings > License Management**.
7. Click **Order New Key**. The Parallels online store page listing available add-ons opens in a new browser window.
8. On this page, select the checkbox next to **Parallels Premium Antivirus** or **Kaspersky Antivirus** and click **ADD TO MY BASKET**.
9. Because Parallels Plesk Panel add-ons are added to the license keys that already exist, you will need to specify the number of your license key to which you add this feature and click **Submit**.
10. In the next steps, indicate the currency, number of keys, provide contact details, billing address, and payment method, and submit the form. You will be notified by e-mail when your order is processed.
11. When you receive the e-mail notice, return to the **License Management** screen (**Tools & Settings > License Management**) and click  **Retrieve Keys** to retrieve the ordered license key. The Panel's License Manager will retrieve the upgraded license key from the Parallels licensing server and install it to your control panel.
12. Go to **Tools & Settings > Virus Protection Settings** (in the **Mail** group).

Under **Antivirus preferences**, select the antivirus you need and click **OK**.

If you installed Parallels Premium Antivirus, you can switch on antivirus protection only on a per-mailbox basis, and only after you have set up mailboxes. By default, virus definitions are retrieved every 5 hours, and this setting is not changeable through the control panel.

Webmail Software

You can install on the server a number of webmail software packages and select which of them should be available to your users. Alternately, you can redirect your users to an external webmail service. To do this, register an external webmail service address with the Panel by adding a corresponding record.

All installed webmail packages and registered external webmail services are listed in the mail settings of hosting plans and subscriptions (on the **Mail** tab). There you can select which webmail to provision to users.

Supported Webmail Software

By default, *Horde* and *RoundCube* webmails are installed on Parallels Plesk Panel for Linux, and only *Horde* is installed on Parallels Plesk Panel for Windows. Additionally, Panel for Linux supports *Atmail*, and Panel for Windows supports the following webmail clients:

- *MailEnable Web Client*
- *SmarterMail Web Client*
- *IceWarp (Merak) Mail Server Web Client*
- *Atmail Open*

Important: If you offer RoundCube to your customers, keep in mind that Panel backups do not include backups of the RoundCube database. This means that RoundCube data such as customers' calendars and contacts is not restored upon restoration of selected subscriptions or the entire server.

External Webmail Services

➤ **To register an external webmail service:**

1. Go to **Tools & Settings > Webmail** (in the **Mail** group).
2. Click **Register Webmail**.
3. Specify the following:
 - a. **Webmail service name**.
 - b. **Webmail service URL**. Specify an address that begins with the `http://` or `https://` prefix.
 - c. Leave the **Available** checkbox selected to make the registered webmail service available for selection in hosting plan settings.
4. Click **OK**.

➤ ***To change the properties of an external webmail record:***

1. Go to **Tools & Settings > Webmail** (in the **Mail** group).
2. Click the appropriate link in the **Name** column.
3. Make the required changes and click **OK**.

➤ ***To make a webmail service unavailable for inclusion into hosting plans:***

1. Go to **Tools & Settings > Webmail** (in the **Mail** group).
2. Do either of the following:
 - To make a service temporarily unavailable without actually removing it, select the corresponding checkbox and click **Disable**.
This works for installed webmail software packages and for links to external webmail services.
 - To permanently remove a service record, select the corresponding checkbox and click **Remove**.
This way you can remove only links to external webmail services. Installed software packages can be removed only by means of Parallels Products Installer (**Tools & Settings > Updates**).

Mailing Lists (Linux)

To provide your customers with capabilities to run their own mailing lists or newsletters, you should install the GNU Mailman package on your server (you could have done so during installation of Parallels Plesk Panel), and set up the mailing list administrator's account, otherwise, it will not work.

➤ ***To set up the mailing list administrator's account from your control panel:***

1. Go to **Tools & Settings > Set Up Mailing Lists Server** (in the **Resources** group).
2. Specify the username and password that you will use for administration of mailing lists and their settings.
3. Click **OK**.

Once you have set up the Mailman administrator's account, you can configure the mailing list software or change your administrative login and password by visiting the URL: <http://lists.yourservername.tld/mailman/admin/mailman>

Note: After you have set up Mailman administrator's account, the **Set Up Mailing Lists Server** icon will be no longer be accessible from the Panel.

Preventing Mass Email Sending (Linux)

➤ *To prevent your users from sending mass email, do the following:*

1. Create a file named `maxrcpt` in the directory `$QMAIL_ROOT_D/qmail/control/`

where `$QMAIL_ROOT_D` is the location defined in the file `/etc/psa/psa.conf` file.

2. Type the number of allowed recipients in this file and save it.

Note that this number also affect sending of messages to mailing list or mail group subscribers. That is, if you set the value to 100, then only 100 subscribers will receive the message sent to a mailing list or a mail group.

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


Mail Queue (Linux)

One of the possible reasons of problems with sending email is that the mail server is overloaded and cannot cope with the amount of received messages. This can happen when somebody is sending spam through your mail server, or the system process responsible for sending mail is down.

To see your mail server message queue, go to the **Tools & Settings > Mail Server Settings > Mail Queue** tab. Panel provides the following information about the queue:

- Total number of undelivered messages. When messages come to your mail server, they are first added to the main queue. Then, the mail server preprocesses them in order to find out whether they should be delivered to a local e-mail account on the same server or sent further to a remote recipient's e-mail address. After preprocessing, the messages directed at local mail recipients are put to a local queue, and the messages directed at remote recipients are put to a remote queue. Once delivered, the messages are removed from the queues.
- Message properties: subject, sender, recipient, queue type (local, remote, not preprocessed), date the message was sent from user's computer, the time elapsed since the moment when message was put to queue (age), and message size.

To return your mail server to an operable state, do any of the following:

- *Delete all messages from the mail queue* using the **Clear** button.
- *Delete only specific messages*. Find the messages with specific settings such as subject, sender, or recipient using the filter that opens when you click , select them, and click **Remove**,

Mass Email Notifications

When you need to inform your customers of scheduled server maintenance, or to introduce new service offerings, you can use the mass email function (**Tools & Settings > Mass Email Messages**) to send notices to all of your customers at once.

You may want to create message templates and use them when needed, or you can send messages without using any templates.

Read this section to learn how to:

- Create message templates for further use.
- Send email to multiple customers.

Next in this section:

Creating, Editing and Removing Message Templates	106
Sending E-mail Notices.....	108

Creating, Editing and Removing Message Templates

➤ *To create a new message template:*

1. Go to **Tools & Settings > Mass E-mail Messages** (in the **Tools** group), and click **Add Mass E-Mail Template**.

2. Specify template name in the **Template name** field.

3. Specify sender's name and e-mail address in the **From** field.

You can specify name, e-mail address or both. To specify both name and e-mail address, use the following format: `Name <your@e-mail.address>`. For example: `John Doe <admin@server.com>`.

4. Select the recipients for your e-mail message:

- If you want to send a message to resellers, select the **Resellers** checkbox and select the required group of recipients: **All** to send message to all resellers, **Selected only** to send message only to the resellers you select manually, **All except selected** to send message to all resellers except the ones you select manually.
- To select several resellers, click **Select Addresses** to the right of the **Resellers** checkbox (note that this button is not available if **All** mode is selected), select the required resellers in the **Available resellers** field and click **Add >>**. To remove resellers from the list of selected resellers, select the required resellers in the **Selected resellers** field and click **<< Remove**.
- If you want to send a message to customers, select the **Customers** checkbox and select the required group of recipients: **All** to send message to all customers, **Selected only** to send message only to the customers you select manually, **All except selected** to send message to all customers except the ones you select manually.
- To select several customers, click **Select Addresses** to the right of the **Customers** checkbox (note that this button is not available if **All** mode is selected), select the required customers in the **Available customers** field and click **Add >>**. To remove customers from the list of selected customers, select them in the **Selected customers** field and click **<< Remove**.
- You can see your choice of selected recipients at any time by clicking the respective **Show/Hide Selected** button.
- If you want a copy of the message to be sent to your mailbox, select the **Parallels Panel administrator** checkbox.

5. Specify the subject of your message in the **Subject** field.

6. Enter your message in the **Message text** field in plain text format. If you want the Panel to automatically insert the recipient names into your message, use `<name>` variable. The names will be taken from the information specified in the **Contact name** field.

7. Click **OK** to save the template.

➤ ***To edit a message template:***

1. Go to **Tools & Settings > Mass E-mail Messages** (in the **Tools** group), and click the required template in the list.
2. Make the required changes and click **OK**.

➤ ***To remove a message template:***

1. Go to **Tools & Settings > Mass E-mail Messages** (in the **Tools** group).
2. Select the checkbox corresponding to the message template you want to remove and click **Remove**.
3. Confirm the removal and click **OK**.

Sending E-mail Notices

➤ *To send an e-mail message to multiple customers at once:*

1. Go to **Tools & Settings > Mass E-mail Messages** (in the **Tools** group).
2. If you want to use a message template that you previously created (as described in **Creating, Editing and Removing Message Templates** (on page 106)), click the corresponding icon in the **Send** column. If you want to send a custom message, click **Send Mass E-Mail**.
3. To insert text from a template, select the template you need and click **Insert**.
4. Specify sender's name and e-mail address in the **From** field.

You can specify name, e-mail address or both. To specify both name and e-mail address, use the following format: `Name <your@e-mail.address>`. For example: `John Doe <admin@server.com>`.

5. Select the recipients for your e-mail message:
 - If you want to send a message to resellers, select the **Resellers** checkbox and select the required group of recipients: **All** to send message to all resellers, **Selected only** to send message only to the resellers you select manually, **All except selected** to send message to all resellers except the ones you select manually.
 - To select several resellers, click **Select Addresses** to the right of the **Resellers** checkbox (note that this button is not available if **All** mode is selected), select the required resellers in the **Available resellers** field and click **Add >>**. To remove resellers from the list of selected resellers, select the required resellers in the **Selected resellers** field and click **<< Remove**.
 - If you want to send a message to customers, select the **Customers** checkbox and select the required group of recipients: **All** to send message to all customers, **Selected only** to send message only to the customers you select manually, **All except selected** to send message to all customers except the ones you select manually.
 - To select several customers, click **Select Addresses** to the right of the **Customers** checkbox (note that this button is not available if **All** mode is selected), select the required customers in the **Available customers** field and click **Add >>**. To remove customers from the list of selected customers, select them in the **Selected customers** field and click **<< Remove**.
 - You can see your choice of selected recipients at any time by clicking the respective **Show/Hide Selected** button.
 - If you want a copy of the message to be sent to your mailbox, select the **Parallels Panel administrator** checkbox.
6. Specify the subject of your message in the **Subject** field.
7. Enter your message in the **Message text** field in plain text format. If you want Parallels Plesk Panel to automatically insert the recipient names into your message, use the `<name>` variable. The names will be taken from the information specified in the **Contact name** field.


8. If you want to save this message (both the text itself and information about its recipients) as a template for further use, select the checkbox to the left of **Save text to a new template named** field and specify the template name in this field.
9. Click **OK** to send the message. If you have chosen to save the message contents as a template, a template will be created and placed in the list of available templates.

Configuring Email Notifications

The Panel notifies you and your customers of disk space and bandwidth overage by sending e-mail notifications. In addition to resource overage, the control panel can notify the users when:

- New user accounts are created.
- New domains are added.
- Hosting accounts are expired (expiration date is defined for user accounts and websites separately).

➤ *To view or modify the notification system settings:*

1. Go to **Tools & Settings > Notifications** (in the **Logs & Notifications** group).
2. By selecting the checkboxes in the **Notifications** table, specify the types of control panel users or external e-mail users who should receive notices on events.
3. To view or edit the default notice text, click the respective  icon in the **Text** column.

In notices you can use tags that will be replaced with actual data (see the table below).

4. Specify when to send the user account and website expiration notices. By default, such notices are sent 10 days in advance. Click **OK**.

Tags Used in Notification Messages

Event type	Tags that can be used in notices	The data that tags denote
Creation of a reseller or customer account	<reseller_contact_name> <client_contact_name>	user's first and last name
	<reseller_login> <client_login>	user name for authorization in the Panel
	<password>	user's password for authorization in the Panel

	<reseller_company_name> <client_company_name>	company name
	<reseller_cr_date> <client_cr_date>	user account creation date
	<reseller_phone> <client_phone>	phone number
	<reseller_fax> <client_fax>	fax number
	<reseller_country> <client_country>	country
	<reseller_state_province> <client_state_province>	state or province
	<reseller_city> <client_city>	city
	<reseller_postal_ZIP_code> <client_postal_ZIP_code>	postal or ZIP code
	<reseller_address> <user_address>	address
	<reseller_id> <user_id>	unique identifier assigned by the system
	<hostname>	host name for access to the Panel
Addition of a new website to the server	<domain_name>	domain name
	<reseller_login> <client_login>	user name for authorization in the Panel
	<reseller_contact_name> <client_contact_name>	user's first and last name

	<dom_id>	unique identifier assigned by the system
	<ip>	IP address the website is hosted on
Subscription expiration notices	<domain_name>	subscription name
	<reseller_login> <client_login>	user name for authorization in the Panel
	<reseller_contact_name> <client_contact_name>	user's first and last name
	<dom_id>	unique identifier assigned by the system
	<domain_expiration_date>	subscription expiration date
	Resource overuse notices	<domain_name>
<reseller_login> <client_login>		user name for authorization in the Panel
<reseller_contact_name> <client_contact_name>		user's first and last name
<disk_usage>		information about disk space usage
<disk_space_limit>		information about the amount of disk space allocated to the account
<resource_table>		information about all resource limits that were or will soon be reached
<traffic>		information about bandwidth usage
<traffic_limit>		information about the bandwidth amount allotted to the account

Note: If you upgraded to Parallels Plesk Panel from an earlier version, then all custom notice templates you previously used remain in effect. Because of changes in user accounts hierarchy and addition of resource overuse scheme, now any type of resource can be overused. Therefore, to show information about all overused resources in notice templates, we recommend using a single variable <resource_table> instead of the variables <disk_usage>, <disk_space_limit>, <traffic>, and <traffic_limit>.

Database Servers

Parallels Plesk Panel needs database servers for storing its own databases, databases used by its components (for example, databases for the webmail service), and databases created by hosting customers' websites and APS applications (for example, a Wordpress database).

Parallels Plesk Panel supports the most popular database engines and is shipped with corresponding database management tools. Panel can work with database servers located on the same server with Panel or on a remote machine.

By default, on Linux servers, database engines are installed on the same server with Panel from the repository of your OS vendor (Linux) or your custom repository. On Windows servers, database engines are packaged with Panel and installed on the same server with Panel.

Database Server Software in Panel for Linux

Panel 11.5 for Linux supports MySQL and PostgreSQL database servers. Panel uses MySQL and PostgreSQL packages from the repository of your operating system. The exception is MySQL 5.5, which is packaged with Panel and supported on a limited number of operating systems.

MySQL is installed during Panel installation. You can additionally install PostgreSQL through **Tools & Settings > Updates and Upgrades > Add/Remove Components > PostgreSQL server support**.

You can also register external MySQL and PostgreSQL database servers in Panel. For details, see **Adding and Removing Database Servers** (on page 114). The list of supported database server versions is provided in **Release Notes**.

On CentOS 5, RHEL 5, and CloudLinux Panel installations, you can use MySQL 5.5. It is packaged with Panel and can be installed through **Updates and Upgrades > Add/Remove Components**.

Database Server Software in Panel for Windows

Panel 11.5 for Windows supports Microsoft SQL Server Express 2008 and 2012, and MySQL 5.1. By default, MySQL and Microsoft SQL Server 2008 are installed during Panel installation. You can additionally install Microsoft SQL Server 2012 through **Tools & Settings > Updates and Upgrades > Add/Remove Components**.

You can also register external Microsoft SQL Servers and MySQL servers in Panel. For details, see **Adding and Removing Database Servers** (on page 114).

To work with other database engines, Panel for Windows uses ODBC. For details, see **Connecting to External Databases (Windows)** (on page 120).

The list of supported database server versions is provided in **Release Notes**.

Note: For instructions on managing databases in Panel, refer to **Website Databases** (on page 542).

In this chapter:

Adding and Removing Database Servers	114
Configuring Backup Settings for Remote SQL Servers	116
Changing Database Administrator's Credentials.....	117
Database Hosting Preferences.....	118
Database Management Tools	119
Connecting to External Databases (Windows).....	120

Adding and Removing Database Servers

Adding External Database Servers to Panel

➤ **To use external database servers with your hosting server:**

1. Set up an external database server:
 - a. Install MySQL, PostgreSQL, or Microsoft SQL software.

For the supported versions, see **Release Notes** for Panel for Linux and **Release Notes** for Panel for Windows.
 - b. Set up the database administrator's account.
 - c. Enable network access to the database server.
2. Log in to Parallels Plesk Panel.
3. Go to **Tools & Settings > Database Servers**, and click **Add Database Server**.
4. Specify the properties of the database server:
 - Specify a database server engine in the **Database server type** box. The list contains database engines supported by your licence key. You can check what components are supported on the **Tools & Settings > Licence Management** page.

Note: To use Microsoft SQL Server with Panel, you need to obtain Parallels Plesk Panel Power Pack.

 - Note that before using a database server engine you should install it in **Tools & Settings > Updates and Upgrades > Add/Remove Components**, unless it was installed with Panel.
 - Specify the hostname or IP address of the database server.
 - Specify the port number the database server is listening on. This option is available only for MySQL. By default, MySQL servers listen on port 3306. You can leave the **Port number** box blank, if your MySQL database server is listening on the default port.

Note: Do not enter the value for MySQL server port equal to 8306, because it is used by Parallels Plesk Panel for communication with its internal database.

 - Specify which database type is running on the database server.
 - To make this database server default for hosting customers' databases, select the **Use this server as default for MySQL** checkbox. If you have a MS SQL database server, select the checkbox **Use this server as default for MS SQL**.
 - Specify the database server administrator's login name and password.
5. Click **OK**.

If you have registered a SQL Server, you may want to provide its backup settings. For configuring the backup settings of a remote SQL Server, refer to **Configuring Backup Settings for Remote SQL Servers** (on page 116).

Removing Database Servers from Panel

You can remove a database server only if it is not the default server and there are no databases on it.

➤ ***To unregister a database server from Panel:***

1. Go to **Tools & Settings > Database Servers**.
2. Select the checkbox to the right of the database server's host name.
3. Click **Remove**.
4. Confirm the operation and click **OK**.

➤ ***To unregister a database server that has databases or is assigned as default for hosting customers' databases:***

1. Delete databases from the database server:
 - a. Go to **Tools & Settings > Database Servers**.
 - b. Click the host name of the database server that you wish to unregister from Panel.
 - c. Select the checkbox in the upper left corner of the list to select all databases.
 - d. Click **Remove**.
 - e. Confirm removal and click **OK**.
2. Make another database server default:
 - a. Click the **Database servers** shortcut in the path bar at the top of the screen.
 - b. Click the host name of a database server that you wish to make default. This should be of the same database server type (MySQL or SQL Server) as the one you are going to delete.
 - c. Click **Preferences** and select the **Use this server as default for MySQL** checkbox. If you have a SQL Server, select the **Use this server as default for MS SQL** checkbox.
 - d. Click **OK**.
3. Return to the list of database servers (**Tools & Settings > Database Servers**).
4. Select a checkbox corresponding to the database server that you no longer need.

5. Click **Remove**.
6. Confirm the operation and click **OK**.

Important: You cannot remove databases used by web applications this way. To remove them, you should first remove the respective web applications from the sites that use them.

Configuring Backup Settings for Remote SQL Servers

If you want to back up databases hosted on a remote Microsoft SQL Server that you registered in Panel earlier, you need to configure the backup settings for that Microsoft SQL Server.

➤ ***To configure backup settings for a remote Microsoft SQL Server:***

1. Go to **Tools & Settings > Database Servers** and click the required remote SQL Server name.
2. Specify the temporary physical directory for the remote SQL Server in the **Temporary directory** field. For example, `C:\db_pleskbackup`.
This temporary physical directory is required for backing up and restoring remote SQL Server databases: SQL Server places temporary backup files in this directory during backup, and Panel places temporary backup files in this directory during restoration. You must create this directory on the remote server and make it accessible by the MS SQL server to read and write.
3. Share the physical directory created in the previous step and specify the network path to this directory in the **Temporary network directory** field. For example, `\\ServerName\db_pleskbackup`.
Panel server will use this directory to download and upload the temporary backup files. You must create the network directory on the remote server, mount it to a temporary physical directory created in the previous step, and make it accessible over network by the user created in the next step.
4. Create a user on the remote server (for example `ServerName\db_backup_user`) and give this user read/write access to the temporary network directory.
Panel server will use this user to access the temporary directory.
5. Specify the user name and password required for accessing the temporary network directory.
6. Click **OK**.

Changing Database Administrator's Credentials

To change the credentials with which Panel accesses a database server, you should first change these credentials on the database server and then update them in Panel. You cannot change the credentials through Panel. The exception is Panel for Windows, which allows you to change the database administrators' password.

Updating Database Administrator's Credentials in Panel

If you have changed the administrator's credentials on the database server, it is necessary to change them in Panel as well

Important: Updating the credentials through Panel does not change them on the database server.

➤ ***To update the database server administrator's credentials in Panel (Linux):***

1. Go to **Tools & Settings > Database Servers**.
2. Click the host name of a database server.
3. Provide the new username and password of the database server administrator.

➤ ***To update the database server administrator's credentials in Panel (Windows):***

1. Go to **Tools & Settings > Database Servers**.
2. Click the host name of a database server and then **Settings**.
3. Provide the new username and password of the database server administrator.

Changing Database Administrator's Password (Windows)

You can change the password of the user that is currently used by Panel to access the database server. When you change the password in the Panel UI, it will be changed on the database server automatically and updated in the database server settings in Panel.

➤ ***To change the database server administrator's password:***

1. Go to **Tools & Settings > Database Servers**.
2. Click the host name of a database server.
3. Click **Change Password**.
4. Enter the new password and click **OK**.

Database Hosting Preferences

These preferences include the naming of databases and database users.

➤ ***To set up naming preferences that will affect all databases created through Parallels Plesk Panel:***

In **Tools & Settings > Database Hosting Preferences** (in the **Applications & Databases** group) select any of the following options:

- **Add username and underscore to the beginning of database names.** Panel will add the Panel user name to corresponding database names. All names of newly created databases will look like `<panel_username>_<database name>`. This will make it convenient to locate databases related to a particular Panel user.

Note: If you select this option, users will not be able to remove the `<panel_username>_` prefix from the names of databases on creation of new databases. If you do not select this option, Panel will prompt users to add the `<panel_username>_` prefix to the database name, and users will be able to add it or remove it.

- **Add username and underscore to the beginning of database user names.** Panel will add the Panel user name to corresponding database users' names. All names of newly created database users will look like `<panel_username>_<database user name>`. This will make it easier to locate database users related to a particular Panel user. Existing database users will not be affected.

Database Management Tools


Database management tools provide a web interface for the administration of databases. The tools also allow running SQL queries from this user interface.

Panel is shipped with the following database management tools:

- *PHPMysqlAdmin* is used for MySQL databases.
- *phpPgAdmin* is used for PostgreSQL databases.
- *ASP.NET Enterprise Manager* and *myLittleAdmin* are used for Microsoft SQL Server - you can choose between them in **Tools & Settings > Server Components > Microsoft SQL Webadmin**.

Note that you need to install these tools first in **Tools & Settings > Updates and Upgrades > Add/Remove Components**.

➤ **To open a database management tool for a selected database server:**

1. Go to **Tools & Settings > Database Servers**.
2. Click the  icon corresponding to the database server you need to manage. One of the supported database management tools (depending on the database engine) will open in a separate browser window.

Alternatively, clicking the **Webadmin** icon (in the settings of a particular database server) opens the corresponding tool depending on the database engine.

Connecting to External Databases (Windows)

If you want your users to access the data from an external database management system, you should use Open Database Connectivity (ODBC) drivers. For example, you can install a Microsoft Access ODBC driver creating a connection to external Microsoft Access database, and customize web applications to use this database for storing their data.

Note that an external database does not necessarily need to be remote; ODBC can be used to access local databases as well.

➤ ***To install a new ODBC driver, creating a connection to an external database:***

1. Go to **Tools & Settings > ODBC Data Sources**.
2. Click **Add New ODBC DSN**.
3. Specify the ODBC connection name and description in the corresponding fields.
4. Select the required driver in the **Driver** field.
5. Click **OK**.
6. Choose the appropriate options on the driver configuration screen. Typically, you should specify the path to the database, user credentials and other connection options, depending on the selected driver.
7. Click **Test** to check whether the connection will function properly with provided settings. Click **Finish** to complete the creation.

➤ ***To change settings of an existing ODBC connection:***

1. Go to **Tools & Settings > ODBC Data Sources**.
2. Click the required connection name in the list.
3. Change the settings as needed.
4. Click **Test** to check whether the connection will function properly with new settings. Click **Finish** to save changes.

➤ ***To remove a redundant ODBC connection:***

1. Go to **Tools & Settings > ODBC Data Sources**.
2. Select a checkbox corresponding to the connection you want to remove.
3. Click **Remove**, confirm the removal and click **OK**.

Server Administration

This section describes the tasks related to server configuration and administration: IP pool, system time, firewall, and other. For the tasks related to Panel configuration and administration, see **Panel Administration** (on page 138).

In this chapter:

IP Pool	122
Scheduling Tasks	126
Server Settings.....	131
System Services	132
System Date and Time.....	134
Firewall.....	135

IP Pool

The *IP pool* is a set of available IP addresses that you can pass on to customers and resellers, or utilize them for your own websites. IP addresses may be designated as either *dedicated*, meaning that the target subscriber becomes the only owner of this address, or *shared*, meaning that this address is shared among many subscribers.

Next in this section we will describe the concepts of IP addresses and how they are allocated in Panel for web hosting purposes.

About IP Addresses

An IP address is a number that uniquely identifies each device, such as a computer, on a network. The use of IP addresses makes it possible for computers to find other computers on a network and communicate with them.

There are two formats of IP addresses:

- **IP version 4.** These 32-bit network addresses look like `192.168.1.1`. They are currently used by most network devices. The number of IPv4 addresses is limited and the last remaining portions of vacant IP addresses have already been allocated to Internet service providers.
- **IP version 6.** These 128-bit network addresses look like `2001:0db8:85a3:0000:0000:8a2e:0370:7334`. IPv6 is the new standard that was developed to address the exhaustion of IPv4 network addresses.

When Parallels Plesk Panel is deployed in IPv6-enabled networks, it can operate simultaneously on IPv4 and IPv6 addresses. Providers can add IPv4 and IPv6 addresses to the server IP pool, allocate them to resellers, and create subscriptions based on them.

Each hosting subscription can be allocated:

- One IPv4 address.
- One IPv6 address.
- One IPv4 + one IPv6 address (dual-stack subscriptions).

Note: Each subscription that needs to host FTP shares accessible by Internet users without password authorization (Anonymous FTP) must be assigned at least one dedicated IPv4 address.

Requirements for Operating on IPv6

The following requirements must be met to ensure the proper operation of Parallels Plesk Panel in IPv6-enabled networks:

- The Panel-managed server must be assigned at least one static IPv4 address. This is required for connections to the Panel licensing servers and application catalogs.
- When running in virtual environments, Parallels Virtuozzo Containers 4.6 or later must be used.

To see the list of Linux operating systems that support this feature, refer to the release notes to Panel, for Linux or for Windows.

Allocation to Resellers and Hosting Customers

The following is an overview of how IP addresses are allocated in Panel:

1. IP addresses are added to the server IP pool.

After installation, Panel reads all assigned IP addresses from the operating system configuration and adds them to the server IP pool. When you obtain new IP addresses that you would like to use on the server, you should add them through Panel to that pool, as Panel might not recognize manual modifications you make to the network configuration files.

Note: If you are running Panel in a Parallels Virtuozzo Container (PVC), you can add IP addresses only on the PVC hardware node.

When adding addresses to the server IP pool (in **Tools & Settings > IP Addresses > Add IP Address**), you select how they should be allocated - either as *dedicated* or *shared*:

- A dedicated IP address can be assigned to a single reseller. Dedicated IP addresses are required for hosting e-commerce sites with SSL encryption and sites that host FTP shares that are accessible without password authorization.

Note: The Server Name Indication (SNI) makes it possible to enable SSL protection for sites on shared IP addresses; however, this might not work for all hosting servers and users' browsers. For more information, see the section **SSL and Shared IP Addresses** (on page 150). On Windows platforms, it is also possible to protect a group of websites with one certificate. See the section **SSL and Shared IP Addresses (Windows)** (on page 150) for more details.

- A shared IP address can be literally shared among several reseller accounts and sites. Sharing of addresses helps to use scarce IPv4 address resources efficiently, but it should not be needed for IPv6 addresses.
2. When setting up reseller plans (in **Service Plans > Reseller Plans > Add New Plan > IP Addresses** tab), you select IP addresses that should be allocated to resellers:
 - For shared IP addresses, you can manually select which addresses should be allocated.
 - For dedicated IP addresses, you can only specify the number of addresses that should be allocated: When you create a new reseller account, a vacant dedicated IP address from the server pool is automatically selected by Panel and allocated to the reseller.

3. When signing up new customers (in **Customers > Add New Customer**) or creating subscriptions for your own needs (in **Subscriptions > Add New Subscription**), you can select IP addresses that should be allocated. All shared and dedicated addresses available from the server IP pool are listed in a menu.

About Using Panel with Dynamic IP Pools

Panel examines its IP pool during the web server start and removes IP addresses that do not exist in the system. This does not allow administrators to allocate non-existing IP addresses to services or subscriptions.

Managing the Server IP Pool

➤ *To view the IP addresses you have at your disposal:*

1. Go to **Tools & Settings > IP Addresses** (in the **Tools & Resources** group).

Your IP addresses are listed and the following supplementary information is given:

- The **IP address**, **Subnet Mask** and **Interface** columns show which IP addresses are on which network interfaces.
- The **Resellers** column shows the number of user accounts whom you assigned a given IP address. To view the users by names, click the respective number in the **Resellers** column.
- The **Sites** column shows a number of websites hosted on an IP address. To view the domain names of these websites, click the respective number in the **Sites** column.

2. To update the list of IP addresses and their status, click **Reread IP**.

You might need to do this if you manually added IP addresses to the network interface in the server operating system, or when operating in Parallels Virtuozzo Containers.

➤ *To add a new IP address to the server:*

1. Go to **Tools & Settings > IP Addresses** (in the **Tools & Resources** group), and click **Add IP Address**.
2. Select the network interface for the new IP from the **Interface** menu. All network cards installed on your server are shown in this menu.
3. Enter the IP address and subnet mask in the corresponding box. For example, `123.123.123.123/16` or `2002:7b7b:7b7b::1/64`.
4. Select the type of the new IP address, shared or dedicated.

5. From the drop-down box, select the default SSL certificate to use for the new IP address. You can select the following certificates:
 - **Default certificate** - the certificate that comes with the Parallels Plesk Panel distribution package. However, this certificate is not recognized by web browsers as it is not signed by a Certificate Authority (a warning message appears). The default certificate is used to provide access to the Panel via the https protocol (https://server-name-or-IP-address:8443/).
 - **Other certificates** - the certificates (self-signed or signed by a Certificate Authority) that you added to the repository of SSL certificates. About adding certificates, see **Customer's Guide**, section **Securing Connections with SSL Certificates**.
6. If your server is running Windows operating system, select the **FTP over SSL** checkbox if you want to enable the ability to use secure FTP connection (FTP over SSL) for the domain on a dedicated IP address.

Note: To enable secure FTP connections, the FTP server installed on your Parallels Plesk Panel server must support FTP over SSL. For example, Gene6, Serv-U FTP, IIS [FTP 7.x](#) servers support FTP over SSL.

7. Click **OK**.

➤ **To remove an IP address from the server:**

1. Go to **Tools & Settings > IP Addresses** (in the **Resources** group).
2. Select the respective checkbox and click **Remove**, confirm removal and click **OK**.

➤ **To assign an IP address to a reseller:**

1. Go to **Tools & Settings > IP Addresses** (in the **Resources** group), and click the corresponding number in the **Resellers** column, then click **Assign**.
2. Select the account you need and click **OK**.

➤ **To revoke an IP address from a reseller:**

1. Go to **Tools & Settings > IP Addresses** (in the **Resources** group), and click the corresponding number in the **Resellers** column.
2. Select the respective checkbox and click **Remove**.
3. Confirm removal and click **OK**.

Since users can refer to a web resource on your server by typing an IP address and there can be several websites hosted on that address, Panel needs to know which of the sites to show in such cases. Panel automatically assigns the first website created on an IP address as the default website; however, you can select any other website and make it default.

- ***To assign a default website (default domain) for an IP address:***
 1. Go to **Tools & Settings > IP Addresses** (in the **Resources** group), and click the IP address you need.
 2. In the **Default site** menu, select the site you need and click **OK**.

- ***To change an IP address allocation type (shared, dedicated) or assign another SSL certificate to an IP address:***
 1. Go to **Tools & Settings > IP Addresses** (in the **Resources** group), and click the IP address you need.
 2. Select the required IP address allocation type and SSL certificate, and click **OK**.

Scheduling Tasks

If you need to run scripts on your server at specific time, use the task scheduler facility on your server to make the system automatically run the scripts for you.

Next in this section:

Scheduling Tasks on Linux-based Servers.....	127
Scheduling Tasks on Windows-based Servers.....	129

Scheduling Tasks on Linux-based Servers

If you need to run scripts on your server at specific time, use the task scheduling facility on your server to make the system automatically run the scripts for you.

Important: To prohibit control panel users from scheduling tasks on behalf of user "root", create on the server's file system an empty file with name `root.crontab.lock` in the location `/parallels_panel_installation_directory/var/`.

During installation of Parallels Plesk Panel, the following tasks are automatically created:

- `autoreport.php` - delivers daily, weekly and monthly reports on clients and domains (three separate tasks)
- `backupmng` - initiates scheduled backing up of domains once every 30 minutes
- `statistics` - generates statistics on the limits imposed on domains, such as traffic, disk usage, and so on
- `mysqldump.sh` - creates a backup copy of three MySQL databases: `psadump`, `MySQL`, and `Horde` databases

Because all these tasks are related to domain statistics, databases and reports, it is strongly recommended that you neither change nor remove them.

➤ *To schedule a task:*

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Select the system user account on whose behalf the task will be executed.
3. Click **Schedule New Task**.
4. Specify when to run your command:
 - **Minute** - enter the value from 0 to 59
 - **Hour** - enter the value from 0 to 23
 - **Day of the Month** - enter the value from 1 to 31
 - **Month** - enter the value from 1 to 12, or select the month from a drop-down box
 - **Day of the Week** - enter the value from 0 to 6 (0 for Sunday), or select the day of the week from a drop-down box

You can schedule the time using the UNIX crontab entry format. In this format, you can

- enter several values separated by commas. Two numbers separated by a hyphen mean an inclusive range. For example, to run a task on the 4th, 5th, 6th, and 20th of a month, type `4-6,20`.
- insert an asterisk to specify all values allowed for this field. For example, to run a task daily, type `*` in the **Day of the Month** text box.

To schedule the task to run every Nth period, enter the combination */N, where N is the legal value for this field (minute, hour, day, month). For example, */15 in the **Minute** field schedules the task to start every 15 minutes.

You can type the contracted names of months and days of the week, which are the first three letters: Aug, Jul, Mon, Sat, etc. However, the contracted names cannot be separated with commas or used together with numbers.

5. Specify which command to run. Type it into the **Command** input box.

For example, if you want to run the backup creation task at the specified time and have the backup file sent to your e-mail, you need to specify the following command in the **Command** input box:

```
/usr/local/psa/admin/sbin/backupmng
```

6. Click **OK**.

➤ ***To temporarily suspend execution of a scheduled task:***

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Select the system user account on whose behalf the task is executed.
3. Locate the task that you want to suspend and click on the command name.
4. Clear the **Switched on** checkbox and click **OK**.

➤ ***To resume execution of a scheduled task:***

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Select the system user account on whose behalf the task is executed.
3. Locate the task whose execution you want to resume and click the command name.
4. Select the **Switched on** checkbox and click **OK**.

➤ ***To cancel a task:***

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Select the system user account on whose behalf the task is executed.
3. Select a checkbox to the left of the task that you want to cancel.
4. Click **Remove**.
5. Confirm removal and click **OK**.

Scheduling Tasks on Windows-based Servers

If you need to run scripts on your server at specific time, use the task scheduler facility on your server to make the system automatically run the scripts for you.

During installation of Parallels Plesk Panel, the following tasks are automatically created:

- Update Parallels Premium Antivirus database - updates antivirus database.
- Statistics calculation - generates statistics on resource usage, such as traffic and disk space.

Because these tasks are related to operation of system services, it is strongly recommended that you neither change nor remove them.

➤ *To schedule a task:*

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Click **Schedule New Task**.
3. Leave the **Switched on** checkbox selected if you want your scheduled task to be active immediately after the creation.
4. Type a name for your task in the **Description** field.
5. In **Scheduler notification**, specify whether the scheduler should notify you when it runs this task. The following options are available:
 - **Switched off** - do not notify you.
 - **Send to the default e-mail** - send the notification to your default e-mail address.
 - **Send to the e-mail I specify** - send the notification to the e-mail specified in the corresponding field. After selecting this option, you need to input the required e-mail in the field on the right.

Click **Set** to save scheduler notifications settings.
6. Specify which command to run. Type it into the **Path to executable file** input box. If you need to run the command with certain options, type them in the **Arguments** field.
 - For example, if you want to run the statistics calculation task to count disc space and see more detailed information for the example.com and example.net domains, you need to specify the following path in the **Path to executable file** input box:

```
C:\Program Files\Parallels\Parallels
Panel\admin\bin\statistics.exe
```

and the following options in the **Arguments** field:

```
--disk-usage --process-domains=example.com, example.net -
verbose
```

- If you want to run your own PHP script using the task scheduler, you need to specify the following path in the **Path to executable file** input box:

```
C:\Program Files (x86)\Parallels\Parallels  
Panel\Additional\PleskPHP5\php.exe
```

and specify the script location in the **Arguments** field:

```
C:\Inetpub\vhosts\mydomain.tld\httpdocs\myscript.php
```

7. Select the appropriate priority in the **Task priority** field. Task priority can be set to **Low**, **Normal** or **High**.
8. Specify when to run your command by selecting the appropriate checkboxes in the **Hours**, **Days of Month**, **Months** or **Days of Week** fields.
9. Click **OK** to schedule the task or click **Run Now** to schedule the task and immediately run it.

➤ ***To temporarily suspend execution of a scheduled task:***

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Choose a task that you wish to suspend and click on the command name.
3. Clear the **Switched on** checkbox.

➤ ***To resume execution of scheduled task:***

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Choose a task whose execution you wish to resume and click on the command name.
3. Select the **Switched on** checkbox.

➤ ***To cancel a task:***

1. Go to **Tools & Settings > Scheduled Tasks**.
2. Select a checkbox to the left of the task that you want to cancel.
3. Click **Remove**.
4. Confirm removal and click **OK**.

Server Settings

In this section, we will describe general Panel server settings. These settings include a set of parameters related to statistics, and miscellaneous options such as server-wide permissions for customers. You can edit the server settings on the **Tools & Settings > Server Settings** page.

Statistics Options

Panel lets you configure the following statistics options:

- **Retain web and traffic statistics for**
Here you set the period for which the server will store web statistics and traffic statistics gathered by Webalizer or AWstats programs. By default, Panel keeps the data for the last three months.
- **Include in the disk space usage calculation**
Here you select object types that Panel will consider when calculating disk space usage.
- **When calculating disk space usage, count**
This option lets you define how Panel will count the disk space used by each object: by its size or amount of used disk space. For information on how exactly Panel calculates disk space usage, see the section **About Disk Space Usage Calculation** (on page 262).
- **Include in the traffic calculation**
Here you select what types of traffic Panel will count when calculating traffic: inbound, outbound, or both of them.

Miscellaneous Options

In addition to the settings related to statistics, this screen lets you edit the following settings:

- **Full hostname.**
The host name of the Panel server.
- **Forbid users to create DNS subzones in other users' DNS superzones.**
When a customer creates a domain, they can specify not only the second-level domain names (like *example.com*) but also third- and lower levels of domain names, for example, *doc.example.com*. When a customer creates *doc.example.com* and the original domain name, *example.com*, was created by another customer, the system will not allow creating such a subdomain if the corresponding option is selected. We recommend that you select this checkbox, otherwise, users will be able to create fake subdomains and set up websites and e-mail accounts which could be used for spamming or even phishing or identity theft.

- **Forbid customers to change the name of their system user.**

When you add a subscription for a hosting customer, you specify a name of a system user associated with this subscription. On behalf of this user, the customer accesses the server over FTP or SSH, works with the file system, and so on.

By default, customers are allowed to change the names of system users associated with their subscriptions. Use this option to prevent customers from modifying these names.

Note: This option works only for customers who are not granted the **Hosting Management** permission. This permission enables customers to modify the name of the system user even if the option is selected.

- **Forbid customers to change the name of their main domain.**

The main domain of a subscription is created when you create the subscription. The name of the main domain is the same as the subscription name. By selecting this option, you can prohibit customers from modifying this name. Note that the Panel administrator and additional administrators are able to modify names of customers' subscriptions, even if this option is selected. By default, this option is not selected.

- *(Only for Windows)* **Include the user's password into the file with Web Deploy publication settings.**


Customers have the option to write code of their websites in WebMatrix® (the development tool) and publish the code directly to their customer accounts through a special protocol called Web Deploy. To set up a connection to their accounts, the customers should specify publishing settings in WebMatrix®. Panel helps such customers by generating the XML file their can provide instead of filling in all the settings. The customer account password along with any other settings is included into this XML file. If you wish to improve the security of your system and prevent stealing the passwords, you can exclude the password from the XML file. The customers then will have to enter the password directly in WebMatrix®. Read more about WebMatrix® in **Web Publishing with Web Deploy (Windows)** (see page 466).




Note: You can change this option programmatically. For details on how to do it, see <http://download1.parallels.com/Plesk/PP11/11.5/Doc/en-US/online/plesk-win-cli/60982.htm>

System Services


You can monitor, start, stop, restart and disable various services, and also change their startup type from the Panel (on Windows-based servers).

➤ **To see the status of a system service:**


1. Go to **Tools & Settings > Services Management**.
2. Click **Show All** to show all services from the service groups. To hide all services, click **Hide All**. The current state of a service or a group of services is marked by an icon:
 -  means that the service or all services in a group are running,

-  means that the service or all services in a group are stopped,
-  means that several services in a group are running and some are stopped,
-  means that the service is not installed or its management capabilities are not supported by the license key.
- In the **Startup Type** field you can see whether the service is started automatically or should be started manually.


➤ **To start a service:**

1. Go to **Tools & Settings > Services Management**.
2. Click the  icon corresponding to the service you wish to start.



➤ **To restart a service:**

1. Go to **Tools & Settings > Services Management**.
2. Click the  icon corresponding to the service you wish to restart.


➤ **To stop a service:**

1. Go to **Tools & Settings > Services Management**.
2. Click the  icon corresponding to the service you wish to stop.

➤ **To set service startup type (on Windows-based servers):**





1. Go to **Tools & Settings > Services Management**.
2. Select the checkbox corresponding to the required service in the list.
3. Select the required startup type:
 - Click  **Manual** to start selected services manually upon the Panel startup.
 - Click  **Auto** to start selected services automatically upon the Panel startup.



➤ **To disable a service:**

1. Go to **Tools & Settings > Services Management**.
2. Select the checkbox corresponding to the required service in the list.
3. Click  **Disable**.

➤ **To make changes to a group of services:**

1. Go to **Tools & Settings > Services Management**.
2. Select the checkboxes corresponding to the required services in the list.

3. Click the button corresponding to the action you want to perform on the selected services:
 - Click  **Start** to start selected services.
 - Click  **Stop** to stop selected services.
 - Click  **Restart** to restart selected services.
 - Click  **Disable** to disable selected services.

 - Click  **Manual** to start selected services manually upon the Panel startup.
 - Click  **Auto** to start selected services automatically upon the Panel startup.

System Date and Time

You can manually set the server date and time through the interface and enable server time synchronization with a Network Time Protocol (NTP) server.

➤ *To adjust the system date and time settings:*

1. Go to **Tools & Settings > System Time**.
2. Change the time and date settings as desired, and select your time zone.

You will need to restart your Parallels Plesk Panel-managed server for the time zone change to take effect.

Note for users of Parallels Panel for Windows: Clear the **Automatically adjust clock for daylight saving changes** checkbox, if you do not want Parallels Plesk Panel to automatically adjust the server clock.

3. To synchronize your server time with that of a server running the Network Time Protocol, select the **Synchronize system time** checkbox, and specify a valid IP address or a domain name. For a list of available NTP servers, visit <http://support.ntp.org/bin/view/Servers/WebSearch>
4. Click **OK**.

Note: Enabling the **Synchronize system time** function will override any time and date you manually enter in the **System date and time** fields. Also, make sure that the domain name or IP address you enter for synchronization is a valid NTP server. Otherwise, this function will not work and your server will continue running with its current time settings.

Firewall

Next in this section:

The Panel Firewall (Linux).....	135
The Panel Firewall (Windows).....	136

The Panel Firewall (Linux)

On Linux, you can use the **Panel Firewall** extension to protect your server and network from unauthorized access. Learn how to use the extension in the section **Firewall Extension** (on page 223).

For details about Panel extensions and how to install them, see **Panel Extensions (Linux)** (on page 203).

The Panel Firewall (Windows)

The firewall component allows you to protect a server from incoming network connections that could be used to compromise the server's security. The firewall comes with a set of predefined rules that allow connections to the services required for the proper functioning of a hosting server, such as web hosting, mail hosting, and FTP.

Turning the Firewall On and Off

In clean installations, the firewall is switched on. You can switch it off and on again at any time using the corresponding button on the **Tools & Settings > Firewall** page.

Viewing and Managing Allowed Inbound Connections

By default, the firewall blocks all inbound connections that are not explicitly allowed. To view the currently applied firewall rules for inbound connections, go to **Tools & Settings > Firewall > Firewall Rules** tab. On this tab, you can do the following:



- *Allow inbound connection to a service.*
If the service is not shown in the list of rules, click **Add Firewall Rule**, specify the rule name for future reference, then specify the port and the protocol for which incoming connections must be allowed. Leave the **Switch on the rule** checkbox selected if you wish to apply the rule immediately.
If the service is already in the list of rules, click the corresponding rule's name and select the **Switch on the rule** checkbox.
- *Temporarily block connections to a service* by clicking the corresponding rule's name and clearing the **Switch on the rule** checkbox.
- *Permanently block connections to a service* by selecting the corresponding rule and clicking **Remove**.
- *Restore the default firewall configuration* by clicking **Default**.
- *Close down all connections to the server.* If your server is compromised and websites are damaged, you may want to make the server unavailable over the Internet and keep it isolated until all vulnerabilities are patched and websites are restored from backup files. To close all connections to the server, click **Panic Mode**.

Allowing and Blocking ICMP Communications



ICMP communications are used for network troubleshooting purposes. By default, all ICMP communications are allowed. For a detailed description of ICMP messages, please refer to <http://msdn.microsoft.com/en-us/library/ms912869>.

➤ **To block or to allow ICMP communications:**

1. Go to **Tools & Settings > Firewall > ICMP Protocol**.

The predefined rules for ICMP communications are listed. The **S** (status) column shows the  icon if the firewall blocks the packets that match the rule, and the  icon if the firewall allows the packets that match the rule to pass through.

2. Do any of the following:

- To allow ICMP requests of a specific type, click the respective  icon in the **S** column.
- To block ICMP requests of a specific type, click the respective  icon in the **S** column.
- To block all ICMP requests, click **Panic Mode**.
- To restore the default settings for ICMP requests, click **Default**.

Panel Administration

In this chapter:

Panel Licensing	139
Securing Panel.....	142
Panel and Network Environments	151
Setting Up Help Desk	155
Trial (Try and Buy) Mode for Presence Builder	157
Changing Your Password and Contact Information	168
Appearance and Branding.....	170
Panel Components.....	176
Web Applications	177
Session Preferences	187
Managing Panel from Mobile Devices	188
Panel Inside Parallels Virtuozzo Containers	192
Remote Access (Windows)	194
Additional Administrator Accounts	195
Event Tracking	198
Migration from Other Hosting Platforms.....	202
Data Transfer from Another Panel.....	202
Panel Extensions (Linux).....	203

Panel Licensing

Panel comes with a trial license key, which is already installed in the system. This license key provides limited functionality and is active only for a short period of time. Therefore, after installing Panel, you should obtain a proper license key from Parallels or its partners and install it.

Panel License Keys

You can install a Panel license key either by entering an *activation code* or by uploading a *license key file* to Panel. Learn how to do this in the section **Installing a Panel License Key** (on page 140).

Panel license keys have a built-in expiration date. This has been implemented to help prevent fraud and theft. It requires the Panel software to check with the Parallels licensing server within a 10-day period before the expiration date to verify that the key has not been reported stolen and is being used in accordance with the End User License Agreement (that is, installed on only one server). Once this is verified, the expiration date is extended. The verification runs automatically and you do not need to do anything unless there is a problem. If the key has expired, go to **Tools & Settings > License Management** and click **Retrieve Keys**. If the key cannot be updated, contact your reseller, or Parallels (if you purchased the license key directly from Parallels).

Note: Panel uses the TCP port 5224 for connections to the licensing server. Please make sure that the port is not blocked by a firewall. To test the connection to the licensing server at anytime, click **Retrieve Keys** in **Tools & Settings > License Management**.

Additional License Keys

Additional license keys are used to activate third-party software in Panel:

- *Additional Panel components.*
Typically, these components are commercial Panel extensions such as anti-virus software, webmail software, and so on. Additional keys are associated with the Panel license key and can be found in **Tools & Settings > License Management > Additional License Keys**. Learn how to order add-ons and install additional license keys in the section **Installing Additional License Keys for Panel Add-ons** (on page 141).
- *APS web apps.*
Since Panel 11.0, it has been possible to purchase a Panel license key that comes in a bundle with APS app licenses. For example, you can purchase a bundle that contains a Panel license key and a key for a commercial online store app. Technically, this means that once a user installs the app on their site, it will be automatically activated without the need to purchase the app license from the vendor.

Note: If you are a hosting provider, you can allow your customers and resellers to use bundled app license keys. To do this, grant them permission using the **Allow activating APS apps using license keys from the Panel license pool** option on the **Permissions** tab of the relevant service plan or subscription. Note that you cannot limit the number of app installations a customer is allowed to perform. Thus, a customer can install a commercial app twice or more times on his websites without being charged for additional installations.

Licenses for APS apps are provided as additional license keys to Panel and can be found in **Tools & Settings > License Management > Additional License Keys**.

Next in this section:

Installing a Panel License Key.....	140
Installing Additional License Keys for Panel Add-ons	141
Upgrading Your License Key	142
Rolling Back to Your Previously Used License Key	142

Installing a Panel License Key

Right after the installation, Panel uses a trial license key. To get a new license key, proceed to the Parallels online store (**Tools & Settings > License Management > Order New Key**).

Once you purchase the key, you will receive an activation e-mail with your activation code and a license key file. You can install a Panel license key either by entering the activation code or by uploading the file from this e-mail.

➤ *To install a license key using an activation code:*

1. Go to **Tools & Settings > License Management > Parallels Panel License Key** and click **Install Key**.
2. Enter the code you received in the e-mail to the **Enter an activation code** field and click **OK**.

➤ *To install a license key using a license key file:*

1. Go to **Tools & Settings > License Management > Parallels Panel License Key** and click **Install Key**.
2. Choose **Upload a license key file**.
3. Specify the path to the key file you received in the e-mail and click **OK**.

Installing Additional License Keys for Panel Add-ons

Typically, Panel add-ons (like Panel extensions, web apps, and so on) are associated with a Panel license key. That is why, when you purchase Panel add-ons at the Parallels online store, you are prompted to enter the number of your license key. Once you purchase a key, you will receive an activation e-mail.

➤ ***To install an add-on license key:***

1. Go to **Tools & Settings > License Management > Additional License Keys** and click **Retrieve Keys**.
2. The Panel's License Manager will retrieve the upgraded license key from the Parallels licensing server and automatically install it to your Panel.

If your activation e-mail contains an activation code or a license key file, you should install the key manually.

➤ ***To install an add-on license key using an activation code:***

1. Go to **Tools & Settings > License Management > Additional License Keys** and click **Install Key**.
2. Enter the code you received in the e-mail to the **Enter an activation code** field and click **OK**.

➤ ***To install an add-on license key using a license key file:***

1. Go to **Tools & Settings > License Management > Additional License Keys** and click **Install Key**.
2. Choose **Upload a license key file**.
3. Specify the path to the key file you received in the e-mail and click **OK**.

Upgrading Your License Key

If you are planning to expand your customer base and host more sites on the server than your current license allows, you need to upgrade your license key. All upgrades are applied to your main Panel license key. Once you purchase upgrades at the Parallels online store, you will receive an activation e-mail.

➤ ***To upgrade the license key:***

1. Go to **Tools & Settings > License Management > Parallels Panel License Key** and click **Order Panel Upgrades**.
2. Order desired upgrade options. Once your order is processed, you will receive a notification e-mail.
3. Go to **Tools & Settings > License Management > Parallels Panel License Key** and click **Retrieve Keys**.
4. The Panel's License Manager will retrieve the upgraded license key from the Parallels licensing server and automatically install it to your Panel.

Rolling Back to Your Previously Used License Key

➤ ***To roll back to the license key you previously used:***

1. Go to **Tools & Settings > License Management > Parallels Panel License Key**.
2. Click **Roll Back Key**. The previously installed license key will be restored.

Securing Panel

Next in this section:

Restricting Administrative Access.....	143
Restricting Remote Access via API RPC.....	144
Setting Up the Minimum Password Strength	144
Turning On the Enhanced Security Mode	145
Using Secure FTP.....	146
SSL Protection	146

Restricting Administrative Access

To alleviate security concerns, you may want to restrict administrative access to your control panel from specific IP addresses.

- ***To allow administrative access to the Panel only from specific IP addresses or networks:***
 1. Go to **Tools & Settings > Restrict Administrative Access** (in the **Security** group).
 2. Click **Add New Network** and specify the required IP addresses. Click **OK**.
To specify subnets, you can use wildcard symbols (*) and subnet masks.
 3. Select the **Denied from the networks that are not listed** option, and click **Set**.
When prompted to confirm the operation, click **OK**.

- ***To prohibit administrative access from specific IP addresses or networks:***
 1. Go to **Tools & Settings > Restrict Administrative Access** (in the **Security** group).
 2. Click **Add New Network** and specify an IP address. Click **OK**.
To specify subnets, you can use wildcard symbols (*) and subnet masks.
 3. Select the **Allowed, excluding the networks in the list** option, and click **Set**.
When prompted to confirm the operation, click **OK**.

Restricting Remote Access via API RPC

For integration purposes, Panel has the API called *API RPC* that lets third party-software interact with Panel. This interface allows Panel operations, for example, creating customer accounts or subscriptions, to be called remotely. At the same time, the remote API can be used for malicious purposes. For example, an attacker can try to use the API to gain control over your server.

To improve Panel protection from attacks that use the remote interface, you can prohibit connections through API RPC completely, or allow them only for a limited number of IP addresses that you trust.

➤ *To restrict access to Panel via API RPC:*

1. Open for editing the configuration file `panel.ini` located in the following directory:

- On Linux: `/usr/local/psa/admin/conf`
- On Windows: `%plesk_dir%\admin\conf\`

If the file does not exist, create it.

2. Add the following lines to the file:

- To prohibit all connections:

```
[api]
enabled = off
```

- To allow connections only from specific IP addresses:

```
[api]
allowedIPAddresses = <IP_addresses>
```

<IP_addresses> here is a comma-separated list of IP addresses from which software can connect to Panel via API RPC.

Setting Up the Minimum Password Strength

In order to improve Panel security, you can set the minimum password strength (in **Tools & Settings > Password Security > Password strength**) for all passwords in the system. Password strength is a measure of how resistant a password is to various types of attacks. Generally, the strength of a password depends on its complexity and overall length.

When any Panel user (the administrator, a customer, reseller, or auxiliary user) sets a new password in Panel (for example, creates a new mail account or changes the password of an FTP user), they are required to adjust the password until it meets the minimum password strength. Note that if you increase the minimum strength, already existing passwords will not be affected by the new requirements.

We recommend that you force your users to employ stronger passwords. However, note that such passwords are harder to remember.

Panel distinguishes five levels of password strength which allow you to get the right balance between required protection and password complexity: **Very weak**, **Weak**, **Medium**, **Strong**, and **Very strong**.

Turning On the Enhanced Security Mode

The enhanced security mode introduces advanced protection of sensitive data in Panel. In this mode, Panel employs multiple security mechanisms to protect the data from unauthorized access. In order to improve Panel security, we recommend that you turn the mode on.

This security measure is absolutely transparent to all Panel users: Turning the mode on does not imply any significant changes in the Panel behavior. The only consequences you should be warned about are the following:

- *Remote API compatibility.*
Once you turn on the mode, it will be impossible to obtain sensitive data (for example, user passwords) using the Panel's remote API. This may affect third-party apps or your custom scripts that use corresponding API RPC functions. Therefore, if you (or your customers) employ such apps, contact the corresponding vendors to ensure they provide the full support for Panel 11.
- *Password reminders behavior.*
A password will no longer be sent by e-mail in case a user forgets it. Instead, the e-mail will contain a link to a page where the user will be able to change the password.

Turning On the Mode

If you have a clean installation of Panel 11, the enhanced security mode is turned on by default.

If you upgraded to Panel 11 from earlier versions, you can turn on the mode in **Tools & Settings > Security Policy**. Note that this is an irrevocable operation.

Note: If you use Parallels Business Automation Standard (PBAs) as an accompanying billing solution, the enhanced security mode should be turned on.

Using Secure FTP

To secure FTP connections to your server, <pp_name> supports the *FTP Secure* (FTPS, FTP-SSL) protocol. Unlike the traditional (plain) FTP, FTPS supposes protecting data transferred to and from your server over FTP with SSL and TLS protocols.

As a Panel administrator, you have the option to select allowed types of FTP connections: secure, plain, or both of them on the **Tools & Settings > Security Policy > Secure FTP** page.

We recommend that you allow only FTPS connections. This option secures data and access credentials transferred between the server and clients. Moreover, if you need to comply with the PCI DSS standard, selecting this option is required.

Though most of modern FTP client applications support FTPS, some of your customers may use clients that are able to work only through plain FTP. To let such clients connect to your server, allow both FTP and FTPS connections.

Next in this section:

Defining FTPS Usage Policy per IP Address (Windows) 146

Defining FTPS Usage Policy per IP Address (Windows)

In Panel for Windows, there is an option to select the FTPS usage policy separately for each IP address. This means that you, for example, can prohibit non-secure FTP connections for certain IP addresses and allow them for other ones.

➤ *To define FTPS usage policy per IP address:*

1. Go to **Tools & Settings > Security Policy**.
2. Select the **Use custom FTPS policy per IP address** option for the **FTPS usage policy**.
3. Go to **Tools & Settings > IP Addresses**.
4. For each IP address, click its name and select the desired option for the **FTPS usage policy** parameter.

SSL Protection

Next in this section:

Getting SSL Certificates 147
 SSL and Shared IP Addresses 150
 Shared SSL Certificates (Windows) 150

Getting SSL Certificates

For security reasons, you can access your control panel only through a secure connection provided by Secure Sockets Layer-enabled hypertext transfer protocol. All data you exchange with the Parallels Plesk Panel-managed server are encrypted, thus preventing interception of sensitive information. The SSL certificate used in the data encryption process is automatically generated and installed on the server during installation of the control panel. This is the so-called self-signed certificate: it is not signed by a recognized certification authority (CA), therefore, upon attempt to connect to your control panel, you and your customers will see warning messages in web browsers.

To gain customer confidence, you should purchase an SSL certificate from a reputable certification authority, and install it to the control panel.

You can either:

- use the functions for purchasing SSL certificates from Comodo, GeoTrust, Inc. or GoDaddy provided by your control panel,
OR
- create a certificate signing request (CSR) from the control panel and submit it to the certification authority of your choice, which will create an SSL certificate for you.

Note: If you are going to use the control panel's facilities for purchasing a certificate through MyPlesk.com online store, you should not use command line tools for creating the certificate signing request.


➤ ***To purchase an SSL certificate from Comodo, GeoTrust, Inc. or GoDaddy through MyPleskCom online store and secure your control panel:***

1. Go to **Tools & Settings > SSL Certificates** (in the **Resources** group). A list of SSL certificates that you have in your repository will be displayed.
2. Click **Add SSL Certificate**.
3. Specify the certificate properties:
 - Certificate name. This will help you identify this certificate in the repository.
 - Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.
 - Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.
 - Specify the host name for which you wish to purchase an SSL certificate. For example: your-domain.com
 - Enter your e-mail address.
4. Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.
5. Click **Buy SSL Certificate**.

Your private key and certificate signing request will be generated. Do not delete them. MyPlesk.com login page will open in a new browser window.

6. Register or log in to an existing MyPlesk.com account and you will be taken step by step through the certificate purchase procedure.
7. Choose the type of certificate that you wish to purchase.
8. Click **Proceed to Buy** and order the certificate. In the Approver E-Mail drop-down box, please select the correct Approver e-mail.
The approver e-mail is an e-mail address that can confirm that certificate for specific domain name was requested by an authorized person.
9. Once your certificate request is processed, you will be sent a confirmation e-mail. After you confirm, the certificate will be sent to your e-mail.
10. When you receive your SSL certificate, save it on your local machine or network.
11. Return to the SSL Certificates repository (**Tools & Settings > SSL Certificates**).

Click **Browse** in the middle of the page and navigate to the location of the saved certificate. Select it, and then click **Send File**. This will upload the certificate to the repository.


1. Select the checkbox corresponding to the certificate you just added, and click  **Secure the Panel**.

➤ ***To secure your control panel with an SSL certificate from other certificate authorities:***

1. Go to **Tools & Settings > SSL Certificates** (in the **Resources** group). A list of SSL certificates that you have in your repository will be displayed.
2. Click **Add SSL Certificate**.
3. Specify the certificate properties:
 - Certificate name. This will help you identify this certificate in the repository.
 - Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.
 - Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.
 - Specify the host name for which you wish to purchase an SSL certificate. For example: your-domain.com
 - Enter your e-mail address.
4. Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.
5. Click **Request**. Your private key and certificate signing request will be generated and stored in the repository.

6. In the list of certificates, click the name of the certificate you need. A page showing the certificate properties opens.
7. Locate the **CSR** section on the page, and copy the text that starts with the line **-----BEGIN CERTIFICATE REQUEST-----** and ends with the line **-----END CERTIFICATE REQUEST-----** to the clipboard.
8. Visit the website of the certification authority from which you want to purchase an SSL certificate, and follow the links on their site to start a certificate ordering procedure. When you are prompted to specify CSR text, paste the data from the clipboard into the online form and click **Continue**. The certification authority will create an SSL certificate in accordance with the information you supplied.
9. When you receive your SSL certificate, save it on your local machine or network.
10. Return to the SSL Certificates repository (**Tools & Settings > SSL Certificates**).

Click **Browse** in the middle of the page and navigate to the location of the saved certificate. Select it, and then click **Send File**. This will upload the certificate to the repository.

1. Select the checkbox corresponding to the certificate you just added, and click  **Secure the Panel**.

➤ ***In case you need to generate a self-signed certificate, follow this procedure:***

1. Go to **Tools & Settings > SSL Certificates** (in the **Resources** group). A list of SSL certificates that you have in your repository will be displayed.
2. Click **Add SSL Certificate**.
3. Specify the certificate properties:
 - Certificate name. This will help you identify this certificate in the repository.
 - Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.
 - Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.
 - Specify the host name for which you wish to purchase an SSL certificate. For example: your-domain.com
 - Enter your e-mail address.
4. Click the **Self-Signed** button. Your certificate will be generated and stored in the repository.

SSL and Shared IP Addresses

Parallels Plesk Panel supports the Server Name Indication (SNI) extension to the Transport Layer Security protocol, which makes it possible to use authentic SSL certificates for sites hosted on shared IP addresses.

SNI helps to efficiently use IPv4 resources and provides the following benefits:

- Providers can run any number of SSL sites with independent certificates on a single IPv4 address.
- Hosting customers can install independent SSL certificates on each of their sites; therefore, there is no need to purchase another subscription. Each customer can install an SSL certificate even if there is only one shared IP address on the whole server.

The SSL support with SNI is possible only if the following requirements are met:

- *The operating system of your Panel server supports SNI.*
 - Linux systems (see the full list in the release notes).
 - Windows 2012.
- *Users' browsers support SNI.*

Most modern web browsers, starting with IE 7, Firefox 2.0, Opera 8.0, and Chrome 1.0, support SNI, unless they are run on Windows XP. To learn more about SNI and the client software that supports it, refer to http://en.wikipedia.org/wiki/Server_Name_Indication.

If SNI is not supported and you (as the administrator) assign an SSL certificate to a site hosted on a shared IP address, Panel will associate that certificate with all other sites hosted on this IP address. In the same case, hosting customers with shared IP addresses will not be able to assign SSL certificates to their sites: the page **Websites & Domains** > <domain_name> > **Secure Your Sites** will be hidden in their Control Panel.

For instructions on assigning SSL certificates to websites, refer to the section **Securing Connections with SSL Certificates** (on page 430).

Turning On Support for SNI

By default, in clean Panel installations (Linux and Windows), the support for SNI is turned on.

If you upgrade Panel for Windows from version 11.0 or earlier, the support for SNI will be switched off. You can turn it on in **Tools & Settings** > **Server Settings**.

On Panel for Linux, the support for SNI is always on and cannot be disabled.

Shared SSL Certificates (Windows)

On Windows-based installations, you can secure access to a site with SSL for site owners without having them purchase their own SSL certificate. Websites that employ shared SSL are, in fact, using the certificate shared by another domain. The domain that shares its SSL certificate with others is called *master SSL domain*.

You can pick any website that belongs to you, switch on SSL support in web hosting settings, install a valid SSL certificate on that site, and make it act as a master SSL domain for all other websites hosted on the server. Or you can pick a website that belongs to one of your users (reseller or customer account), switch on SSL support in web hosting settings, install a valid SSL certificate on that site, and make it act as a master SSL domain for all websites of this user.

Once the master SSL domain is assigned, you or your customers need to add shared SSL links for each website that needs secure access.

➤ ***To configure the master SSL domain and enable shared SSL on your server:***

1. Go to **Tools & Settings > Shared SSL** (in the **Resources** group).
2. Select the **Switch on shared SSL** checkbox.
3. Select the required website from the **Domain name** menu. Only websites that are hosted on your server and have SSL enabled are present in the list.
4. Click **OK**.

For information about adding shared SSL links for websites, refer to **Customer's Guide**, section **Using Shared SSL Certificate (Windows)**.

➤ ***To disable shared SSL on your server:***

1. Go to **Tools & Settings > Shared SSL** (in the **Resources** group).
2. Clear the **Switch on shared SSL** checkbox.
3. Click **OK**.

Panel and Network Environments

Next in this section:

Ports Used by Panel.....	152
Running Panel Behind a Router with NAT	153
Configuring Port Range for Passive FTP Mode (Windows)	153

Ports Used by Panel

This section provides information about setting up the firewall built into your panel so as to allow access to Panel and its services.

The following is a list of ports and protocols used by Parallels Plesk Panel services.

Service name	Ports used by service
Administrative interface of Panel over HTTPS	TCP 8443
Administrative interface of Panel over HTTP	TCP 8880 *
Samba (file sharing on Windows networks)	UDP 137, UDP 138, TCP 139, TCP 445
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.

Running Panel Behind a Router with NAT

Every time you set up a new website in Panel, the domain name used by your website is associated with the IP address of your Panel-managed server in the DNS zone of this domain. If you are running the Panel behind a routing device with NAT (network address translation), this IP address will be an internal network address like 192.168.1.10. The website will not be accessible to the Internet users. To work around this, you have to associate this domain name with the public IP address of the routing device in the DNS zone of this domain. This is done by adjusting the Panel DNS template.

➤ ***To move your Panel server behind a router with NAT:***

1. Configure your routing device so as to ensure the proper address translation. Refer to the documentation of your routing device for detailed instructions.
2. Log in to the Panel and go to **Tools & Settings > DNS Template** (in the **General Settings** group).
3. Locate all resource records of A type. These records look like the following:
 - <domain>. A <ip>
 - mail.<domain>. A <ip>
 - ns.<domain>. A <ip>
 - webmail.<domain>. A <ip>
4. Edit all of these A type records:
 - a. Click the corresponding links in the **Host** column.
 - b. In the **Enter IP address** input box, delete the <ip> templates, and type the public IP address of the routing device.
 - c. Click **OK**.
5. Apply DNS template changes to all domains in the system by clicking **Apply DNS Template Changes**.

After this, all existing and newly created domains will get proper DNS configuration: Their A DNS records will point to the public IP address.

Configuring Port Range for Passive FTP Mode (Windows)

- *To set a specific port or port range for connecting to the server over FTP in passive mode:*
 1. Go to **Tools & Settings > FTP Settings**.
 2. Specify the required port or port range in the **Port or port range for passive FTP mode connections** field and click **OK**.

Setting Up Help Desk

To allow your customers to submit problem reports through Control Panel, you can do the following:

1. Set up a subscription for hosting your corporate website.
2. Install on your site the application osTicket 1.6 or later from Application Catalog. Among available free solutions, osTicket is considered the best for its ease of use and feature set. For information about osTicket, visit their website at <http://osticket.com>.

➤ ***To set up a subscription for hosting your own website:***

1. In Server Administration Panel, click the **Subscriptions** link in the navigation pane, under the **Hosting Services** group.
2. Click **Add New Subscription**.
3. Type the domain name of your corporate site, for example `provider-example.com`.
4. Select IP address.
5. Type the username and password that you will use for connecting to the web space over FTP and managing files.
6. In the **Service plan** menu, select **Unlimited** to allow your site to consume unlimited amounts of resources.
7. Click **OK**.

Next time you log in to Server Administration Panel, the **Install Help Desk** link will appear in the navigation pane. You can use it to install osTicket on your website.

➤ ***If you want to start installation immediately, without logging out and then logging in again:***

1. Click the link **Control Panel** next to your site's domain name. Control Panel will open in a new browser window or tab.
2. On the **Home** tab, click the **osTicket** link in the **Applications** group.
3. Click **Install**.
4. Read the terms of license agreement, confirm that you accept them, and click **Next**.

5. To open all application settings, click the link **Show All Settings** and specify the following:

- Path to the installation directory on the server.
- Administrative access to the application. Leave the **Grant administrative access to existing user** option selected, and select **Admin** from the menu if you want to use your site's FTP account username and password for managing Help Desk.
- Administrator's e-mail. Specify the Help Desk administrator's e-mail address.
- Website name. For example, Company Name customer service portal.
- Default system e-mail. Specify an e-mail address that you will advertise on your site as a means to contact your support engineers. For example, support@example.com.
- Database administrator's password.

6. Click Install.

Once installation is finished, you will be able to use the **Help Desk** link in the navigation pane of Server Administration Panel for configuring Help Desk and processing tickets submitted by your customers and customers of your resellers.

The customers will be able to submit tickets by clicking the link **Help Desk** in their Control Panels, in the **Custom Buttons** group.

Trial (Try and Buy) Mode for Presence Builder

If you have Parallels Panel with Presence Builder and Business Manager, you can tune your system to offer Presence Builder in the *Try and Buy* (or *trial*) mode. This mode lets everyone evaluate the editor and create websites for free. However, to acquire such websites, a site owner will need to subscribe to your hosting plan or purchase a plan add-on.

Note: If you use some other billing solution instead of Business Manager, you can use the Try and Buy mode as well. Learn more in the section **Offering the Try and Buy with Alternative Billing Solutions** (on page 165).

How the Try and Buy Mode Works

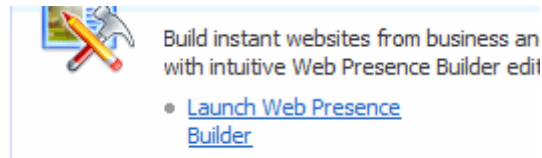
The Try and Buy mode is aimed at customers who wish to create their own sites but have little or no programming skill. Panel helps such customers by giving them full access to Presence Builder functions to create sites at no charge. To claim the created sites the customers subscribe to a hosting plan in Panel or upgrade the existing one. The more people you attract by this promotion, the more hosting subscriptions with Presence Builder you will have.

The Try and Buy mode targets two different groups:

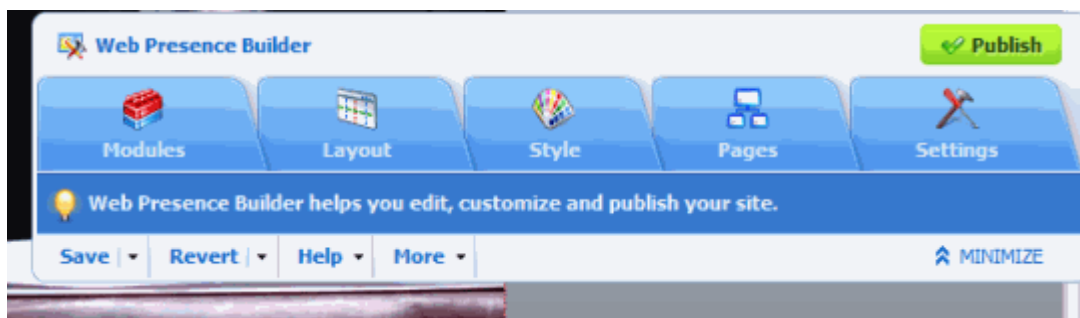
- Existing customers who want to have a website but are unable to launch Presence Builder due to various limitations. For example, their hosting plan does not provide this option, or they have exceeded the number of sites to publish. By using the Try and Buy, you can upsell Presence Builder to these customers. Learn more in the section **Configuring the Try and Buy for Existing Customers** (on page 160).
- New customers who have created a trial site and now want to claim it with a new hosting plan. Learn how to configure the Try and Buy mode for such customers in the section **Configuring the Try and Buy for Potential Customers** (on page 161).

➤ **The scenario for upselling to existing customers works this way:**

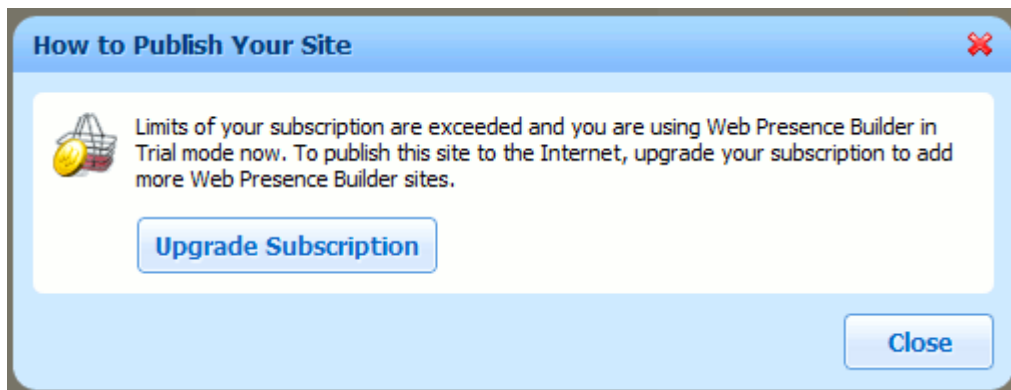
1. Links to launch Presence Builder become available to such customers on a number of pages in Control Panel. The customers see the links and click them.



2. Panel forwards these customers to Presence Builder where they create trial sites.



3. When the site is ready and the customers click Publish, they are prompted to upgrade their subscription.



- If the upgrade is successfully completed, the site can be published to the upgraded hosting account.

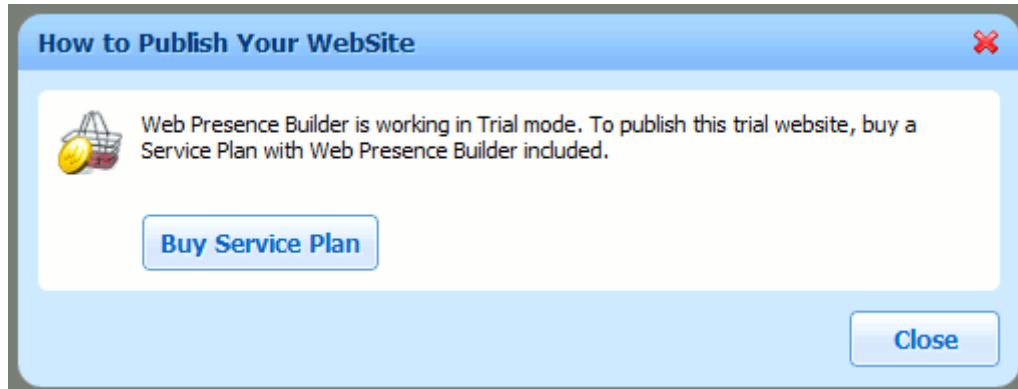
➤ **The scenario for selling hosting with Presence Builder to potential customers is as follows:**

- You enable public access to the Presence Builder trial mode in Panel by selecting the corresponding checkbox in the **Server Administration Panel > Tools & Settings > Try and Buy Mode Settings**. If this mode is activated, everyone who follows a special promotional link is able to create a trial site.

Enable public access to trial mode

If you want to attract customers by advertising hosting with Web Presence Builder and publish trial mode access URL on your website.

- You obtain the promotional link from the Panel GUI and put this link on your website so that potential customers can access it.
- When the customers click the link, they are forwarded to Presence Builder where they create trial sites. The editor interface is identical to the one that appears in step 2.
- As soon as the site is ready, the customers click Publish, and Panel requests them to buy a hosting plan.



- The customers subscribe to a new plan and are free to publish the site.

Note: All notifications that customers receive while using the Try and Buy mode can be customized. Learn more in the section **Customizing Trial Mode Notifications** (on page 162).

Next in this section:

Configuring the Try and Buy for Existing Customers	160
Configuring the Try and Buy for Potential Customers	161
Customizing Trial Mode Notifications.....	162
Offering the Try and Buy with Alternative Billing Solutions.....	165

Configuring the Try and Buy for Existing Customers

Use the Try and Buy mode if you want your existing customers to create trial sites even if Presence Builder is not provided with their license or they have exceeded the number of sites they can publish.

To configure the mode, update the settings of your hosting plans. To do that, open the settings and select the item **Allow customer to create trial Presence Builder websites**. After you update the plan settings, customers are able to launch Presence Builder by clicking the corresponding link in the Control Panel.

This feature is controlled on a per plan basis, so you can offer the Try and Buy mode only for certain plans. If you deselect this item, your customers will still see the buttons to launch Presence Builder but they will not be able to actually launch it unless their plan includes Presence Builder support.

Note: If the hosting plans you want to change are imported from Business Manager and you want to keep them synced, go to the properties of corresponding plans in Business Manager, make sure that the item **Allow up-selling Presence Builder sites** is selected, and send changes to Panel by clicking **Events > Run Events**.

For details on how to edit hosting plan properties in Business Manager, see the section **Setting Up Hosting Plans in Business Manager**.

Configuring the Try and Buy for Potential Customers

Acquire potential hosting customers with Presence Builder by giving them a link to Presence Builder in the Try and Buy mode. After your customers follow this link, create a site, and try to publish it, Panel forwards them to the default online store of Business Manager. In the store, customers choose a plan with Presence Builder and subscribe to it. The subscription automatically includes the newly created site. On completing the billing and subscription setup routines, the customers become owners of the site and can publish it. You are free to block access to the trial mode URL thus make Presence Builder unavailable.

➤ **To offer the Try and Buy mode to potential customers, do the following:**

1. Prepare the default online store in Business Manager to display Presence Builder-compatible plans.

This step requires a cosmetic update: Make sure that all plans available to potential customers include at least one Presence Builder site. By default, customers see the plans from the default online store. For each of these plans, go to plan properties and check that the value of item **Sites published with Presence Builder** is not 0. If a plan includes 0 sites, your customers will not be able to publish them after subscribing to such a plan.

For details on how to edit hosting plan properties in Business Manager, see the section **Setting Up Hosting Plans in Business Manager**.

2. Enable the Try and Buy in the Server Administration Panel.

This allows customers to launch Presence Builder by following the trial mode access URL. In the Server Administration Panel, go to **Tools & Settings > Try and Buy Mode Settings**, and ensure that the **Enable public access to trial mode** checkbox is selected.

3. Obtain the trial mode access URL and put it on your website to advertise hosting with Presence Builder and attract customers.

The trial mode access URL is also available on the Presence Builder settings page.

4. (Optionally) Configure lifetime of trial sites.

On the same page you can optionally specify how often to remove unclaimed sites.

5. (Optionally) Forward customers to a separate online store. This is relevant when you want to display a separate list of plans to potential customers who want hosting with Presence Builder.

If you wish to have a separate store for the trial offering, extend the trial mode access URL with a store ID to point to a particular store. The syntax of the new URL is: `<existing URL>&storeId=<custom store ID>`. To control the plans list view, independently add a widget ID to the URL. The syntax of the new URL is: `<existing URL>&widgetId=<custom widget ID>`.

Note: The store and widget IDs must exist in Business Manager.

Learn how to create online stores in the section **Adding an Online Store**.

Learn how to create and manage website widgets in the section **Using Website Widgets to Embed Stores into Websites**.

Once you complete these steps, your potential customers will be able to create trial sites and acquire them. To block this feature, deselect access to the Try and Buy mode on the mode settings page.

Customizing Trial Mode Notifications

The Presence Builder settings (**Tools & Settings > Try and Buy Mode Settings**) let you either display the Try and Buy mode notification to customers or hide it. The notification is displayed in a bar at the top of the editor page. This section explains how to change the notification text or add some extra information to the notification. By default, Presence Builder in trial mode uses messages from the `tbbMessagesDefault.lng` file of the used locale.

➤ *To customize notifications displayed to your customers by Presence Builder in trial mode:*

1. Go to the `/usr/local/sb/resources/locale/<locale_name>` directory on Linux operating systems, or to `C:\Parallels\Plesk\sbs\resources\locale\<locale_name>` directory on Windows operating systems.

`<locale_name>` is the name of the locale for which you change the notifications. For example, the default English locale name is `en_US`.

2. Copy the `tbbMessagesDefault.lng` and rename it to `tbbMessagesCustom.lng`.

When the `tbbMessagesCustom.lng` file exists, Presence Builder uses it instead of `tbbMessagesDefault.lng`.

3. Edit messages in the `tbbMessagesCustom.lng` file.

You can edit the following messages:

Message Keyword in Locale	Message Description
<code>startUpsellLimitExceedingTitle</code>	Title of the dialog window shown on Presence Builder start page to a customer who has exceeded the limit on the websites published with Presence Builder.
<code>startUpsellLimitExceedingBody</code>	Body of the dialog window shown on Presence Builder start page to a customer who has exceeded the limit on websites published with Presence Builder.
<code>startUpsellNoSitesTitle</code>	Title of the dialog window shown on Presence Builder start page to a customer whose subscription does not include Presence Builder.
<code>startUpsellNoSitesBody</code>	Body of the dialog window shown on Presence Builder start page to a customer whose subscription does not include Presence Builder.
<code>editorTopMessageTrialSite</code>	"Call to action" bar message at the top of Presence Builder Editor shown to a new customer who creates a trial site.
<code>editorTopMessageUpsellLimitExceeding</code>	"Call to action" bar message for a trial site at the top of Presence Builder Editor shown to a customer who has exceeded the limit on the websites published with Presence Builder.

editorTopMessageUpsellNoSites	"Call to action" bar message for a trial site at the top of Presence Builder Editor shown to a customer whose subscription does not include Presence Builder.
defaultPersonalName	Default name of the customer shown on Presence Builder start page to existing customers.
initialMailSubject	Subject of website creation e-mail confirmation sent to a new customer.
initialMailHtml	Body of website creation e-mail confirmation sent to a new customer.
limitsExceededTitle	Title of the dialog window shown upon clicking the Publish button to a customer who has exceeded the limit on the websites published with Presence Builder.
limitsExceededMsg	Body of the dialog window shown upon clicking the Publish button to a customer who has exceeded the limit on the websites published with Presence Builder.
firstSitePublishTitle	Title of the dialog window shown upon clicking the Publish button to a customer whose subscription does not include Presence Builder.
firstSitePublishMsg	Body of the dialog window shown upon clicking the Publish button to a customer whose subscription does not include Presence Builder.
licenseExceededMsg	Error message shown in the Status bar upon clicking the Publish button to a customer when the number of Presence Builder websites allowed by the Panel license has been reached.
trialSiteSignUpPublishTitle	Title of the dialog window shown upon clicking the Publish button to a new customer who creates a trial site.
trialSiteSignUpPublishMsg	Body of the dialog window shown upon clicking the Publish button to a new customer who creates a trial site.
trialFeatureDisabled	Error message shown in the Status bar when a new customer tries to verify ownership in the settings of a trial site.

You can use the following placeholders in Presence Builder trial mode notifications:

- ppServerId - unique ID of Parallels Plesk Panel server;
- billingSignUpEntryPoint - entry point to Business Manager for new customers;
- billingUpSellEntryPoint - entry point to Business Manager for existing customers;
- subscriptionId - unique ID of the user subscription;
- sbSiteUuid - unique ID of a website in Presence Builder;
- sbOneTimeBackUrl - link Presence Builder that can be used only once;
- locale - locale name;
- trialSiteLifeTime - time that passes before trial websites that were not purchased by customers are removed from the server;
- trialSiteExpireDate - expiration date of trial websites;
- trialSiteUrl - link to trial website;
- siteOwnerName - name of the user owning the website;
- siteOwnerCompanyName - user's company name;
- siteOwnerEmail - user's e-mail;
- siteOwnerPhone - user's phone number;
- siteOwnerAddress - user's address;
- siteOwnerCity - user's city;
- siteOwnerCountry - user's country;
- queryString - an additional query string passed to trial mode access URL;
- helpUrl - link to Presence Builder documentation;
- sbHttpHost - Presence Builder host name.

When using placeholders in messages, use the following placeholder markers:

- &placeholder_name& - when you use a placeholder inside a hyperlink;
- @placeholder_name@ - when you use a placeholder inside a JavaScript code;
- %placeholder_name% - when you use a placeholder in plain text.

Offering the Try and Buy with Alternative Billing Solutions

If you wish to offer the Try and Buy mode for Panel with Presence Builder and a custom billing solution, you should also carry out the following operations:

1. Forward customers from Presence Builder to a custom store and save details about created sites.

When a customer clicks to purchase a site, Presence Builder sends an HTTP POST request to a billing entry point. This request contains information about the customer and the created site. Business Manager (billing engine) uses this information to associate the site with the customer's hosting account. To shift to a custom billing engine, you should change the billing entry point URL and extend your billing engine logic to save the POST parameters that come to the URL.

2. Ensure that customers purchase a hosting plan or add-on.
This solely depends on the billing system and *is beyond the scope of the CAS integration*.
3. (For new customers only) Create a customer account, a subscription, and a site in Panel.
4. Associate the site created in Presence Builder with an appropriate site in Panel.

This appendix explains how to complete operations 1, 3, and 4.

How to Forward Customers to a Custom Entry Point

By default, the store entry point URL points to Business Manager. This URL is stored in two placeholders (*billingSignUpEntryPoint* and *billingUpSellEntryPoint*) in file `tbbMessagesDefault.lng`. The location of this file depends on a Panel installation directory (we assume that you use the default one), server OS and architecture. Find the file in one of the following directories:

- (On Microsoft Windows) `C:\Program Files\Parallels\sb\Resources\locale\en_US` or `C:\Program Files (x86)\Parallels\sb\Resources\locale\en_US` depending on the server architecture.
- (On RPM package-based Linux) `/usr/local/sb/resources/locale/en_US`
- (On DEB package-based Linux) `/opt/sb/resources/locale/en_US`

To customize the entry point URL, you should create a copy of the `tbbMessagesDefault.lng` file, name it `tbbMessagesCustom.lng`, and modify the settings in the latter file.

Note: We assume that you change the entry point for a store in the `en_US` locale. To change the entry point for other locales, create and modify the `tbbMessagesCustom.lng` file in the respective directories that are on the same level with `en_US`.

To change the entry point URL, substitute all occurrences of the placeholders *billingSignUpEntryPoint* and *billingUpSellEntryPoint* with the URL you need, and remove leading and trailing "@" and "%" symbols in all occurrences of the placeholders in the file. For example, if the new entry point URL is <http://www.example.com>, you should change *@billingUpSellEntryPoint@* to <http://www.example.com>.

What Parameters to Save

The billing entry point receives POST requests that contain information about customers and trial sites they have created. Although the requests contain a number of parameters, you need to save only one - *sbSiteUuid*. This is the unique identifier of the created site. To move the site to the customer's hosting account, you should associate the parameter with an appropriate site in Panel.

How to Create a Customer Account, a Subscription, and a Site

To create these three objects, use API RPC - the protocol to create and manage Panel objects remotely. First, you should create a customer account and save the resulting ID. Then, create a subscription with the *owner-id* (in *add/gen_setup*) set to the customer ID. Finally, create a site with the *webpace-id* (in *add/gen_setup*) set to the subscription ID. Each of these three operations is presented by a packet you send to Panel.

If you wish to quickly get started with sending API RPC packets, read **API RPC Manual**. It contains the chapter **Client Code Samples** that describes how you can implement your own packet sender by using samples of client applications (PHP, C#, VB.NET).

Find samples of the packets in **API RPC Manual**, sections:

- **Supported Operations > Managing Customer Accounts > Creating Customer Accounts > Request Samples**
- **Supported Operations > Managing Subscriptions (Webspaces) > Creating a Subscription (Webpace) > Request Samples**
- **Supported Operations > Managing Sites (Domains) > Creating a Site > Request Samples**

How to Associate a Site Created in Presence Builder with a Panel Site

An association between a Presence Builder site and Panel site is also achieved through API RPC. One of the protocol calls turns a trial site into a regular site and associates it with a Panel site. This association means that when a customer clicks **Edit in Presence Builder**, their previously created site is displayed. This operation requires two parameters - the GUID of a Panel site and *sbSiteUuid* that you previously received.

The protocol call (or packet) to associate Presence Builder and Panel sites is found in **API RPC Manual**, section **Supported Operations > Managing Integration With Presence Builder > Assigning a Trial Site > Request Samples**. This section contains call samples that you can reuse with your own values. Details on how to find a site GUID are also included in the reference document, section **Supported Operations > Managing Sites (Domains) > Getting Information About Sites > Request Samples**.

What to Do Next

After you have successfully achieved the basic integration, you can extend your application to work with existing customers as well. This involves you showing them the options of upgrading their current subscription with Presence Builder support (existing customers are forwarded to *billingUpSellEntryPoint*, while new customers go to *billingSignUpEntryPoint*) rather than creating new subscriptions.

You can also personalize the store interface by using parameters received from Presence Builder. For example, you can adjust the store locale based on customers' personal data, or use the data in messages displayed to customers.

Changing Your Password and Contact Information

➤ *To change your password:*

1. Click the **Change Password** link in the navigation pane.
2. Enter your old and new passwords.
3. Click **OK**.

➤ *To update your contact information:*

1. Click the **Profile & Preferences** link in the navigation pane.
2. Update your information as required, and click **OK**.

➤ *If you forgot your password:*

1. In your web browser's address bar, type the URL where your Parallels Plesk Panel is located.
For example, `https://your-server.com:8443`.
2. Press **ENTER**. Parallels Plesk Panel login screen will open.
3. Click the **Forgot your password?** link.
4. You will be prompted to specify your login name and e-mail address registered in the system. Type your login name into the **Login** box, type your e-mail address registered in the system into the **E-mail** box, and click **OK**.
5. If your password cannot be sent by e-mail because it was stored by the system in encrypted form, you will be prompted to set up a new password using a secret code that will be generated for that purpose and sent to your e-mail.
6. Once you received the e-mail from the password reminder, click the link in the message body. A new browser window will open.
7. At this step, specify your login name and a new password.
The **Secret Code** field of the form should be automatically filled by the system, and if it is not, copy the secret code from the message you received to the clipboard and paste to the form.
8. Click **OK** to submit.
The instructions on how to restore your password will be sent to your e-mail address.

If Your Panel Works with Parallels Customer and Business Manager

For the Panel to work fine with Parallels Customer and Business Manager, you will have to actually change two passwords. The first is that you and Business Manager use to work with the Panel, and the second is a global password you use to log in to both Business Manager and the Panel.

➤ **To change your password if you employ Business Manager:**

1. Change your password in the Panel by following instructions from section **Changing Your Password and Contact Information** (on page **168**).
2. Update this password in connection settings of Business Manager.
 - a. Click **Business Setup > All Settings**.
 - b. Click **Hosting Panels**.
 - c. Select the ID of the group where the Panel resides (*PleskUnix* or *PleskWin*).
 - d. Click **Edit**.
 - e. Change the password to the one you specified at step 1.
3. Set this password as global account password.
 - a. Make sure you are in Business Manager and click the **Profile** link in the upper-right corner of the page.
 - b. Repeat the password you specified at step 1.

Appearance and Branding

Next in this section:

Appearance.....	170
Branding and Themes	176

Appearance

Next in this section:

Interface Preferences	171
Administrator's Interface Language	172
Setting Up Supported Languages.....	173
Adding and Removing Custom Buttons	174

Interface Preferences

Changing Panel View

Depending on your goals, Panel provides two different views you can choose from when working with Panel:

- Select *Service Provider* if you use Panel for selling web hosting services.
- Select *Power User* if you use Panel for you own needs, for example, to manage hosting on a VPS.

Read more about the views in **Interface Views** (on page 24).

To quickly change your view, go to **Tools & Settings > Interface Management**.

Hiding Panel Controls

To make Panel interface better suit your needs, you can hide predefined sets of controls in Panel. For example, by default, Panel offers domain names and SSL certificates from the MyPlesk.com online store to your customers in the Control Panel. If you resell domain names or SSL certificates from other providers, you can hide the links to MyPlesk.

The tools for hiding Panel controls are available at **Tools & Settings > Interface Management > Interface Controls Visibility** tab. Here you can show or hide the following things:

- **Hide buttons for domain registration.** Hides links to domain registration services provided by the MyPlesk.com online store. Select this option if you are reselling domain registration services from other registrars.
- **Hide buttons for certificate purchasing.** Hides links to SSL certificates purchasing services provided by the MyPlesk.com online store. Select this option if you are reselling SSL certificates from other registrars.
- **Hide buttons for extra services.** Hides links to extra services provided by the MyPlesk.com online store.
- **Hide controls for rejection of messages for non-existent mail addresses.** Select this option if you want to prohibit your users from using their own mail bounce policies for email addressed to non-existent recipients within their domains.
- **Hide newsfeeds in webmail and on default domain pages.** Hides news feeds shown on default website pages.
- **Hide Parallels Virtuozzo Containers promotion page.** Hides Parallels Virtuozzo Containers promotional links in Panel.
- **Disconnect Customer & Business Manager.** This option is shown only if Parallels Customer and Business Manager is installed on the server. Select this option if you installed Parallels Customer and Business Manager by mistake or want to stop using it. Panel will hide the Parallels Customer and Business Manager links in the left navigation pane and stop interacting with Parallels Customer and Business Manager. Note that this will not actually remove Parallels Customer and Business Manager from the server.

Administrator's Interface Language

➤ ***To change the interface language and other settings for your Panel:***

1. Click the **Profile & Preferences** link in the navigation pane.
2. Specify the following:
 - a **Administrator's interface language.** Select the language for your Panel.
 - b **Button label length.** To prevent lengthy button captions in languages other than English from overlapping in the Panel, you may want to specify a limit here. Any button caption longer than the defined limit will be shortened and ended with ellipsis (...).
 - c **Allow multiple sessions under administrator's login.** By default Parallels Plesk Panel allows multiple simultaneous sessions for several users logged in to the Panel using the same login and password combination. This can be useful when delegating management functions to other users or in case if you accidentally close your browser without logging out, thus becoming unable to log in again until your session expires. You may want to switch off this capability, if you do not need it.




➤ ***To select the default interface language for your customers:***



1. Go to **Tools & Settings > Languages** (in the **Panel Appearance** group).
2. Select a checkbox corresponding to the language that will be set as default for new Panel users and click **Make Default**.

Setting Up Supported Languages

Panel includes language packs, the translations of user interface into different languages. If you would like to see the list of supported languages, refer to the product release notes available at <http://www.parallels.com/products/plesk/docs/>. All the supported languages are installed during the Panel installation (either clean installation or upgrade), and do not require any additional actions from you to start using them. The number of languages you can use depends on the Panel license you purchased. The Panel will alert you when you attempt to use more languages than allowed.

➤ *To view the interface languages installed in the Panel:*

1. Go to **Tools & Settings > Languages** (in the **Panel Appearance** group). The following information is displayed:
 - Language status icon shows the current status of the language pack:  language pack is accessible to users,  not accessible,  the language pack is not available to users because the limit on the number of language packs supported by your current license is exceeded.

Note: you can make a language unavailable to control panel users. To do this, click an icon . To make a language available to users, click an icon .

- **Language pack** contains the four-letter language code;
- **Language** shows the name of the language;
- **Country** displays the countries where this language is native;
- **Used** displays the number of control panel users at all levels that use this language in their interface.

➤ *To select a new default language for the Panel:*

1. Go to **Tools & Settings > Languages** (in the **Panel Appearance** group).
2. Select the checkbox corresponding to the language you wish to set as default and click **Make Default**.

Adding and Removing Custom Buttons

You can add custom hyperlink buttons to the Panel and make them visible for your resellers and customers. The links may lead to web resources, such as your corporate site, or to a web application that can process online requests and accept additional information about the users who click these links.

You can specify what information about users should be passed:

- Subscription ID.
- Primary domain name associated with a subscription.
- FTP account username and password.
- Customer's account ID, name, e-mail, and company name.

You can place the buttons in the following locations of the Server Administration Panel and Control Panel, and decide who should be able to see them:

- On the **Home** page in the Server Administration Panel, visible only to you and to the users logged in under additional administrator accounts. This is achieved by selecting the **Administrator's Home page** option in the button properties.
- On the **Home** page in the Server Administration Panel, visible only to your resellers. This is achieved by selecting the **Reseller's Home page** option in the button properties.
- On the **Home** tab in the Control Panel, visible to the hosting service customers and their users who are allowed to log in to the Control Panel. This is achieved by selecting the **Customer's Home page** option in the button properties.
- On the **Websites & Domains** tab in the Control Panel, visible to the hosting service customers and their users who are allowed to log in to the Control Panel. This is achieved by selecting the **Websites & Domains page of Subscription** option in the button properties.
- On the **Home** page in the Server Administration Panel and Control Panel, visible to you, all resellers and customers. This is achieved by selecting the **Common access** option in the button properties.

➤ ***To add a custom hyperlink button to the Server Administration Panel or Control Panel:***

1. Go to **Tools & Settings > Custom Buttons** (in the **Control Panel Appearance** group), and click **Add Link to Service**.
2. Specify the following properties of the button:
 - Type the text that will show on your button in the **Button label** box.
 - Choose the location for your button.
 - Specify the priority of the button. Your custom buttons will be arranged in the Panel in accordance with the priority you define: the lower the number, the higher the priority. Buttons are placed in the left-to-right order.
 - To use an image for a button background, type the path to its location or click **Browse** to browse for the desired file. It is recommended that you use a 16x16 pixels GIF or JPEG image for a button to be placed in the navigation pane, and 32x32 pixels GIF or JPEG image for buttons placed in the main frame or desktop.
 - Type the hyperlink of your choice to be attached to the button into the **URL** box.

- Using the checkboxes, specify whether you want the customer information and other data to be transferred within the URL. These data can be used for processing by external web applications.
- In the **Tooltip text** input field, type in the help tip that will be displayed when you hover the mouse pointer over the button.
- Select the **Open URL in Parallels Panel** checkbox if you want the destination URL to be opened right on the Panel page, otherwise, leave this checkbox cleared to open the URL in a separate browser window or tab.
If the URL leads to a Panel extension or web app, you can use the **Do not use frames** option to specify how the extension/app should be displayed on the Panel page: in a frame or as a part of the Panel GUI. The latter is recommended as the extension/app is seamlessly integrated into the Panel GUI. Note that the **Do not use frames** option is relevant only for the extensions/apps that support this feature. If an extension/app does not support the integration with the Panel GUI, it will be displayed in a frame regardless of the **Do not use frames** option.
- If you want to make this button visible only to you, select the **Show to me only** checkbox.

3. Click **Finish** to complete creation.

➤ ***To remove a hyperlink button from the Panel:***

1. Go to **Tools & Settings > Custom Buttons** (in the **Control Panel Appearance** group).
2. Select a checkbox corresponding to the button that you want to remove and click **Remove**.

Branding and Themes

Configure your own branding for Parallels Plesk Panel by modifying page titles, logo, or applying custom Panel themes (former skins). The branding tools are available in **Tools & Settings > Panel Branding** (in the **Panel Appearance** group).

Here we provide details about each of the options:

- *Title of Panel pages* is the title your customers see at the top of the browser window when they log in to Panel. By default, it is *Parallels Plesk Panel 11.5.30*.
- *Logo* is a banner in the top frame visible to your customers when they log in to their Panels. You can also make your logo a clickable hyperlink. You should use a GIF, JPEG, or PNG format file for your logo, preferably not larger than 100 kilobytes to minimize the download time. It is recommended that you use an image of 50 pixels in height.





In addition to these two options, you are able to change the visual appearance and branding of the Panel by applying custom themes. Two themes are available by default: Panel 11 and Panel 10. You can try the new look or continue using the appearance of the previous Panel version. For information about using custom themes, refer to the document **Creating Custom Themes**.

Panel Components

Panel orchestrates the work of a number of web, mail, DNS, and other services. Technically, Panel does not provide the services by itself; it just takes control over a number of third-party components. For example, when a customer creates a website through the Panel GUI, Panel propagates this request to a web server (Apache or IIS) and the latter adds a new virtual host to the system. The list of components is defined during Panel installation (see the **Installation, Upgrade, Migration, and Transfer Guide** for details). Panel allows you to view the list of installed components, add new ones, switch between interchangeable components, and remove them (only in Windows).

Viewing Panel Components

You can view the list of installed components and their versions in **Tools & Settings > Server Components**. *Panel for Windows* has an additional indication of a component state (the appearance of the icons depends on the Panel theme):

-  means that Panel is using this component, and the component is working.
-  means that Panel is not using this component (usually because a license key has expired or missing), but the component is working.
-  means that Panel is not using this component because the component is stopped.
-  means that Panel is not using this component, but the component is installed on the system and is available.

Installing Panel Components

If you did not include a component in your Panel installation, you can add it later in **Tools & Settings > Updates and Upgrades > Add Components**.

Switching Between Interchangeable Components

Some Panel components are interchangeable. For example, in Windows you can use either MS DNS Server or BIND as your DNS server; in Linux you can choose between Postfix and Qmail for mail delivery, and so on.

On *Panel for Linux*, you can switch between interchangeable components in two ways:

- *Using service settings.* Some Panel components with a similar purpose can be installed side-by-side on the same Panel server. For example, if you have two installed antivirus components, you can specify the one that will process your mail in **Tools & Settings > Mail Server Settings**.
- *Using Parallels Installer.* Some Panel components with a similar purpose do not allow side-by-side installation. For example, there can be only one mail server in Panel: either Postfix or Qmail. In this case, you should choose the component you want in **Tools & Settings > Updates and Upgrades > Add Components**.

On *Panel for Windows*, you can switch between interchangeable components in **Tools & Settings > Server Components**. To perform the switch, click on the component name (for example, **Mail Server**) and select the required component from the list.

Removing Panel Components (Windows)

If you no longer need a certain Panel component, you can remove it from Panel in **Tools & Settings > Updates and Upgrades > Add/Remove Components** or by clicking the **Add or Remove Components** link on the Home page.

Web Applications

The majority of customers purchase web hosting accounts to run different web applications: Webmail, CRM, e-commerce systems, blogs, image galleries and so on. Typically, such users are unable to install the apps by themselves because they lack the necessary technical skills and experience, so they ask their service providers to do it. Hence, the provider's staff becomes overloaded with routine operations related to the apps. To ease the installation (and maintenance) of web apps and reduce the staff's workload, Parallels offers a number of free and commercial apps available to Panel users directly from their Control Panel.

There are various factors that regulate what apps are available to your customers. For example, the app list is restricted by service plan or subscription properties, local repository settings and so on. To see how the apps list is formed, refer to the **How Apps Become Available to Your Customers** section.

App Types

Parallels offers two types of apps:

- Apps that are installed directly on a website (such as the WordPress blogging platform or the Joomla! content management system).
- Apps that do not require a website for their installation. These are usually external apps located somewhere on the web that only provide a link to their services (such as the iMind videoconference service or OfficeDrive - an online office suite).

Apps can be either *free* or *commercial*. Commercial apps require providing a license key to start working with them. You or your customers can buy licenses for commercial apps right from the Control Panel: In the **Applications** tab such apps are accompanied by the **Buy Now** button instead of **Install Now**. If your Panel license comes in a bundle with licenses for certain commercial apps, you do not need to additionally obtain app licenses.

App Installation and Maintenance

The process of installation does not require any specific skills from customers. They fill in app settings (for example, administrator credentials), and Panel installs the app for them. Subsequent app management is also facilitated as apps are updated or removed directly in Panel. Moreover, customers can access some functions that apps make available in the Control Panel (without the need to log in to an app). For example, customers can upload a new WordPress theme or add a SugarCRM user account directly from their Control Panel. Such app functionality is a *service* the app provides to customers.

Apps Backup and Restoration

Apps are backed up by standard Panel means (the `backup` utility). Since the backup unit is a subscription, all apps in a subscription must be backed up at once. The apps from a backup are restored along with other subscription data.

Application Vault and Application Catalog

If there are no restrictions on app availability, the list of available apps in the Control Panel includes all apps from the following two sources:

1. Application Catalog - the remote repository held by Parallels, the main source of apps.
2. Application Vault - a local repository in Panel. Every Panel has own Application Vault that is available through the Server Administration Panel (**Server Management > Tools & Settings > Application Vault**).

The main purposes of the Application Vault are to:

- *Extend the list of available apps by uploading your own APS packages.* This is relevant if you want to offer some apps to your customers but these apps are not listed in the Application Catalog.

- *Apply updates to apps installed from the Application Catalog.*
- *Gain control over apps from the Application Catalog.*
Download an app from the Catalog to the Vault to control some of its options. For example, you can toggle its visibility to customers or configure its server-wide settings.

For more information on managing apps through the Application Vault, refer to the **Managing Apps with the Application Vault (on page 183)** section.

Summing up, the Application Vault is not only a local repository of apps but a tool to control versioning, visibility, and server-wide settings of apps from the Application Catalog. For better understanding of the Application Vault, refer to the scheme shown in the **How Apps Become Available to Your Customers** section.

Sharing Apps among Panel Servers

Adding an APS package to the Application Vault will make it available only to your customers. If you wish to share your app with users of other Panel servers, add an app to the Application Catalog. The Catalog accepts only apps packaged according to Application Packaging Standard (APS) - the set of rules that allows easy app installation and management. After you have packaged your app, it must pass the certification procedure. For details on how to do this, see <http://www.apsstandard.org/why-aps/isv/>.

Storefront

Since Panel 10, Parallels Partner Storefront program offers you the possibility to earn by selling commercial apps to customers in a revenue-share model. Within this program, you select the apps you want to sell and Parallels adds them to the list of apps available in Control Panel. Once customers choose one of the paid apps selected for the program, they are forwarded to a store with your own branding to complete the order. This branded store is called the Storefront.

All ordering, licensing, and billing aspects are handled by the Storefront. You just track the sales and receive a profit from each app sold.

Note: Storefront may contain some commercial apps that are available in Application Catalog as well. In this case, Storefront apps have a priority and customers always see them first in the list of available apps.

Note that you should have the appropriate Panel license to participate in the program. For more information on Parallels Partner Storefront, refer to the <http://www.parallels.com/products/plesk/storefront/>.

For the details about how you can manage the availability of Storefront apps to your customers, refer to the section **How Apps Become Available to Your Customers** (on page 181).

Next in this section, we will provide details on how to manage apps using the Application Vault as well as the information on how apps become available in the customer's Control Panel.

Next in this section:

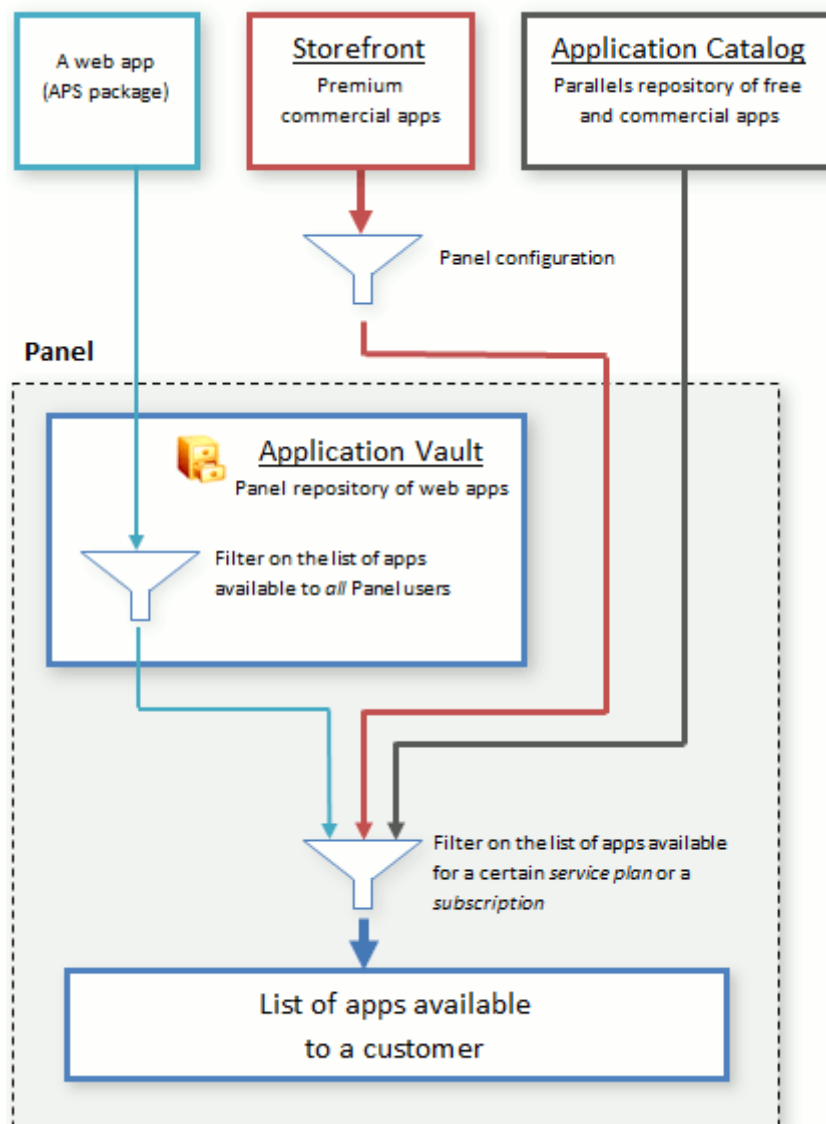
How Apps Become Available to Your Customers 181
Application Vault..... 183

How Apps Become Available to Your Customers

The list of apps available to a customer depends on various factors, such as the service plan settings, the Application Vault configuration, and so on. Moreover, service providers are able to forbid accessing apps for all Panel users. If you do not adjust the app availability, your customers will see all apps from Application Catalog, Storefront (either yours or Parallels's), and all apps you uploaded to the Vault.

To view the list of apps available to a certain customer, go to the **Applications** tab > **All Available Applications**.

This diagram explains how the list of available apps is formed.



Before an app becomes available in the app list of a certain customer, it passes through a series of filters. The app is filtered on the following levels:

1. Panel configuration (Storefront apps only).

Since Panel 10.4, you can specify whether you want to offer premium commercial apps to your customers in **Tools & Settings > Interface Management > the Interface Controls Visibility** tab. Turning this option on implies the following:

- If you participate in the Storefront program, customers will proceed to your own branded store to buy premium commercial apps. You will receive the commission for each app.
- If your license does not have the Storefront feature, customers will be able to buy premium apps as well but the purchase will be performed in Parallels Storefront (Parallels online store). In this case, you do not get any sales revenue.

If you decide not to offer premium commercial apps, they will not be shown to your customers in Control Panel regardless of your participation in the Storefront program.

2. Application Vault.

Panel lets you toggle the availability of APS packages you have uploaded to the Vault. Note that this works *only for your own packages*: There is no way to control the availability of apps downloaded from the Catalog. Learn more about apps management in the **Managing Apps with the Application Vault** (on page 183) section.

3. Service plan.

Panel allows you to specify what apps to include in a certain service plan. The filter affects all customers with this service plan.

4. Subscription.

If you want to select the apps available to a particular customer, update the apps list in the respective subscription.

The resulting app list is available to your customers.

Application Vault

Application Vault performs the functions of a local repository and an apps management tool. The repository functionality allows you to add, update, and remove app packages. Using the management capabilities, you can view what apps were installed in Panel, configure apps, or make them unavailable for installation. In addition, you can delete temporary installation files by clearing the Vault cache. Next in this section, you will find detailed instructions on performing these operations with apps.

Application Vault is available in the Server Administration Panel: **Server Management > Tools & Settings > Application Vault**.

Next in this section:

Adding Your Apps to Panel	184
Configuring Server-Wide Settings of Apps.....	184
Managing Apps Availability to Customers.....	185
Removing App Packages	185
Tracking App Installations	185
Updating Installed Apps.....	185
Clearing the Application Vault Cache	186
Troubleshooting App Installations.....	186

Adding Your Apps to Panel

If you have a web app that you want to offer to your customers in addition to Catalog apps, you should add it to the Application Vault. Note that you can only upload apps packaged in the APS format.

To upload your app, use **Tools & Settings > Application Vault > My Apps > Add App**. After you upload the app, it will appear in the Control Panel of all customers.

Configuring Server-Wide Settings of Apps

In some cases, apps from the Catalog require server-wide configuration before customers can install them. For example, if an app installation affects some Panel services, it may require an administrator password. When your customers attempt to install such an app, they are asked to contact their provider (you) to perform the configuration. After you configure the settings, customers can install the app on their websites.

Generally, server-wide settings of an app are the settings that apply to all app installations and they cannot be changed by customers. For example, customers cannot install the ePages e-commerce app until you define how customers should access the app, either by HTTP or HTTPS.

To configure server-wide settings, complete these two steps:

1. Add the Catalog app by using **Tools & Settings > Application Vault > My Apps > Add App**.
2. Select the app from the list in the **My Apps** tab and submit the settings.

Managing Apps Availability to Customers

After an APS package is uploaded to the Vault, you can manage its availability to customers. This can be useful when you want to temporarily hide your app from *all* customers. In that case make the app unavailable in the **Tools & Settings > Application Vault > My Apps** tab. The app will disappear from the list of available apps of all customers. To return the app to the list, make it available in the **My Apps** tab. Note that you cannot perform these operations on apps you downloaded from the Catalog.

Removing App Packages

You can *only* remove packages stored in the Vault. If you remove an app from the **Tools & Settings > Application Vault > My Apps** tab, the Vault will delete the app package.

This operation does not affect *app installations*. Installed apps can be removed only by particular customers (installation owners) from their Control Panel.

Tracking App Installations

In general, customers install apps directly from the Application Catalog, bypassing the local repository. The only exceptions are apps that you have added to the Vault. Nevertheless, *all* app installations are registered in the Vault. You can view the details on the installations in the **Tools & Settings > Application Vault > Installed Apps** tab. A zero number of app installations in the list means that the app package is stored in the Vault but is has not been installed by any customers.

Updating Installed Apps

The Application Vault allows updating of any app installed in Panel to the latest version available in the Catalog. There are two main scenarios of updating apps in Panel: either when a certain app installation is updated by you or by your customer (installation owner). You can check for app updates by clicking the app name in the **Tools & Settings > Application Vault > Installed Apps** tab. If an update is available, you can apply it by clicking the link **Updates are available**. To learn how customers can update their app, refer to the section **Updating Apps** (on page 425).

Forced Apps Updating

You can force automatic updating of all installed apps in Panel. In this case, Panel will automatically update all app instances once updates are available.

➤ **To turn on forced automatic updates:**

1. Go to **Tools & Settings > Application Vault > Installed Apps > Update Settings** page.
2. Select the option **Force updates for all installed apps**.

We recommend that you use this option only if you are sure that this will not affect the functionality of websites. This may happen, for example, if your customers use app extensions: An extension developed for a certain app version may be incompatible with newer versions.

Note: If you force app updates, your customers will be unable to turn off automatic app updating as described in the section **Updating Apps** (on page 425).

Clearing the Application Vault Cache

After customers install an app from Application Catalog, the app package is stored in a temporary directory on the server, the Vault cache. The files in the cache can speed up further app installations, but you can delete these files to free disk space on your server.

To delete temporary files from the Application Vault cache, use the **Tools & Settings > Application Vault > Installed Apps** tab > **Clear Cache**.

Troubleshooting App Installations

When an app cannot be installed to a customer's website due to some reason, a customer gets an error message with the recommendation to contact their hosting provider (you). The error message also contains the brief error description that should help you find the reason of a problem.

The most common problem that may occur during an app installation is when PHP does not meet app requirements:

- *PHP version is not supported.*
To resolve the problem, install the latest available PHP version in **Tools & Settings > Updates and Upgrades**.
- *Required PHP extension is turned off.*
To resolve the problem, turn on the required extension. You can do this by adding a certain PHP directive to the server-wide `php.ini` file or to the custom PHP configuration of the subscription (in case you want the extension to be available to a certain user only). Learn how to do this in the section **Customize PHP Configuration** (on page 54).
After you add the directive, restart a web server. Learn how to do this on Linux and on Windows.

Session Preferences

You can adjust the allowed idle time for all sessions in Parallels Plesk Panel as required.

➤ ***To adjust session security parameters:***

1. Go to **Tools & Settings > Session Idle Time** (in the **Security** group).
2. Specify the required **Session idle time** in minutes in the appropriate field. Should a user session remain idle for the time period exceeding the one specified as the **Session idle time**, the control panel terminates this session.
3. Click **OK**.

➤ ***To allow IP changes during one client session (available only on Windows hosting):***

1. Go to **Tools & Settings > Session Idle Time** (in the **Security** group).
2. Select the **Allow IP changes during one session** checkbox. This option will allow customers with dynamic IP addresses and unstable Internet connection to work with Parallels Plesk Panel at the cost of increasing the security risks.
3. Click **OK**.

➤ ***To reset all parameters back to their default values:***

1. Go to **Tools & Settings > Session Idle Time** (in the **Security** group) and click **Default**. The default session idle time will be set to 30 minutes.
2. Click **OK**.

Managing Panel from Mobile Devices

If you need a mobile app to keep pulse on Panel <PP_short_v> server indicators, use the *Parallels Plesk Mobile Server Monitor*. If you also need to take immediate actions on Panel servers right from your mobile device, take advantage of the other application, *Parallels Plesk Mobile Server Manager*. This section discusses the features of these apps, their installation and usage instructions.

Application Features

With *Mobile Server Monitor*, administrators can:

- View the list of services on a particular server.
- View information about a server: OS, CPU, Panel version and so on.
- View vital indicators of a server health: CPU load average, memory consumption, swap usage, etc.
- Receive information about certain Panel events.

Mobile Server Manager incorporates the features of Mobile Server Monitor and additionally gives administrators control over core Panel administration functions.

With Mobile Server Manager, administrators can:

- View the list of services on a particular server.
- View information about a server: OS, CPU, Panel version and so on.
- View vital indicators of a server health: CPU load average, memory consumption, swap usage, etc.
- Receive information about certain Panel events.
- Authenticate themselves by a secret key.
- View health monitor events.
- Roll back and retrieve a Panel license key.
- Restart a server.
- Stop and start services on a particular server.

Note: Mobile Server Manager works only with servers which license includes *Parallels Plesk Panel Power Pack*. This is the license add-on that can be acquired when purchasing a Panel license or added to the license later on. Along with mobile server management, Power Pack offers premium commercial antivirus protection, web hosting of Tomcat applications and many other features. Learn more about Power Pack at <http://www.parallels.com/products/plesk/power-pack/>. You are welcome to try Mobile Server Monitor for free; if you feel you need control over your servers, add Power Pack to your Panel servers and enjoy Mobile Server Manager.

Supported Operating Systems and Devices

Currently, Monitor and Manager apps are supported on Android, Blackberry, and iPhone. Use the following links to download the apps from the respective app stores.

Operating System and Devices	Server Monitor	Server Manager
Android 2.2+ compatible devices.	https://play.google.com/store/apps/details?id=com.parallels.panel.monitor	https://play.google.com/store/apps/details?id=com.parallels.panel.manager
BlackBerry OS 5.0+ compatible devices: <ul style="list-style-type: none"> ▪ Bold 9000, 9650, 9700, 9780, 9788, 9790, 990, 9930 ▪ Curve 9330, 8350i, 8520, 8530, 8900, 8910, 8980 ▪ Curve 3G 9300, 9330, 9350, 9360, 9370, 9380 ▪ Pearl 3G 9100, 9105 ▪ Storm 9500, 9530 ▪ Torch 9800, 9810, 9850, 9860 ▪ Tour 9630 	http://appworld.blackberry.com/webstore/content/62901?lang=en	http://appworld.blackberry.com/webstore/content/62900/?lang=en
iOS 4.0+ compatible devices.	http://itunes.apple.com/us/app/parallels-panel-server-monitor/id477441966?mt=8	http://itunes.apple.com/us/app/plesk-manager/id477441273?mt=8

Installation and Usage Instructions

If you have a Panel installation, find guidelines on how to install and use the mobile apps at the following URLs:

- Mobile Server Monitor - https://Server_URL:8443/admin/promotion/mobile-monitor/

Mobile Server Manager - https://Server_URL:8443/admin/promotion/mobile-manager/ Here *Server_URL* stands for the IP address or host name of your server.

Configuring Panel to Work with Mobile Apps

To interact with Mobile Server Manager or Mobile Server Monitor 1.1 and earlier, Panel uses the built-in mechanism and does not need any additional configuration.

Starting with Mobile Server Manager and Mobile Server Monitor 1.2, Panel uses the *Mobile Center* extension for interaction with the apps. Panel installs this extension automatically after you try to connect the apps to your Panel server.

The Mobile Center extension accepts requests from the mobile apps to the Panel server, processes them, and sends responses back to mobile apps.

The extension writes information about its activities and problems to its own log file. The log file location on the Panel server is the following:

- On Linux: `/usr/local/psa/var/modules/plesk-mobile/MobileConnector.log`
- On Windows: `%plesk_dir%/var/modules/plesk-mobile/MobileConnector.log`, where `%plesk_dir%` is the path to the Panel installation directory.

There are three types of log entries:

- *Notices* - general information that may be useful for troubleshooting, for example, updating the extension database.
- *Warnings* - information about events that may cause problems but the system solves them automatically. For example, if the extension's configuration file is unavailable, the system will create a new file automatically and add the corresponding warning message to the log.
- *Errors* - information about failing certain operations, for example, when the extension fails to deliver a response to the mobile app because the mobile device is unavailable.

On the Mobile Center page (**Extensions > Mobile Center**), you can define the following settings:

- *The verbosity of the extension log* (the **Log level** parameter). Once you choose a certain level, the extension will write entries of the selected type and entries with higher severity as well. For example, if you choose the **Warning** log level, the log will contain warnings and errors. The **Off** level turns off logging.
- *iOS push notification service*. If you use Mobile Manager or Mobile Monitor on iOS, you may configure Panel to send *push notifications* to your device. Such notifications enable your device to inform you about important events on Panel server by showing alert messages when the apps are not running in foreground. Note that to accept push notifications, you should switch on the corresponding option in your mobile apps as well.

Panel Inside Parallels Virtuozzo Containers

The following operations are not available from the Panel when it is operating inside Parallels Containers:

- Adding to and removing IP addresses from the server's network cards.
- Changing host name.
- Setting system date and time.

After adding IP addresses to the Parallels Virtuozzo Containers hardware node, you need to use the **Reread IP** function in Server Administration Panel (in **Tools & Settings > IP Addresses**) to update the Panel's IP pool.

When installing the Panel inside a Parallels Container, you need to configure the Offline Service parameter for the Container to ensure that the both Parallels Plesk Panel web interface and the Parallels Power Panel, used for managing Containers, are accessible.

By default, the Container is configured so that the following parameters are enabled for the Offline Management service: **VZPP-plesk** (redirection of connections on the port 8443) and **VZPP** (redirection of connections on the port 4643). You need to disable the **VZPP-plesk** service. You can do this on Parallels Virtuozzo Containers for Linux and Windows by using the Parallels Management Console utility.

➤ ***To configure the container using the Parallels Management Console:***

1. Open the Parallels Management Console.
2. Connect to the Parallels Containers hardware node.
3. Click **Virtuozzo Containers**.
4. Select the Container, right-click it, and select **Properties** from the context menu.
5. Go to **Network > Offline Management**, and disable the **VZPP-plesk** service.

➤ ***To configure the container using the command line tools on a Linux-based hardware node:***

1. Connect to the hardware node over SSH.
2. Issue the following command:

```
vzctl set CT_ID --offline_management yes --offline_service vzpp --save
```


➤ ***To configure the container using the command line tools on a Windows-based hardware node:***

1. Connect to the hardware node over Remote Desktop.
2. Issue the following commands:

```
vzctl set CT_ID --offline_management yes --save  
vzcfgt set CT_ID offlineservices vzpp
```

After configuring the Container, you will be able to access the Container management functions from the Panel (at Tools > **Manage Your Container** [in the **Server Management** group]).

Remote Access (Windows)

The remote desktop (RDP) access feature allows you to remotely log in to the Parallels Plesk Panel server and interact with it using standard Microsoft Windows desktop interface.

➤ **To access the server via Remote Desktop interface:**

1. Go to **Tools & Settings > Remote Desktop**.
2. Set up screen resolution for the session in the **Screen resolution for terminal session** menu.

Note: Higher resolutions are more taxing for your connection, decreasing the interaction speed and spending more bandwidth.

3. Select the connection method according to your browser:
 - **Microsoft RDP ActiveX** - recommended to use with Internet Explorer browser, since it may not work with other browsers. When you use this method for the first time, your browser will automatically install the required ActiveX component, if Internet Explorer security settings permit this. If your browser shows security alerts, try to temporarily lower security measures in the browser options.
 - **properoJavaRDP** - recommended to use with Netscape, Mozilla, or Firefox browsers, since it may not work with Internet Explorer. Only 8.0 and higher versions of Opera are supported. This component requires Java Runtime Environment (JRE) to be installed on your system. If you do not have JRE, you can download it from <http://www.java.com/en/download/manual.jsp> (version 1.4 and higher) and install it before using the remote desktop feature.

Note: You don't need to install JDK (Java Development Kit) in order for the RDP feature to work.

If you use Internet Explorer or Mozilla, you should open the Terminal Services Configuration console in Microsoft Windows (**Start > Administrative Tasks**), and set the **Licensing** option to **Per user** on the **Server Settings** screen.

4. Click **OK**. A new window will open with an area where your interaction with the server's desktop will take place.
5. Log in to the system. By default, the Panel uses the subscription's FTP/Microsoft FrontPage username. You can supply any valid username and password.
6. After logging in to the system you can start working with it as with a regular Windows desktop.

➤ **To finish your Remote Desktop session:**

- Close the browser window with the remote desktop session. This way, the session you had will be detached from your desktop, but it will keep running on the server, so when you log in there next time, you will see the remote desktop in the state you left it, or
- Select **Start > Log off** if you want to quit the session permanently (all running sessions consume the server's resources).

Additional Administrator Accounts

You can create additional Administrator level accounts for your technical support engineers, enabling them to perform a virtually limitless variety of administrative tasks. All actions performed by additional Parallels Plesk Panel administrator accounts are logged, which gives the actual Parallels Plesk Panel administrator an unprecedented level of control over additional administrator accounts' activities. Additional administrator accounts have virtually all the privileges that the actual server administrator has, except the following:

- View and manage additional administrator accounts belonging to other users.
- View and manage administrator account settings.
- Clear Action Log.

Next in this section:

Creating Additional Administrator Accounts	196
Modifying Additional Administrator Accounts.....	196
Suspending and Activating Additional Administrator Accounts.....	197
Removing Additional Administrator Accounts.....	197

Creating Additional Administrator Accounts

➤ *To create additional administrator account:*

1. Go to **Tools & Settings > Additional Administrator Accounts**.
2. Click **Create Account**.
3. Specify administrator account properties:
 - Specify account login, password and e-mail address in the corresponding fields.
 - Specify the name of additional administrator account user in the **Contact name** field.
 - Use **Comments** field to add your own comments about this particular additional administrator account and its user. This can be useful to differentiate between the accounts: for example, you can create one account for a technical support engineer who manages user accounts, and another account for a technical support engineer who works with all mail-related issues. By adding appropriate comments in the **Comments** field, you can always tell who's doing what, and avoid confusion.
4. Click **OK** to finish the creation of additional administrator account.

Now you can tell account login and password to its owner.

Modifying Additional Administrator Accounts

➤ *To modify settings of additional Administrator account:*

1. Go to **Tools & Settings > Additional Administrator Accounts**.
2. Click the required additional administrator account login in the list.
3. Specify new administrator account properties:
 - Specify new account login, password and e-mail address in the corresponding fields.
 - Specify the new name of additional Administrator account user in the **Contact name** field.
 - Use **Comments** field to add your own comments about this particular additional Administrator account and its user. This can be useful to differentiate between the accounts: for example, you can create one account for a technical support engineer who manages customer accounts, and another account for a technical support engineer who works with all mail-related issues. By adding appropriate comments in the **Comments** field, you can always tell who's doing what, and avoid confusion.
4. Click **OK** to update the information of additional administrator account.

Suspending and Activating Additional Administrator Accounts

➤ *To suspend additional administrator account:*

1. Go to **Tools & Settings > Additional Administrator Accounts**.
2. Click the required additional administrator account login in the list.
3. Clear the **Allow access to control panel** checkbox and click **OK**.

➤ *To activate additional administrator account:*

1. Go to **Tools & Settings > Additional Administrator Accounts**.
2. Click the required additional administrator account login in the list.
3. Select the **Allow access to control panel** checkbox and click **OK**.

Removing Additional Administrator Accounts

➤ *To remove additional administrator account:*

1. Go to **Tools & Settings > Additional Administrator Accounts**.
2. Select the checkbox corresponding to the account you want to remove and click **Remove**.
3. Confirm removal and click **OK**.

Event Tracking

The Event Manager is designed to help you organize data interchange between Parallels Plesk Panel and external systems. It works the following way:

1. Create a script to be executed upon a certain control panel event: Shell script file for Linux or batch file for Windows.
2. Create an event handler that triggers the event processing. You can process a single event by a number of different handlers.
3. Assign your script to the event handler.

For the full list of event parameters passed by event handlers, refer to **Appendix C: Event Parameters Passed by Event Handlers** (on page 579).

Note for users of Linux: The server administrator can create the event handlers that will be run on the server on behalf of user root. If you wish to restrict usage of the root account, create an empty file with name `root.event_handler.lock` in the location `/parallels_panel_installation_directory/var/`.

Next in this section:

Adding Event Handlers (Linux)	199
Adding Event Handlers (Windows)	200
Removing Event Handlers	201

Adding Event Handlers (Linux)

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

```
#!/bin/bash

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

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

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

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

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

echo "login: ${NEW_LOGIN_NAME}" >> /tmp/event_handler.log #
customer's username in the Panel

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

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

Note: We strongly recommend that you use shell script files to handle events. Although you can assign direct system commands, they might not work. For example, commands with output redirection operators `<` or `>` will not work.

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

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

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

5. Select the system user, on behalf of which the handler will be executed ("root" user, for example).

6. In the **Command** input field, specify a command to be executed upon the selected event. In our example it is `/usr/local/psa/bin/test-handler.sh`.

7. Click **OK**.

Note: In the script, we have specified the variables `$NEW_CONTACT_NAME` and `$NEW_LOGIN_NAME`. During execution of the handler, they will be replaced with name and username of the created user account respectively. The entire list of available variables is provided in **Appendix C: Event Parameters Passed by Event Handlers** (on page 579).

Now if you log in to your Parallels Plesk Panel and create a new customer account, specifying the value 'Some Customer' in the **Contact name** field, and 'some_customer' in the field **Login**, the handler will be invoked, and the following records will be added to the `/tmp/event_handler.log`:

```
Fri Mar 16 15:57:25 NOVT 2007

uid=0(root) gid=0(root) groups=0(root)

customer created

name: Some Customer

login: some_customer
```

If you want to specify one or few handlers more, repeat the actions above for another handler.

Adding Event Handlers (Windows)

➤ *To add an Event Handler:*

For instance, let's create an event handler for the 'customer account creation' event. The handler will accept a customer's name as the first parameter, and the customer's username as the second. For simplicity, we will use a batch file called `test-handler.bat` that looks as follows:

```
echo "-----" >> c:\windows\temp\event_handler.log
rem information on the event date and time
date /T >> c:\windows\temp\event_handler.log
rem information on the created customer account
echo "customer created" >> c:\windows\temp\event_handler.log
rem customer's name
echo "name: %1" >> c:\windows\temp\event_handler.log
rem customer's username in the Panel
echo "login: %2" >> c:\windows\temp\event_handler.log
echo "-----" >> c:\windows\temp\event_handler.log
```

This script prints some information to a file so that we could control its execution.

Suppose that our script is located in the directory `c:\program files\parallels\parallels panel\scripts\`. Let's register it by creating an event handler via the Administrative Panel:

1. Go to **Tools & Settings > Event Manager**.
2. Click **Add New Event Handler**.
3. Select the event you wish to assign a handler to in the **Event** drop-down box.
4. Select the priority for handler execution, or specify a custom value. To do this, select **custom** in the **Priority** drop-down list and type in the value.

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

5. Select the system user, on behalf of which the handler will be executed.
6. In the **Command** input field, specify a command to be executed upon the selected event. In our example, it is `c:\program files\parallels\parallels panel\scripts\test-handler.bat` `<new_contact_name>` `<new_login_name>`.

Note that if directory names or the file name contains spaces, the path should be quoted.

7. Click **OK**.

Note: In the command, we have specified the parameters in the angle brackets `<new_contact_name>` and `<new_login_name>`. Before executing the handler, they will be replaced with name and username of the created customer. The entire list of available parameters is provided in the section **Event Parameters Passed by Event Handlers** (on page 579).

Now if you login to your Parallels Plesk Panel and create a new customer account, specifying the value 'Some Customer' in the **Contact name** field, and 'some_customer' in the field **Login**, the handler will be invoked, and the following records will be added to the

`c:\windows\temp\event_handler.log`:

```
Mon March 15 21:46:34 NOVT 2010
customer created
name: Some Customer
username: some_customer
```

If you want to specify one or few handlers more, repeat the actions above for another handler.

Removing Event Handlers

➤ *To remove an event handler:*

1. Go to **Tools & Settings > Event Manager**.
2. Select the corresponding checkboxes in the list of handlers and click **Remove**.

Migration from Other Hosting Platforms

If you have a server with a different hosting platform (for example, cPanel, Confixx, or other supported solution) and want to switch from this platform to Panel, you should *migrate* all hosting data from this server (*source*) to your Panel server (*destination server*).

Panel 11.5 supports migration from the following platforms:

- cPanel for Unix, versions 9, 10, 11
- Confixx 3.3.7 for Linux
- Parallels Pro Control Panel for Linux version 10.3.4 (formerly known as Ensim Pro)
- Parallels Helm 3.2
- Parallels Small Business Panel 10.x

To migrate data from another hosting solution, we recommend that you use the *Migration & Transfer Manager* utility. Before running the utility, you should perform a number of preparation steps which may vary depending on your source platform. For the detailed instructions on how to perform migration, refer to the chapter **Migrating to Panel** of the **Installation, Upgrade, Migration, and Transfer Guide**.

Data Transfer from Another Panel

If you want to relocate your Panel to another server, the easiest way to do this is to transfer Panel data to this server. In terms of Panel, *transfer* is a process of moving hosting data from one Panel server (*source*) to another server with Panel of the same version (*destination server*). There are two ways to transfer data from one Panel to another:

- *Transfer with the Migration & Transfer Manager utility (recommended).*
We recommend that you transfer hosting data using the *Migration & Transfer Manager* utility. This utility runs on a destination server and automatically copies hosting data from your source Panel.
- *Transfer through backup files.*
You can also transfer data from the source to destination server using backup files. To perform the data transfer, you should back up data on the source server, transfer the resulting archive file to the destination server manually, and restore the data on this server.

For the detailed instructions on transferring data between two Panels, refer to the chapter **Transferring Panel Data** of the **Installation, Upgrade, Migration, and Transfer Guide**.

Panel Extensions (Linux)

Using extensions is another way of increasing the functionality of your Panel for Linux. Extensions are functional components (such as a file server, firewall, or system monitor) developed by Parallels or third parties.

To obtain add-ons developed by Parallels partners, visit our online store at <http://www.parallels.com/store/plesk/partners/>.

The extensions can be easily installed, removed, and configured directly from Panel (**Extensions > Manage Extensions**). Learn more about installing Panel extensions in the **Installation, Upgrade, Migration, and Transfer Guide**, in the chapter **Installing Panel Extensions**.

This section contains information on how to configure extensions developed by Parallels:

- *Counter-Strike game server extension*. Used to deploy Counter Strike game servers. Starting from Plesk 11.5, this extension is no longer shipped with Plesk. However, it might still be available to users who upgrade to Plesk 11.5 from earlier versions.
- *File Server extension*. Used to share directories on a network directly from Panel.
- *Firewall extension*. Used to protect the Panel server and private networks from unauthorized access.
- *Watchdog extension*. Used for system monitoring.
- *VPN extension*. Used for establishing communications between geographically distributed LAN segments over public networks.

For information on how to configure extensions developed by third parties, refer to the respective documentation.

Next in this section:

Counter-Strike Game Server Extension.....	204
File Server Extension	215
Firewall Extension	223
Watchdog (System Monitoring) Extension.....	230
VPN Extension	242

Counter-Strike Game Server Extension

Note: Starting from Plesk 11.5, this extension is no longer shipped with Plesk. However, it might still be available to users who upgrade to Plesk 11.5 from earlier versions.

With this extension you can:

- Deploy, configure, and uninstall Counter-Strike game servers.
- Specify which maps each game server should use.
- Start, stop, and restart game servers.
- Add and update game mods with the Steam utility provided by Valve.
- Delegate permissions for managing game servers to other users.

Next in this section:

Deploying Game Servers	205
Starting, Stopping, Restarting Game Servers	213
Updating Game Servers	214
Removing Game Servers	215



Deploying Game Servers

Once you install the Counter-Strike Game Server extension on your Parallels Plesk Panel, you will need to take a few steps to install the game server program files and other required components. These files will be shared among all game servers that you will set up.

➤ *To obtain and install the core components of game servers:*

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. The installation program starts searching for an installed game server engine. If it does not detect it, the installer will offer you the two options:
 - **Install the game server automatically** - download the game server files from the official directory servers on the Internet and install them automatically. This procedure might take much time and hundreds megabytes of data transfer, depending on the number of components you wish to install. During automatic installation, you will be asked to choose the game version (Counter-Strike, Counter-Strike Source, and Counter-Strike Condition Zero) to install.
 - **Use an existing installation** - if you already have the game server engine installed, use this option to specify the path to the directory where it is installed.
3. Click **OK**.
4. Install the Steam software. Steam is an online content delivery system designed by Valve Corporation. To be able to download, install and update games from the Valve website through the Internet, you need to install the Steam client.

Important: By downloading and installing the Steam client, you assume responsibility for the consequences of using this software. Use it at your own risk!

- If you do not have the Steam client program or Counter-Strike game server installed, leave the **Download from the official Valve site and install** option selected and click **OK**. The Steam software will be downloaded from the official download site (<http://www.steampowered.com/download/hldsupdateool.bin>). Then, the License Agreement with Valve Corporation will appear. Click **Accept** to accept the license agreement to download and install the Steam client.
 - If you have already downloaded this file (hldsupdateool.bin) and have it on your local machine, select the **Install from the local machine** option to upload it. Click **OK**. Then, specify the path to the hldsupdateool.bin file and click **OK**. Click **Accept** to accept the license agreement.
 - To specify the path to an existing Steam installation, select the **Use an existing Steam client installation on your Plesk server** option and click **OK**. Locate the Steam distribution package and click **OK**.
5. All game modifications (also commonly referred to as mods) that are available for downloading are shown in a list. Each mod title is accompanied with the following icon indicating whether the mod is already installed:  - the game mod is already installed and  - game mod is not installed.

If you have a steam account that you would like to use for retrieving installation files or updates from Valve, click the **Switch Steam Account** icon, specify your username and password, and click **OK**.

Select the checkboxes corresponding to the game mods you wish to install and click **OK**.

6. When the selected game components are installed, click **OK** to quit the wizard.

Now the core components of the selected game servers are installed, and you can proceed to setting up your game servers.

Next in this section:

Setting Up a Game Server	207
Choosing Maps for the Game.....	211
Delegating Permissions for Managing Game Servers to a Panel User	212

Setting Up a Game Server

➤ *To set up a new game server:*

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Click the **Add CS Game Server** icon in the **Tools** group.
3. Select a game modification you want to run on your server. Click **Next >>**.
4. Choose the operation mode. If your server is going to be restricted to LAN clients only, select the **Server is running in LAN-Only mode** option. If you are serving both LAN and Internet clients, select the **Server is running in LAN & Internet mode** option.
5. To prevent the players connected through the Internet from cheating on your server, select the **Use Valve anti-cheat extension** option.
6. Click **Next >>**.
7. Specify the maximum number of players who can connect simultaneously to your server. Click **Next >>**.
8. Enter the name for this game server. Click **Next >>**.
9. Select how you want to configure your game server:
 - If you wish to customize the default configuration prior to running the game server, select the **Customize the default configuration prior to running the game server** option.
 - If you wish to create the game server with default configuration and run it upon completion, select the **Run the game server with the default configuration** option.
10. Click **Finish**.

The game server with optimal configuration will be set up.

If you selected the **Run the game server with the default configuration** option, the game server will run.

If you chose the **Customize the default configuration prior to running the game server**, you will be taken to the game server configuration screen on which you can adjust the following settings for your game server.

Setting	Description
Game server name	The name that you would like to call your server.
Configuration file	Select the configuration file that will be used for this game server. This drop-down list contains all configuration files available for this game mod. To edit the selected configuration file, click the Edit button on the right.

Operation mode	If your server is going to be restricted to LAN clients only, select the Server is running in LAN-Only mode option. If you are serving both LAN and Internet clients, select the Server is running in LAN & Internet mode option.
IP address	Specify the IP addresses at which the game server will be accessible.
Game server port	The port number the game server will work on. Default is 27015.
Maximum number of players	The maximum number of players who can simultaneously connect to your game server.
Game server auto update	Use this to automatically update the game server through the Internet upon each start.
Use WON authorization server	If you set up a game server in LAN without Internet access, and do not want your game server to connect to WON authorization server, leave this checkbox cleared.
Use Valve anti-cheat module	Valve Anti-cheat is the program that bans cheaters from game. The ban issued to the cheater depends on the severity of the cheat, and the number of offenses.
RCON password	Remote Console password is required if you wish to manage the game server remotely. The RCON password is also used by Parallels Plesk Panel for restarting the game server.
Game server entry password	If you wish to restrict access to your game server, specify the password that the authorized users will use for entering this game server.

Subsequently, when you need to modify these settings, you will access this screen by clicking **Extensions > Counter-Strike > game server name > Configuration tab**.

➤ **To fine tune your game server by modifying configuration files:**

1. Go to **Extensions > Counter-Strike > game server name > Configuration tab**.
2. In the **Configuration file** group, select the configuration file you need and click the **Edit** button.
3. In the **Commands** text input area, enter a list of commands. To generate the list of commands, we recommend that you use the Configuration Editor Tool available at <http://server.counter-strike.net>. To use the Configuration Editor, open <http://server.counter-strike.net/server.php?cmd=tools#> in a new browser window and click the **config editor** link in the left navigation pane. A pop-up window will open. Specify required settings and click **Configure!** at the bottom of the page. A list of commands will be generated and displayed in the **Generated Server.cfg** section of the page. Copy the generated commands to the clipboard, then return to your Parallels Plesk Panel and paste them into the **Commands** text input area.

Note: Changes made to the configuration file will affect all game servers that run on a given configuration.

4. Click **OK** to submit the changes.

➤ **To create a new configuration file:**

1. Go to **Extensions > Counter-Strike**.
2. Click the **Configuration Files** icon.
3. Click the **New Configuration** icon.
4. Enter the mod name, configuration name (not the file name!) in the **Name** field, and a description of this configuration file that will be displayed in the list of game servers.
5. In the **Commands** text input area, enter a list of commands. To generate the list of commands, we recommend that you use the Configuration Editor Tool available at <http://server.counter-strike.net>. To use the Configuration Editor, open <http://server.counter-strike.net/server.php?cmd=tools#> in a new browser window and click the **config editor** link in the left navigation pane. A pop-up window will open. Specify required settings and click **Configure!** at the bottom of the page. A list of commands will be generated and displayed in the **Generated Server.cfg** section of the page. Copy the generated commands to the clipboard, then return to your Parallels Plesk Panel and paste them into the **Commands** text input area.
6. Click **OK** to submit your configuration.
7. If you wish to apply this configuration to a game server at this time, go to **Extensions > Counter-Strike > game server name > Configuration tab**, select the configuration file you need in the **Configuration file** group, and then click **OK**.

➤ ***To modify a configuration file you created:***

1. Go to **Extensions > Counter-Strike**.
2. Click the **Configuration Files** icon.
3. Click the configuration name you need.
4. Modify the settings as desired and click **OK**.

➤ ***To remove a configuration file:***

1. Go to **Extensions > Counter-Strike**.
2. Click the **Configuration Files** icon.
3. Select the corresponding checkbox and click **Remove Selected**.
4. On the next page, confirm the removal and click **OK**.

Note: You cannot delete the default configuration file. You can only edit it.

Choosing Maps for the Game

➤ **To select maps that will be available for users playing a specific type of game:**

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Click the game server's name.
3. Click the **Maps** tab. The tab has two lists: the left-hand list displays all available maps and the list on the right contains all maps available for users playing on this game server.
4. To add a map to the game, move maps from the list of available maps to the list of selected maps by using the **Add >>** and **<< Remove** buttons.
5. Click **OK**.

To simplify map selection, you can sort all maps by mission types, such as saving hostages, assassination of VIP persons, planting a bomb, knife arena, team deathmatch, escape from the area, or Arctic Warfare Police. To view all maps related to the category of interest, select the category in the **Map categories** menu.

The maps for a game will be played consequently as they go in the list, starting from the default map selected in the **Default map** menu. To move a map downward or upward in the list, use the **Move Up** or **Move Down** buttons, respectively.

Note: Each game mod has a standard set of maps. If you remove such a standard map from the list of maps (do not confuse the standard map with the default map!), they will be automatically installed during updating of your game server.

Next in this section:

Adding and Removing Maps212

Adding and Removing Maps

➤ ***To add or remove maps that your game servers can use:***

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Click the **Maps Management** icon. The list of all maps for all game mods will show.
3. To view only the maps related to a specific game mod, select the respective option in the **Select the game modification** group.
4. To upload a new map, click the **Browse** button, select the map file you need (in zip or bsp file format), and then click **Upload**.
5. To remove the map you do not need, select the corresponding checkbox and click **Remove Selected**.

Delegating Permissions for Managing Game Servers to a Panel User

➤ ***To delegate permissions for managing game servers to one of your customers registered with your Parallels Plesk Panel:***




1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Click the **Game Server Operator** button.
3. On the page that opens, enter the username of a Parallels Plesk Panel user in the **Login** field.




➤ ***To revoke permissions to manage game servers from a user:***

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Click the **Game Server Operator** button.
3. On the page that opens, delete the username from the **Login** field and leave this field blank.

Starting, Stopping, Restarting Game Servers



➤ *To start, stop or restart a game server:*

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Click the  icon to stop a running game server,  to start a stopped game server and the  icon to restart it.

Alternatively, you can click a game server name. Then click the  button to run a game server, the  button to start it, and  to restart it.

Updating Game Servers

➤ *To update the game server files and components:*

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Click the **Update Game Servers** icon.
3. A page displaying all game modifications available for updating will appear. Each mod title is accompanied with the following icon indicating whether the mod is already installed:  - the game mod is already installed and  - game mod is not installed.
4. If you want to use another Steam account for updating, click **Switch Steam Account**.
5. Select the checkboxes corresponding to the game mods you want to update and click **OK**.
6. In the next step, the selected game components will be updated. When finished, click **OK** to quit the wizard.

In case of updating failure you can view the log file for details. To do this, click the link next to the operation result icon.

Removing Game Servers

➤ *To remove a game server:*

1. Click the **Extensions** shortcut in the navigation pane and, in the **Extensions** group, click the **Counter-Strike game server** icon.
2. Select the checkboxes corresponding to the game servers you want to remove, and click **Remove**. On the next page, confirm removal and click **OK**.

File Server Extension

The File Server extension enables Parallels Plesk Panel administrators to share directories on a network directly from the Parallels Plesk Panel. Using the Parallels Plesk Panel File Server, you can share access to a directory on your server, grant access to this directory to specific users or hosts, and assign read-only or write permissions for this directory. File Server uses the Microsoft SMB (Server Message Block) protocol to share resources on a Samba server for network users.

For the Parallels Plesk Panel File Server, the Samba server (version 2.2.x or 3.x) must be installed and properly configured.

Next in this section:

How to Access File Server	216
Configuring File Server.....	217
Managing Shares	219
Managing Users	220
Managing Broadcast Interfaces	221
Limiting Access to the File Server	222

How to Access File Server

➤ *To access the File Server:*

Click the **Extensions** shortcut in the navigation pane > **Samba File Server Configuration**.

The page that opens is the File Server management page from where you can perform all File Server operations. This page has five tabs: **Status**, **Shares**, **Users**, **Interfaces**, and **Access**. Each of these tabs contains tools for managing shared resources, file server properties, network interfaces, and users and computers who will have access to the shared directories.

Configuring File Server

This section describes how to perform the following operations:

- Configure the file server.
- View the current usage of shared resources.
- Refresh server statistics.
- Disable your file server.

➤ *To view the current status of your file server:*

1. Go to **Extensions > File Server > Status**.
2. In the **Current statistics** section, view whether your file server is started or stopped. The statistics on the current connections to shared directories is provided in the table with the following columns:
 - **Share**, name of the shared resource.
 - **Host**, name of the remote host currently connected to the shared directory.
 - **User**, user name who is currently connected to the shared directory.

➤ *To configure the file server:*

1. Go to **Extensions > File Server > Status > Preferences**.
2. To change the workgroup for your server on the Microsoft network, click in the **Workgroup** field and enter the name of a workgroup. If needed, edit the description in the **Description** field containing an optional description of your file server.
3. You can also configure the following security parameters for your Samba server:
 - **Authentication mode**. Select one of the following security modes:
 - **Share** - in this security mode, the user authenticates themselves separately for each share. The user sends a password along with each tree connection (share mount). Passwords are meant to be associated with each share, independent of the user.
 - **User** - this security mode is based on verifying the username and password. The server can either accept or reject the username and password combination. At this stage the server has no idea what share the client will eventually try to connect to, so it bases the accept/reject decision only on the username and password and the name of the client machine.
 - **Server** - in Server Security Mode, the Samba server receives the username and password from the client and sends a session setup request to the machine designated as the password server. If the password server is in user-level security and accepts the password, Samba accepts the client's connection. The client sends all passwords in encrypted form. This security mode requires the use of a password server (see Authentication server).

- **Domain** - in Domain Security Mode, the Samba server has a domain security trust account (a machine account) and causes all authentication requests to be passed through to the domain controllers. In other words, domain security has basically the same concept as server security mode, with the exception that the Samba server becomes a member of a Windows NT domain. This means that the Samba server can participate in things such as trust relationships.
- **ADS** - in this mode, the authentication procedure is performed through an Active Directory domain. Samba in this security mode can accept Kerberos tickets.
- **Authentication server.** If you set the security mode to either Server, Domain, or ADS, you will need to specify the password server (or the authentication server). For user and share modes, the password server is not required.

In this field, enter the NetBIOS name of the SMB server used as a password server, on which the Samba server will check the entered passwords. You can list multiple NetBIOS names separated with a space. This allows Samba to attempt a session setup request to each machine in the list in order until a server is contacted. This means that the next machine on the list is contacted only if the previous machine was unavailable.

You must use only the NetBIOS name of the password server (not the IP address), and Samba must have a way of resolving the name to an IP address in order to attempt the connection.

To create a local account for all users that access the Samba server and disable the password field, set this field to the asterisk character (*).

- **Encrypt password.** Select **Yes** if you want to store passwords used to authenticate users in encrypted form or **No** if password encryption is not required.
- **Guest account.** In this menu, select the system user whose rights will be granted to users logged on under the guest account. If you have no guest account on your server, select the **no guest account** option. If you need a guest account for anonymous users, it is advised that you select the **nobody** option.

For details on the Samba security configuration options, please refer to the relevant Samba documentation.

➤ ***To refresh data on the current connections to your file server:***



1. Go to **Extensions > File Server > Status**.
2. Click the **Refresh** button. The list of current connections and file server status will be refreshed.

➤ ***To disable your file server:***

1. Go to **Extensions > File Server > Status**.
2. Click the **Disable** button.

Managing Shares

➤ *To view the list of existing shared resources:*

1. Go to **Extensions > File Server > Shares**.
2. View the following information about each share:
 - **Name**, displays the name of the shared resource.
 - **Real path**, shows the path to the shared resource.
 - **Description**, contains the description of the shared directory as specified during its creation.
 - **W**, write permissions show whether users can add new files to this directory. The  icon means that write permissions are set for this directory. The  icon means that the directory is read-only.

➤ *To add a new shared resource:*

1. Go to **Extensions > File Server > Shares > Add New Share**.
2. In the **Preferences** group, enter the name of the shared directory, full path to the directory you want to share and its description. If you want to give write permissions for this directory to network users, select the **Writable** checkbox.
3. To select the users that will have access to the shared directory:
 - Select the **Any user** option if you want to grant access to the shared directory to all network users.
 - Select the **Selected only** option to grant access to the shared directory only to specified users. Select the users that will have access to this directory from the **Available users** list by using the **Add** and **Remove** buttons. If access is allowed for some users, they should specify their login and password to access this folder.

Note: If you want to add other users to the **Available users** list, you must first add them using the **Add New User** button on the **Users** tab. See *Managing Users* (on page 220) on how to add new users.

4. Click **OK**.

➤ *To edit the properties of a share:*

1. Go to **Extensions > File Server > Shares**.
2. Click the name of the shared directory you want to edit.
3. Change the necessary parameters.
4. Click **OK**.

Managing Users

➤ ***To view users who can have access to the shares:***

1. Go to **Extensions > File Server > Users**.
2. View users listed in a table with the following columns:
 - **Name**, displays the username.
 - **System user**, shows the system user account this File Server user belongs to.

➤ ***To add a new user to the list of available users:***

1. Go to **Extensions > File Server > Users > Add New User**.
2. Specify the following parameters:
 - **System user** - select the corresponding system user from the menu.
 - **Name** - username that will be used to access a share.
 - **Password** - password used to access a share.
 - **Password confirmation** - confirm the password.All these fields are mandatory.

Note: You can add only one File Server user for each Unix system user.




➤ ***To edit the user data:***

1. Go to **Extensions > File Server > Users**.
2. Click the user name you want to edit.
3. Change the parameters as needed and click **OK**.


Managing Broadcast Interfaces

By default, broadcast mode is disabled for all network interfaces mainly for security reasons. Broadcast mode enables sending data packets to the broadcast address. However, you can manually prevent your File Server from sending broadcast packets to specified network interfaces.



➤ *To view the list of network interfaces:*

1. Go to **Extensions > File Server > Interfaces**.
2. The list is organized as a table with the following columns:
 - **S** - an icon indicating the status of the network interface. The  icon shows that the broadcast mode for the interface is enabled, the  icon shows that the broadcast mode is disabled for this interface, and the  icon means that broadcast mode for this interface was enabled but now the interface is physically unavailable (was removed or corrupted).
 - **Interface name** - the name of the interface, for example, eth0, eth1, and so on.
 - **IP Addresses** - all IP addresses and subnet addresses that work on this interface.

➤ *To enable broadcast mode for an interface:*

1. Go to **Extensions > File Server > Interfaces**.
2. Click the  icon in the **Status** column of the table listing interfaces. The selected interface will be set to work in broadcast mode.

➤ *To disable broadcast mode for an interface:*

1. Go to **Extensions > File Server > Interfaces**.
2. Click the  or  icons in the **Status** column of the table. Broadcast mode will be switched off for the selected interface.

Limiting Access to the File Server

If you want to enhance the security of your file server, you can regulate what hosts or networks will have access to your shared resources. Connections from other hosts will be refused by your file server.

➤ ***To view all hosts and networks that have access to your file server:***

1. Go to **Extensions > File Server > Access**.
2. View the table. If the list is empty, all hosts can access your file server. This is the default option.

➤ ***To allow access to your server only from a specific range of hosts:***

1. Go to **Extensions > File Server > Access > Add New Host/Network**.
2. Enter the IP address of the host you want to allow access (for example, 123.123.123.1) or the range of hosts (for example, network address/subnet mask written as 123.123.123.0/255.255.255.0).
3. Click **OK**.

This will allow only the specified hosts to connect to the shared resources on your file server. All connections from other hosts will be refused by the file server.

➤ ***To edit the list of hosts that have access to your server:***

1. Go to **Extensions > File Server > Access**.
2. Click the address of the host in the list of allowed hosts.
3. Edit the host IP address or subnet mask (for multiple hosts) in the **Network/Host address** field.
4. Click **OK**.

➤ ***To remove an address from the list:***

1. Go to **Extensions > File Server > Access**.
2. Select the checkbox corresponding to the host address you want to remove and click **Remove**.
3. Select the **Confirm removal** checkbox and click **OK**.

Firewall Extension

Parallels Plesk Panel Firewall is an extension that protects your Parallels Plesk Panel-enabled server and private network from unauthorized access. With this extension, you can easily set firewall rules and fine tune them through a user-friendly interface.

Next in this section:

Setting Up Firewall	224
Predefined Firewall Rules Specifications	229

Setting Up Firewall

After you installed the extension, you can do the following:

- View and change the predefined rules that control connections to the following system services: Administrative control panel; Web server; FTP server; SSH server; SMTP server; POP3 server; IMAP server; mail password change service; MySQL server; PostgreSQL server; Samba file sharing server for Windows clients; VPN; domain name server; ICMP echo requests. By default, these rules allow all incoming connections to these services.
- View and change the predefined system policies that define what to do with all incoming, outgoing, and transit communications that do not match the explicitly defined rules.
- Add, change, and remove custom rules. For example, you may want to add a rule that will allow access to FTP accounts on the server in passive mode.

Next in this section:

Managing Access to System Services	224
Managing System Policies	225
Managing Custom Rules	226

Managing Access to System Services

For each system service, you can choose whether to allow or deny all incoming communications, or allow only communications coming from specific IP and network addresses.

➤ *To allow or restrict access to a service on your Parallels Plesk Panel server:*

1. Go to **Extensions > Firewall > Edit Firewall Configuration**.
2. Click the service name.
3. Do any of the following:
 - To allow all incoming connections, select the **Allow** option and click **OK**.
 - To deny all incoming connections, select the **Deny** option and click **OK**.
 - To deny access to a service from specific IP and network addresses, select the **Allow from selected sources, deny from others** option, specify the IP address or network address from which access to the selected service is allowed, and click **Add**. After you specify the required addresses, click **OK**.
4. To apply all changes to the firewall configuration, click **Activate**, and then click **Activate** again.

Managing System Policies

System policies define what to do with all incoming, outgoing, and transit communications that do not match the explicitly defined rules. The system policies are usually displayed at the bottom of the list of rules.

➤ ***To allow or deny communications of specific type:***

1. Go to **Extensions > Firewall > Edit Firewall Configuration**.
2. Click the icon to the left of the policy name you want to change. If the policy currently allows all connections, clicking this icon will prohibit all connections and vice versa.
3. To apply the changes, click **Activate**, and then click **Activate** again.

Managing Custom Rules

This section describes how to add, modify, remove custom rules, and change the order in which the rules are applied. This section also covers the steps required for enabling passive mode for FTP connections.

➤ **To add a custom rule:**

1. Go to **Extensions > Firewall > Edit Firewall Configuration**.
2. Click **Add Custom Rule**.
3. Enter the name of the new rule in the **Name of the rule** field.
4. Select one of the following communication directions: **Incoming** for the communications inbound to the server, **Outgoing** for communications outbound from this server, or **Forwarding** for communications transiting through your server in any direction.

For incoming communications you can specify the destination ports on your server, the protocol used for this communication, and the IP address the communications come from.

For outgoing communications you can specify the destination ports, destination IP address, and the protocol used for the communication.

For transit communications going through the server, you can specify the destination ports and source / destination IP addresses.

5. To specify the port number, type it into the **Add port** input box, and click **Add**. To remove a port number from an existing rule, select it from the list and click **Remove**. If the list of ports is empty, this rule will be applied to all TCP and UDP ports.
6. To specify the IP address or network address, type it into the **Add IP address or network** input box, and click **Add**. To remove an IP address or network from the list, select it in the list and click **Remove**. If the list of IP addresses is empty, this rule will be valid for all IP addresses.
7. Specify the action that will be applied to the communications that match the defined criteria: **allow** or **deny**.
8. Click **OK** to submit the rule.
9. After you have defined the required rules, click **Activate** to apply them to your system. A confirmation screen will open, in which you can preview the shell script generated to apply your rules (this might be of interest only to advanced users). Click **Activate** to apply the new configuration.

When the new configuration is being applied, the extension will check for connection with the Parallels Plesk Panel. If there are some connection problems, the Firewall extension will automatically revert to the previous active configuration in 60 seconds. Thus, if you misconfigure your firewall in such a way that access to your Parallels Plesk Panel is prohibited even for you, this wrong configuration will be automatically discarded and you will be able to access your server in any case.

Note: Unless your configuration is activated, you have a chance to discard all the rules you configured. To do this, click the **Revert to Active Configuration** button.

Under FreeBSD, all currently established TCP connections will drop when the new configuration is activated!

➤ ***To edit a custom rule:***

1. Go to **Extensions > Firewall > Edit Firewall Configuration**.
2. Click the rule name in the list of existing rules. Make necessary changes (the options are the same as when creating a new rule).

➤ ***To remove a custom rule:***

1. Go to **Extensions > Firewall > Edit Firewall Configuration**.
2. Select the checkbox corresponding to the rule you want to remove and click **Remove Selected**.

➤ ***To change the order in which your custom rules are applied:***

1. Go to **Extensions > Firewall > Edit Firewall Configuration**.
2. Click the icons **Up** or **Down** in the **Order** column. This will move the rule relatively to other rules covering the same direction (incoming communications, outgoing communications, or data forwarding).

➤ ***To enable passive mode for FTP connections on your server:***

1. Log in as "root" to the server shell over SSH.
2. Edit your ProFTPD configuration file.
 - a. Issue the command `vi /etc/proftpd.conf`.
 - b. Add the following line anywhere within the <Global> section:

```
PassivePorts 49152 65534
```
 - c. Save the file.
3. Log in to Parallels Plesk Panel as "admin", go to **Extensions > Firewall**, and click **Edit Firewall Configuration**.
4. Click **Add Custom Rule**.
5. Specify the following:
 - a. **Rule name**.
 - b. **Direction**: select **Incoming**.
 - c. **Action**: select **Allow**.
 - d. **Ports**: in the **Add port** input box, enter the value `49152-65534`. Leave the **TCP** option selected, and click **Add**.

6. Click **OK**.
7. Click **Activate**, and then click **Activate** again.

Predefined Firewall Rules Specifications

The following table lists the system services to which you can restrict access using the Firewall's predefined rules.

<u>Service name</u>	<u>Ports used by service</u>
Parallels Plesk Panel administrative interface	TCP 8443
Samba (file sharing on Windows networks)	UDP 137, UDP 138, TCP 139, TCP 445
Parallels Plesk Panel VPN service	UDP 1194
WWW 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
PostgreSQL server	TCP 5432
Tomcat administrative interface	TCP 9008, TCP 9080
Domain name server	UDP 53, TCP 53
ICMP requests	<ICMP echo request>

Watchdog (System Monitoring) Extension

The Watchdog extension is a solution that ensures that your server is clean from malware, all services are up and running and there is enough free disk space on the server.

Watchdog can monitor the following services:

- Web server providing the control panel interface
- Web server providing WWW service to users' sites
- SMTP Server (QMail)
- IMAP/POP3 Server (Courier-IMAP)
- DNS Server (BIND)
- Tomcat
- ColdFusion
- MySQL
- PostgreSQL
- SpamAssassin
- Parallels Premium antivirus

It can start, stop, and restart the services it monitors, and it can be configured to take actions depending on the stability of a service over some time period.

It can run other utilities and notify you when disk space usage has reached the specified amount.

For the purpose of monitoring services and disk space usage, Watchdog uses the monit utility. For information on the monit utility, visit the monit developers' website at <http://www.tildeslash.com/monit/>.

The Watchdog can scan the server file system for rootkits, backdoors, exploits, trojan horses and other malicious software on demand or on schedule. It can notify you by e-mail of scanning results and show reports through the control panel. It updates its security knowledge base through the Internet before each scan.

For the purpose of scanning the server for malware, Watchdog uses the Rootkit Hunter utility. For information on Rootkit Hunter, visit the Rootkit Hunter developer's Web site at <http://www.rootkit.nl>.

Next in this section:

Setting Up and Starting Watchdog Services	231
Viewing Status of System Services	238
Viewing Status of Hard Disk Drives and Connected Storage Devices	239
Viewing CPU and RAM Usage Statistics	240
Viewing Server Scanning Reports	241
Troubleshooting.....	242

Setting Up and Starting Watchdog Services

After you install the Watchdog extension, you should configure the settings common for all Watchdog services, and then switch on each specific type of service you need.

➤ *To configure Watchdog settings common for all services:*

1. Click the **Extensions** shortcut in the navigation pane > **Watchdog**. A list of Parallels Plesk Panel services will be displayed.
2. Click the **Preferences** icon in the **Tools** group.
3. Specify the following settings:
 - **Interface language.** Select the language in which Watchdog should show and send e-mail notices and alerts. By default, the language set for your Parallels Plesk Panel administrator's account is selected.
 - **Automatically refresh pages.** Leave this option selected, if you wish to have the information presented on the screens automatically updated on each poll.
 - **Monitor all services started by administrator.** Leave this option selected if you wish the extension to monitor all the Parallels Plesk Panel services that you start. If you install a new system service later on, the extension will automatically start looking after it. Clear this checkbox, if you are going to shut down some of the Parallels Plesk Panel services and you do not want the extension to bring them up automatically or bother you with any alert messages.
 - **Polling interval.** Specify the interval between service status queries in seconds.
 - **Store resource usage statistics.** Leave this option selected if you wish the system to keep reports on CPU and RAM usage for the amount of time you specify.
 - **Repeat security scanning.** Specify how often Watchdog should scan the server for malicious code.
 - **Send reports.** Specify how often Watchdog should send you consolidated reports on CPU and RAM load, monitored services, disk space partitions and security scanning results.
 - **Send e-mail to.** Specify the e-mail address where Watchdog should deliver alerts and reports. By default, the Parallels Plesk Panel administrator's e-mail address is used.
 - **Send e-mail from.** E-mail address on behalf of which the reports and alerts should be sent. By default, this e-mail address is `watchdog@your-host-name`.
 - **SMTP server for sending alerts.** Specify local or remote SMTP servers that should be used for sending alert messages. You can specify several host names or IP addresses separated by commas. Leave the **localhost** entry to use your server's SMTP service. If your Parallels Plesk Panel server is not running SMTP service, be sure to specify another remote mail server, otherwise, Watchdog will not be able to send you alerts.
4. Click **Apply** to submit the settings.

You have specified the general settings, and now you can further customize and run the Watchdog services you need: Monitoring of system services and monitoring of disk space usage require fine tuning before you can start them, however, regular security scanning requires no additional setup and therefore will start immediately after you have specified the general settings. By default, security scanning is started at 2 a.m. local time at the beginning of the specified time period.

Next in this section:

Setting Up and Starting Monitoring of System Services.....	233
Setting Up and Starting Monitoring of Disk Space Usage	235
Setting Up and Starting Security Scanning	237






Setting Up and Starting Monitoring of System Services

➤ *To specify what services should be monitored and to start monitoring:*




1. Go to **Extensions > Watchdog**.

All services controlled by Parallels Plesk Panel will be listed on the **Services** tab.

An icon in the **S** (status) column shows whether a service is currently monitored by Watchdog and it indicates the status of a service returned by the last poll:


-  - the service is not currently monitored.
-  - you started monitoring but the service has not yet been polled for its status.
-  - the service is monitored and Watchdog reports that the service is running.
-  - the service is monitored and Watchdog reports that the service is down.
-  - the service is no longer monitored by Watchdog because this service was unstable.

An icon in the **M** (Monitoring) column shows whether you set Watchdog to monitor the service and it also indicates whether the service was installed on the server and properly configured:

-  - the service is not installed or is not configured.
-  - you did not set Watchdog to monitor the service.
-  - you set Watchdog to monitor the service.

2. Specify the services that should be monitored and specify monitoring preferences:


- a. Click a service name.
- b. Select the **Monitor the service** checkbox to set the Watchdog to monitor the service.
- c. Select the **Save service statistics** checkbox if you wish Watchdog to keep the information on CPU and RAM resources used by the service, and present it in graphical reports (**Extensions > Watchdog > Statistics**).
- d. Select the **Stop monitoring the service if it frequently restarts** option, if you wish Watchdog to stop monitoring the service if it fails the specified number of times, and specify the failure ratio. Otherwise the Watchdog will bother you with alert messages each time it attempts to restart a non-responsive service. The default value of five failed attempts should be enough.
- e. Specify the time during which Watchdog will be waiting for response from the polled service in the **Connection timeout** box. Watchdog polls the service and then is waiting for response during the specified amount of time. If Watchdog receives no response, it restarts the service. If you host a great number of sites and e-mail accounts on your machine, you are recommended to set the **Connection timeout** for Qmail mail server to 120 seconds, and Apache Web server to 15 seconds, otherwise Watchdog will consider the busy services to be malfunctioning and will restart them.

- f. Review the commands that Watchdog uses to start and stop the service. It is recommended that you leave the prefilled values unchanged. You can write custom scripts that, for example, will clean up log files or send an SMS to your cell phone before actually starting the service, and specify the commands to run your scripts in the **To start the service, run the command** field.
 - g. If you are using the default commands for running the services, leave the predefined value of 60 seconds in the **Service startup time** box. If you are running custom scripts, and they take more than 60 seconds to execute, specify the required time in the **Service startup time** box. When a script is executed but does not complete its work within the specified time frame, Watchdog terminates execution of that script.
 - h. Click **OK** to submit the settings.
 - i. Repeat this procedure to configure monitoring for all services you need. If you are satisfied with the default monitoring settings we have predefined for each service, you can set Watchdog to monitor the required services by simply clicking the respective  icons in the list of services.
3. Once you have specified all services you would like Watchdog to monitor, click the **Enable** icon in the **Tools** group.

Now the services will be monitored in accordance with the settings you specified. If you decided to use the default settings, the following actions will be taken:

- All services will be automatically restarted in case of failure.
- Watchdog will stop monitoring all services failing 5 times out of 5 polls.
- Alert messages will be sent to the e-mail address specified in the Parallels Plesk Panel administrator's account on any event.

➤ ***To stop monitoring a specific service:***

1. Go to **Extensions > Watchdog**.
2. Click a  icon corresponding to the service you would like Watchdog to stop monitoring.

➤ ***To stop monitoring all services:***

1. Go to **Extensions > Watchdog**.
2. Click the **Disable** icon in the **Tools** group.

Important: Performing this action affects the whole monitoring service, meaning that not only all system services, but all disk partitions (see page 235) will stop being monitored.





Setting Up and Starting Monitoring of Disk Space Usage

➤ *To configure and start monitoring disk space usage:*



1. Go to **Extensions > Watchdog > the Disks tab.**

All connected (mounted) devices will be listed.

An icon in the **S** (status) column shows whether a hard disk partition or storage device is currently monitored by Watchdog and it indicates the current disk space usage rate:

-  - the disk drive or partition is not currently monitored.
-  - you started monitoring but the disk or partition has not yet been checked.
-  - the disk drive or partition is monitored and Watchdog reports that disk space usage has not reached the threshold you defined.
-  - the disk drive or partition is monitored and Watchdog reports that disk space usage has reached the threshold you defined and soon there will be no free space left on that disk or partition.

An icon in the **M** (monitoring) column shows whether you set Watchdog to monitor disk space usage on a storage device or disk partition:

-  - you did not set Watchdog to monitor the disk space or partition.
-  - you set Watchdog to monitor the disk space or partition.

The **Device** and **Mount point** columns show information on storage device and the partition mount point. The **Mount point** column shows hyphen (-) if a partition is no longer connected to the file system: when the partition is reconnected to the system, Watchdog will resume monitoring it.

The **Disk space usage rate** column shows the amount of disk space that can be used without drawing your attention. You can specify the amount of disk space either in percentage from total amount or in measurement units: gigabytes, megabytes or kilobytes. When the specified amount is reached, Watchdog will notify you and run the command you defined. A hyphen (-) in this column shows that the partition or device is not monitored.

The **Files number rate** column shows the amount of files or directories that can be stored on the file system without drawing your attention. The number of files or directories is limited not only by disk space, but also by the file system capacity. You can specify either the exact number of files and directories (if you know it) or a percent from the total amount. Watchdog will notify you when the specified amount is reached. A hyphen (-) in this column shows that the partition or device is not monitored.


The **Command** column shows the command that Watchdog will run when the disk space threshold is reached.

2. Specify the hard drive partitions that should be monitored and specify monitoring preferences:

- a. Click a partition or device name.
- b. Specify the amount of disk space that can be used without drawing your attention. When this threshold is reached, Watchdog will send you an alert and run the command you specified. We would recommend leaving the 80 % value selected.

- c. Specify the number of files and directories that can be created on the server without drawing your attention. When this threshold is reached, Watchdog will send you an alert. We would recommend leaving the 80 % value selected. You can specify the exact number of files, if you know the total capacity of your file system: to find it out, log in as root to the server and run the command `dumpe2fs <device name>` from shell.
 - d. Specify the command that Watchdog will run when the specified disk space threshold is reached. This can be a command to run a disk space cleaning utility like a `tmpwatch` on RedHat Linux systems.
 - e. Click **OK**.
 - f. Repeat the procedure to configure monitoring for all the partitions you need.
3. Once you have specified all partitions you would like Watchdog to monitor, click the **Enable** icon in the **Tools** group.

➤ ***To stop monitoring a specific partition:***

1. Go to **Extensions > Watchdog > the Disks** tab.
2. Click an icon  corresponding to the partition you would like Watchdog to stop monitoring.

➤ ***To stop monitoring all partitions:***

1. Go to **Extensions > Watchdog > the Disks** tab.
2. Click the **Disable** icon in the **Tools** group.

Important: Performing this action affects the whole monitoring service, meaning that not only all disk partitions, but all system services (see page 233) will stop being monitored.

Setting Up and Starting Security Scanning

➤ ***To set up and start regular security scanning:***

1. Go to **Extensions > Watchdog > the Preferences tab.**
2. Specify how often Watchdog should scan the server for malicious code in the **Repeat security scanning** menu.
3. Click **Apply**.

Security scanning will start immediately and will repeat in accordance with the settings you defined. By default, security scanning is started at 2 a.m. local time.

➤ ***To run on demand scanning:***

1. Go to **Extensions > Watchdog > the Security tab.**
2. Click the **Start** icon in the **Tools** group.

Watchdog will update its knowledge base and start scanning. Upon completion, a detailed report will be presented on the screen.

➤ ***To switch off regular security scanning:***

1. Go to **Extensions > Watchdog > the Preferences tab.**
2. Select the **disabled** value from the **Repeat security scanning** menu.
3. Click **Apply**.

Viewing Status of System Services

➤ **To view the status of Parallels Plesk Panel-managed services:**






- Click **Tools & Utilities > Services Management**. A list of Parallels Plesk Panel services will show. From that screen you can manage services and view their status.

Or




- Click **Extensions > Watchdog**. A list of Parallels Plesk Panel services will show. From that screen you can view service statuses and manage monitoring preferences.

The following information is displayed:

An icon in the **S** (status) column shows whether a service is currently monitored by Watchdog and it indicates the status of a service returned by the last poll:

-  - the service is not currently monitored.
-  - you started monitoring but the service has not yet been polled for its status.
-  - the service is monitored and Watchdog reports that the service is running.
-  - the service is monitored and Watchdog reports that the service is down.
-  - the service is no longer monitored by Watchdog because this service was unstable.

An icon in the **M** (Monitoring) column shows whether you set Watchdog to monitor the service and it also indicates whether the service was installed on the server and properly configured:

-  - the service is not installed or is not configured.
-  - you did not set Watchdog to monitor the service.
-  - you set Watchdog to monitor the service.





Viewing Status of Hard Disk Drives and Connected Storage Devices

➤ *To view the status of hard disk drives and other connected storage devices:*



1. Go to **Extensions > Watchdog > the Disks tab**.
2. View all connected (mounted) devices listed.

Note: Watchdog might not detect properly some mounted devices.

An icon in the **S** (status) column shows whether a hard disk partition or storage device is currently monitored by Watchdog and it indicates the current disk space usage rate:

-  - the disk drive or partition is not currently monitored.
-  - you started monitoring but the disk or partition has not yet been checked.
-  - the disk drive or partition is monitored and Watchdog reports that disk space usage has not reached the threshold you defined.
-  - the disk drive or partition is monitored and Watchdog reports that disk space usage has reached the threshold you defined and soon there will be no free space left on that disk or partition.

An icon in the **M** (monitoring) column shows whether you set Watchdog to monitor disk space usage on a storage device or disk partition:

-  - you did not set Watchdog to monitor the disk space or partition.
-  - you set Watchdog to monitor the disk space or partition.

The **Device** and **Mount point** columns show information on storage device and the partition mount point. The **Mount point** column shows hyphen (-) if a partition is no longer connected to the file system: when the partition is reconnected to the system, Watchdog will resume monitoring it.

The **Disk space usage rate** column shows the amount of disk space that can be used without drawing your attention. You can specify the amount of disk space either in percentage from total amount or in measurement units: gigabytes, megabytes or kilobytes. When the specified amount is reached, Watchdog will notify you and run the command you defined. A hyphen (-) in this column shows that the partition or device is not monitored.

The **Files number rate** column shows the amount of files or directories that can be stored on the file system without drawing your attention. The number of files or directories is limited not only by disk space, but also by the file system capacity. You can specify either the exact number of files and directories (if you know it) or a percent from the total amount. Watchdog will notify you when the specified amount is reached. A hyphen (-) in this column shows that the partition or device is not monitored.

The **Command** column shows the command that Watchdog will run when the disk space threshold is reached.

Viewing CPU and RAM Usage Statistics

➤ *To view the statistics on CPU and RAM usage by system services:*

1. Go to **Extensions > Watchdog > the Statistics tab.**
2. In the **Statistics presentation preferences** group, select the period and system services for which you would like to view statistics.
3. Click **Apply.**

CPU and RAM usage diagrams will be presented on the screen. The CPU Usage diagram will show the total load for all CPUs your server may have.

Viewing Server Scanning Reports

➤ *To view the report for the last system scan:*

1. Go to **Extensions > Watchdog > the Security** tab.
2. View the detailed report will be presented on the screen. If you wish to run a new scan, click the **Start** icon in the **Tools** group.

Troubleshooting

Issue: When I stop a Parallels Plesk Panel service, it starts automatically, and the extension does not seem to work properly.

Resolution: Make sure you did not remove the Parallels Plesk Panel event handlers that are required for the proper work of the extension:

```
Service started lowest (0) psaadm /usr/local/psa/admin/bin/php
/usr/local/psa/admin/bin/modules/watchdog/wd --monit-service=<new_service>
--plesk-name
Service stopped lowest (0) psaadm /usr/local/psa/admin/bin/php
/usr/local/psa/admin/bin/modules/watchdog/wd --unmonit-
service=<new_service>
--plesk-name
```

Note: If you use Debian Linux or Ubuntu Linux, the path to Watchdog's system files is `/opt/psa/admin/modules/watchdog/`.

Issue: No alerts are delivered.

Resolution: Please check if the outgoing SMTP server settings you specified are correct.

VPN Extension

Virtual Private Networking technologies allow communications between geographically distributed LAN segments over public networks. VPN message traffic passes through public networking infrastructures, such as the Internet, via secure tunnel protocols.

One of the most useful implementations of VPN is allowing access to a local network for a single remote host. For example, if a user needs to get access to a remote network from his home computer, they must establish a VPN connection.

The Parallels Plesk Panel VPN extension extends Parallels Plesk Panel with the ability to support peer-to-peer communication between two Parallels Plesk Panel hosts or between your Parallels Plesk Panel host and any other computer. At present, the Parallels Plesk Panel VPN extension supports connection to the server only from a single remote host and does not support connections from multiple hosts. The extension is based on the OpenVPN solution which uses OpenSSL for encryption and the virtual TUN/TAP driver for tunneling.

Next in this section:

Software Requirements	243
Accessing the VPN Extension	243
Setting up VPN Preferences	244
Managing Keys	245
Using Client Packages	246
Starting and Stopping a VPN Connection	247

Software Requirements

You should have one of the following operating systems to use the OpenVPN solution: Linux, Windows 2000/XP and higher, OpenBSD, FreeBSD, NetBSD, Mac OS X, or Solaris.

Accessing the VPN Extension

➤ *To access the Parallels Plesk Panel VPN extension:*

Click the **Extensions** shortcut in the navigation pane > **Virtual Private Networking**.

If you access the extension for the first time, the first page that opens is the VPN Preferences page (on page 244). You cannot get access to other VPN extension options unless you specify the preferences for your VPN connection.

Setting up VPN Preferences

➤ *To set up a VPN connection:*

1. Go to **Extensions > Virtual Private Networking**.
2. On the **Preferences** page that opens, specify the following parameters:
 - **Remote Address**, enter the host name or the IP address of the host you want to communicate to. Leave this field blank if you wish the other party to be able to connect to your server from different addresses or if the remote IP address is not known in advance. Note, however, that one server cannot be involved in simultaneous communication with two or more remote hosts.
 - **Remote UDP port**, specify the port on the remote host to which UDP packets from this server will be sent. The default port is 1194. Note that though VPN uses only UDP for the encrypted traffic flow, all IP protocols, including TCP, are supported over the virtual private network. You can leave this field blank if you have not specified the remote address above.
 - **Local UDP port**, your server will listen for incoming VPN traffic on this local UDP port. The default port is 1194. You can leave this field blank if you do not want to allocate a specific port, but in that case you must specify the remote address and port fields above to allow the local host to be the initiating party.
 - **Local peer address** and **Remote peer address**, two hosts connected by a VPN channel need to have a pair of virtual network interfaces to route the traffic through. You need to assign two IP addresses to them, one for each side of the VPN circuit. These IP addresses should be chosen from some private address spaces and it is important that they should not overlap with any of the IP addresses present within the local networks on either side of the tunnel. These two addresses must differ only in the two least significant bits. You can pick .1 and .2 for the last octets, for example. Note that the default values are only an illustration! Always check the real configuration of your network so that you do not run into IP collision problems.
3. Click **OK**.

Note: The Parallels Plesk Panel VPN extension is initially disabled. To use the VPN functionality, enable the extension by clicking the **Enable** button.

Managing Keys

To establish a VPN connection between your Parallels Plesk Panel server and a remote host, both sides must have the same cryptographic key. This key is required for authentication and encryption of your traffic, ensuring that your communications cannot be eavesdropped or interfered by a third party. Do not forget to share the same key between both communicating parties each time you generate or upload a new key.

A cryptographic key is generated automatically and saved to a special directory during extension installation. However, you might want to replace the initial key with the new one.

➤ ***To generate a new VPN key:***

1. Go to **Extensions > Virtual Private Networking**.
2. Click **Generate Key**. The new key will automatically replace the existing key.

Note: After the new key is generated, your old key will become invalid. In order to continue communication, you must share the new key with the other communicating party.

➤ ***To save the generated key to your local machine:***

1. Go to **Extensions > Virtual Private Networking > Download Key**.
2. Save the key to a specified location on your disk.

You can then transmit this key file to another host on removable media or through another secure way.

➤ ***To upload a cryptographic key that you received from another machine:***

1. Go to **Extensions > Virtual Private Networking > Upload Key**.
2. Specify the location of the key file and click **OK**.

This way of key management is especially useful if you are establishing a VPN connection between two Parallels Plesk Panel-enabled servers. If the remote host does not have Parallels Plesk Panel, it is more convenient to use client packages (on page 246).

Using Client Packages

To simplify the task of connecting a non-Plesk host to your Parallels Plesk Panel server, Parallels Plesk Panel supplies preconfigured client packages containing configuration files and the cryptographic key for the other party. The contents of the archives are specifically tailored to the preferences you have specified earlier.

- If your user is running Windows, click **For a Windows Client** to download and save the client package on your local machine.

The client package is a ZIP archive that contains the following files:

- `Install TAP device.bat` - installs the TAP driver on your computer.
- `Uninstall TAP device.bat` - removes the TAP driver from your computer.
- `Connect to VPN.bat` - establishes a VPN connection.
- `System folder` - contains the cryptographic key and your VPN preferences.

To install and uninstall the TAP drivers, you must have Windows administrator rights on your computer.

To install the TAP driver, run the `install TAP device.bat` file. After the driver is installed, you can establish a VPN connection to the Parallels Plesk Panel-enabled server by running the `connect to VPN.bat` file. The OpenVPN software itself is contained within the client package and does not require any installation or removal procedures.

- If your user is running Unix, click **For a Unix client** to download and save the client package on your local machine.

The package contains the `openvpn.conf` file with your current VPN preferences and the `vpn-key` file that is a cryptographic key for your VPN connection. If you are using this package, OpenVPN (version 2.0) must be already installed on the client machine. For smooth operation, we advise that you use OpenVPN 2.0 beta 11 as the extension was tested on this beta version.

If the preferences on the Parallels Plesk Panel server change or a new key is generated or uploaded to the Parallels Plesk Panel server, the client packages must be downloaded again because they include your current key and existing VPN preferences.

Starting and Stopping a VPN Connection

➤ ***To enable a VPN connection from Parallels Plesk Panel:***

1. Go to **Extensions > Virtual Private Networking**.
2. Click **Enable**.

➤ ***To disable a VPN connection from Parallels Plesk Panel:***

1. Go to **Extensions > Virtual Private Networking**.
2. Click **Disable**.

If you want to disable a VPN connection on a Windows client, close the **Connect to VPN** dialog box that appeared when you established your connection. When the Windows user logs out, the VPN connection shuts down as well.

Panel Updates and Upgrades

Panel is constantly evolving in terms of functionality, and new security enhancements are introduced with each update. To ensure that your Panel software is up-to-date, we recommend that you switch on automatic updates.

There is also the option to upgrade Panel to the latest versions. While *updates* include some minor fixes for Panel, *upgrades* introduce more complex changes in product functionality.

The information about the current Panel version and available updates and upgrades is always displayed in the **System Overview** group of the **Home** page.

Panel Versioning

The full Panel version identifier consists of a number of fields. For example, the identifier *Panel 10.3.0 Update #12 General release* appears as follows.

Version number			Update	Release tier
Major	Major	Minor		
10	3	0	12	General release

Information about how updates (on page 249) and upgrades (on page 251) affect these fields is provided next in this section.

Note: By default, Panel updates and upgrades are downloaded from the official update server. Learn how to install updates and upgrades from other locations in the section **Changing the Updates/Upgrades Source** (on page 253).

In this chapter:

Panel Updates.....	249
Panel Upgrades	251
Changing the Updates/Upgrades Source	253
Reporting Upgrade Problems	254

Panel Updates

Updates are fixes that enhance Panel security and stability. There are four types of update:

- *Security updates.*
These updates address security vulnerabilities. Such vulnerabilities may be exploited by hackers attempting to get access to your server. We strongly recommend that you apply security updates as soon as possible. Panel always warns you about missed security updates on the **Home** page.

Note: Some security updates that Parallels considers to be mandatory are applied automatically, regardless of your update policy.

- *Important updates.*
These are updates that significantly improve Panel reliability. We strongly recommend that you apply such updates once they become available.
- *Recommended updates.*
Recommended updates improve the overall stability or introduce enhancements developed after the Panel release.
- *Optional updates.*
These are minor fixes and enhancements that do not have any serious impact on your work in Panel and do not require immediate installation.

Updates are distinguished by types only for your convenience; the update type just indicates the urgency of applying an update. For example, a security update should be applied as soon as possible, while an optional update can be installed at any convenient time.

Applying Panel Updates

Updates can be applied only to a current Panel version. Thus, Panel does not change its version after an update; information about the applied update is just added to the product version name, for example, *Panel 10.3.0 Update #12*. Updates are free of charge and are available for all Panel installations, regardless of their license key.

You can update Panel in two ways:

- *Manually* from the **System Overview** group of the **Home** page. This page contains information about the latest available update, including its type and a link for applying the update.
- *Automatically (recommended)*. If you activate automatic updates at **Tools & Settings > Update and Upgrade Settings**, Panel will check for updates once a week. If updates are available, Panel automatically downloads and installs them.

Note: Panel updates are applied sequentially. Therefore, you cannot install only a specific update or skip one of the updates.

Updating Third-party Panel Components

Panel is shipped with a number of third party components such as MySQL, Postfix, and so on. As well as Panel itself, these components require updating with time. You can automate this process by turning on automatic updates for third-party components. In this case, the components will be updated together with Panel (Updates for shipped components are included into Panel updates).

Warning: Use such automatic updates with care. Websites hosted on your server may be incompatible with newer versions of certain components. This is why automatic updates of third-party components are turned off by default.

➤ ***To turn on/off automatic updates for third-party components:***

1. Select or deselect the option **Automatically install updates for third-party components (such as MySQL, PHPMyAdmin, and others)** on the **Tools & Settings > Update and Upgrade Settings** page.

Panel Upgrades

Upgrades always bring a significant number of Panel enhancements or even introduce new Panel features and behavior. After an upgrade, Panel increases its major or minor version:

- Typically, if an upgrade only improves the existing functionality, then Panel increments its minor version number (e.g. from 10.3.0 to 10.3.1).
- If an upgrade includes more complex changes in Panel, then the major version number is incremented (e.g. from 10.3.1 to 10.4.0).

Panel Upgrades and Release Tiers

During its lifecycle, each major Panel version passes through a number of development stages (see the diagram below). It is natural that in earlier stages, some newly implemented features may not be in their final state and may require some further modification. The functionality of such features in subsequent Panel versions is improved as they receive more customer feedback over time. To indicate the stage of the current Panel version, we assign one of the following release tiers to it: *Testing release*, *Early Adopter release*, *General release*, and *Late Adopter release*.

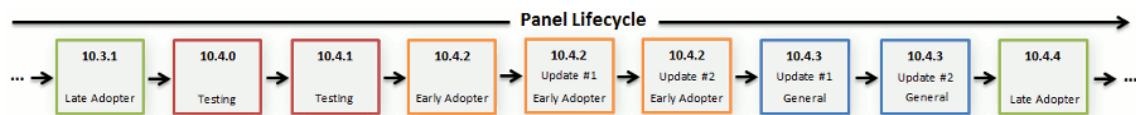
Notes:

1. By default, testing builds are not shown as available for installation. You can install the testing Panel version only by running Parallels Installer with one of the special options. Learn more in the **Installation, Upgrade, Migration, and Transfer Guide**, in the chapter **Installing Panel**.
 2. Upgrade to the next testing release is available only to the owners of a testing build. Subsequent Panel builds do not have the corresponding option in the GUI.
-

The decision on what tier to use is absolutely up to you. For example, consider upgrading to the early adopter release if you want to try new features before Panel becomes generally available. On the other hand, if you want to get the solution that has received all major updates and is being successfully used by a number of service providers, wait until Panel gets the late adopter release status (which may be a couple of months after the general release).

Once you have decided what version you need, set up Panel to notify you when upgrades to the chosen version become available. After you select the version type in **Tools & Settings > Update and Upgrade Settings**, Panel will check for upgrades once a day. When an upgrade with the selected release tier becomes available, Panel will notify you on the **Home > System Overview**. Note that Panel always notifies you when a version with a "higher" release tier becomes available. For example, if you set Panel to notify you about early adopter releases, you will still receive all upgrade notifications about general and late adopter releases. However, if you decide to use only late adopter releases, notifications for all early adopter and general release upgrades will be skipped.

The diagram below shows the rough Panel lifecycle (the version numbers are given only as examples and have no correlation with the real ones).



Applying Panel Upgrades

As upgrades imply multiple changes in the product and may require significant downtime, Panel does not apply them automatically. Instead, it displays upgrade notifications on the **Home** page. Once you receive such a notification, you can initiate the upgrade either from **Home > System Overview** or **Tools & Settings > Updates and Upgrades** at any time that suits you.

The scenario described above is called in-place upgrade as Panel components are updated within one server. However, there is another way to upgrade Panel - *upgrade by transfer*. This way implies transferring Panel data to another server with a later version of Panel. Upgrade by transfer is suitable, for example, when you want not only to upgrade Panel but also to move it to a more productive server or another operating system. To learn more about differences between upgrade ways and get detailed instructions on upgrading Panel, read the **Installation, Upgrade, Migration, and Transfer Guide**.

Panel Upgrades and License Keys

Note that some Panel licenses do not grant permission to perform complex upgrades (upgrades that change the major version number: e.g. from 10.3.1 to 10.4.0). If you attempt to perform such an upgrade, Panel will warn you about license limitations. Nevertheless, you will still be able to perform the upgrade. When it is finished, you will need to obtain and install the license key for the new Panel version. For more information about installing a license key after an upgrade, refer to the section **Upgrading Your License Key** (on page 142).

Notes on the In-Place Upgrading Procedure

- After upgrading to a new Panel version, you will receive a report on the upgrade procedure. The notification message will include the event log and a list of installed packages if the upgrade has been successful. However, you may not receive any error notice if your mail server fails. In this case you can check for errors in the `autoinstaller3.log` file located in the `/tmp` directory on the server hard drive.
- All Panel operations are suspended during installation of the so-called *base* packages that affect the Panel's core functionality.
- Starting from 10.3, Panel provides the ability to install alternative component versions (PHP 5.3, MySQL 5.5, etc.) directly from the **Updates and Upgrades** page.

Changing the Updates/Upgrades Source

By default, updates and upgrades for Parallels Plesk Panel and your operating system are downloaded from the official updates server at <http://autoinstall.plesk.com>.

➤ ***If you want to receive Parallels Plesk Panel updates from another location on the network:***

1. Go to **Tools & Settings > Updates**. Updater will open in a new browser window or tab.
2. If Updater starts downloading updates and you would only like to change settings at the moment, click **Cancel**.
3. Click **Updates source and installation settings**, and specify the source of update packages:
 - By default, the **Official Parallels Updates server** is selected. Specify the location where the installation files will be stored. By default, the installation files are stored in the `/root/parallels` directory.
 - If you select **Mirror server**, specify the `.inf3` file location in the **URL to the directory with .inf3 file field**. Specify the location where the installation files will be stored. By default, the installation files are stored in the `/root/parallels` directory.
 - If you select **Local media**, specify the `.inf3` file location in the **Absolute path to the .inf3 file field**.
4. If you use a proxy server, select the **Connect using a proxy** checkbox and specify the following settings:
 - Specify proxy host name and port number in the **Proxy address** and **port** fields.
 - If this proxy server requires authentication, select the **Require authentication** checkbox and specify username and password.
5. Click **Save** to save the settings.

Reporting Upgrade Problems

During Panel installation or in-place upgrade, Parallels Installer captures all the problems it encounters and sends them to Parallels. These reports do not contain any personal or sensitive information. Our technical experts analyze and resolve these problems making future installations and upgrades more reliable.

It is up to you whether to let Parallels Installer submit problem reports to Parallels. The Installer asks your decision during the first installation or in-place upgrade and remembers it for the Panel lifetime. If you decide to stop sending the reports to Parallels, run the Installer with the following option:

```
<full path to Parallels Installer> --disable-feedback
```

To start submitting the reports, use:

```
<full path to Parallels Installer> --enable-feedback
```

Statistics and Monitoring

In this chapter:

Action Logs	256
Viewing Statistics	259
Server Health Monitor	266
Monitoring Connections to Panel.....	269

Action Logs

You may wish to keep track of actions performed by various users in the system. All actions will be recorded in a log file that you will be able to download for viewing. The following system events (actions) can be logged:

- Administrator information changed
- System service restarted, started, or stopped
- IP address added, removed, changed
- Login settings (allowed period of inactivity for all user sessions in the control panel) changed
- Customer account created, deleted, personal or system information changed
- The status of customer account changed (suspended/activated)
- Customer's interface preferences changed
- Customer's IP pool changed
- Web applications were added to or removed from a customer's pool
- The limit on disk space is reached for a customer account
- The limit on traffic usage is reached for a customer account
- The limit on disk space is reached for a website
- The limit on traffic usage is reached for a website
- Website created, deleted, settings changed
- Website owner changed
- Website status changed (suspended/activated)
- DNS zone updated for a website
- Subdomain created, deleted, settings changed
- Domain alias created, deleted, settings changed
- DNS zone of the domain alias changed
- Resource allotments were changed for a customer account
- Customer's permissions for operations were changed
- Resource allotments were changed for a website
- Users logged in and out of the Panel
- Mail accounts created, deleted, changed
- Mailing lists created, deleted, settings changed
- Website hosting set up, deleted, changed
- Web forwarding hosting accounts were created, deleted, reconfigured
- Web application installed, reconfigured, uninstalled
- Web application package installed, uninstalled, updated
- License key expired or updated
- Database server created, deleted, updated
- Database created or deleted

- Database user account created, deleted, updated
- Customer's GUID updated
- Domain's GUID updated
- Parallels Plesk Panel component was updated or added

Next in this section:

Setting Up Action Logging.....	257
Downloading the Action Log	257
Clearing the Action Log.....	258

Setting Up Action Logging

➤ *To set up action logging:*

1. Go to **Tools & Settings > Action Log** (in the **Logs & Notifications** group).
2. In the **Logged actions** group, select the actions to be logged using the checkboxes.
3. In the **Store records in the database** field, specify the action log cleaning options: on a daily, weekly or monthly basis, or in accordance with the specified number of records stored in the database.
4. To retain all action log records, select the **Do not remove records** option.
5. To apply all the changes made, click **OK**.

Downloading the Action Log

➤ *To download the action log to your machine:*

1. Go to **Tools & Settings > Action Log** (in the **Logs & Notifications** group).
2. In the **Log files** section, select the time period using the drop-down boxes, and click **Download**.

The dialog window will open, prompting you to select the location for the downloaded log file to be saved to.

3. Select the location, and click **Save**.

Clearing the Action Log

➤ *To clear the action log:*

1. Go to **Tools & Settings > Action Log** (in the **Logs & Notifications** group).
2. In the **Log files** section, click **Clear Log**.

Viewing Statistics

➤ **To view the information on usage of server resources:**

1. Go to **Tools & Settings > Server Information**.

The following information will be presented:

- Processor information.
- Parallels Plesk Panel version and build number.
- Operating system and its kernel version.
- Parallels Plesk Panel license key number.
- Server uptime.
- Processor load averages for the last 1 minute, 5 minutes and 15 minutes.
- The amount of RAM installed and used.
- The amount of swap space used.
- Hard disk usage by partitions and directories.
- The connected (mounted) storage and network storage devices.
- The number of hosted domains: **active** shows the domains that are online; **problem** shows the domains that have exceeded the disk space and bandwidth allotments but still online; **passive** shows the domains that are offline because they were suspended by you or your resellers.

2. Click **Refresh** to update the server statistics with the latest data.

➤ **To view a report on resource usage by your resellers, customers, and websites:**

1. Go to **Tools & Settings > Summary Report**.

2. To view a summary on bandwidth usage by months, click **View Traffic History**.

Operations on reports:

- To get more details, select the **Full Report** option from the drop-down menu.
- To adjust the amount of information presented in a report, edit an existing report template or create a new one. To edit a template, click **Properties**, and then modify the report template.

To create a new template, go to **Report Layouts > Create Report Layout**, and specify how much information you want in each section of the report: select **None** if you do not want any information, select **Summary** if you want a concise overview, or select **Full**, if you need a detailed report. Select the **Use as default report** checkbox and click **OK**.

To delete a custom report layout, select the checkbox corresponding to the report layout name and click **Remove**.

- To print the report, click **Print**. A report will open in a separate browser window. Select the **File > Print** option from the browser's menu to print the report.

- To send the report by e-mail, type the recipient's e-mail address into the input box located to the right of the Report group and click **Send by E-Mail**. If you are the recipient, then you do not need to specify an e-mail address: the system assumes by default that you are the report recipient and specifies your e-mail address registered with your Panel account.
- To have the reports automatically generated and delivered by e-mail on a daily, weekly, or monthly basis, click **Delivery Schedule** and follow the instructions supplied in the section Automating Report Generation and Delivery by E-mail (on page 260).

➤ **To view a report on traffic usage by users and sites:**

1. Click **Tools & Settings**.
2. Do any of the following:
 - To view reports on the amount of traffic used by resellers, click **Traffic Usage By Resellers** (in the **Resources** group).
 - To view reports on the amount of traffic used by all resellers and customers, click **Traffic Usage By Users** (in the **Resources** group).
 - To view reports on the amount of traffic used by domains (websites), click **Traffic Usage By Domains** (in the **Resources** group).

Next in this section:

Automating Report Generation and Delivery by E-mail	260
Viewing Virus and Spam Protection Statistics (Windows)	261
About Disk Space Usage Calculation	262

Automating Report Generation and Delivery by E-mail

➤ **To schedule a report delivery on a regular basis:**

1. Go to **Tools & Settings > Summary Report > Delivery Schedule**.
2. Click **Add Report Delivery Schedule**.
3. To send reports to your e-mail address registered with the system, select the **the server administrator** value from the **Deliver to** menu. To send reports to another e-mail address, select the **the e-mail address I specify** option and type the e-mail address.
4. In the **Delivery frequency** menu, select how often the report should be sent: daily, weekly, or monthly.
5. Click **OK**.

Viewing Virus and Spam Protection Statistics (Windows)

➤ *To view the information about viruses detected and removed by Kaspersky Antivirus:*

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group) > **Statistics** tab, and click **Virus Statistics**.
2. Select the period for which you want to view virus statistics.

If you want to view more detailed information about viruses, or e-mail addresses of e-mail senders or recipients, click the respective tab.

➤ *To view the information about spam messages detected and filtered by SpamAssassin:*

1. Go to **Tools & Settings > Mail Server Settings** (in the **Mail** group) > **Statistics** tab, and click **Spam Statistics**.
2. Select the period for which you want to view spam statistics.

If you want to view more detailed information about spam message recipients, click the **Recipients** tab.

About Disk Space Usage Calculation

When a Panel user creates a subscription or a webspace, Panel starts calculating disk space usage for this entity. The disk space that can potentially be consumed is categorized into the following types:

- (Always included) Website, FTP, and web users' content.
- Log files and statistic reports.
- Databases.
- Mailboxes.
- Java applications.
- Mailing lists.
- Subscription backup files.
- Subscription backups that are a part of server-level backups.

This section explains how Panel calculates disk space usage for each of these categories on Linux and on Windows. If you would like to include or exclude options from disk space calculation, you can do it on the **Tools & Settings > Server Settings** page.

The total disk space usage is available in **Tools & Settings > Summary Report**. The summary report shows the sum of disk space consumption of all subscriptions and webspaces. If you would like to view the disk space usage per subscription, go to **Subscriptions** and click a subscription name.

Variables

Next in this section we use the following variables to simplify the description:

- *HTTPD_VHOSTS_D*. This is the absolute path to the directory with virtual hosts.
- *CATALINA_HOME* is the absolute path to the Tomcat installation directory.
- *PRODUCT_ROOT_D* is the absolute path to the Panel installation directory.
- *PLESK_MAILNAMES_D* is the absolute path to the directory with mailboxes.
- *PGSQL_DATA_D* and *MYSQL_VAR_D* is the absolute path to the directory with MySQL and PostgreSQL databases correspondingly.

The variable values depend on the operating system. On Linux, you can find the values in `/etc/psa/psa.conf`.

Website Content, Anonymous FTP Content, Web Users' Content

This category of content is always included in the calculation of disk space usage.

On Windows, the size of website content is the total size of the

`"%plesk_vhosts%\<domain_name>"` directory excluding these directories:

`"%plesk_vhosts%\<domain_name>\anon_ftp"`

`"%plesk_vhosts%\<domain_name>\<subdomain_name>\anon_ftp"`

```
"%plesk_vhosts%\<domain_name>\.plesk\statistics"
"%plesk_vhosts%\<domain_name>\<subdomain_name>\.plesk\statistics"
"%plesk_vhosts%\<domain_name>\web_users"
"%plesk_vhosts%\<domain_name>\<subdomain_name>\web_users"
```

On Linux, the size of website content is the total size of the following directories:

```
HTTPD_VHOSTS_D/<domain_name>/cgi-bin
HTTPD_VHOSTS_D/<domain_name>/error_docs
HTTPD_VHOSTS_D/<domain_name>/httpdocs
HTTPD_VHOSTS_D/<domain_name>/<subdomain_name>
HTTPD_VHOSTS_D/system/<domain_name>/pd
```

On Windows, the size of anonymous FTP content is the total size of the following directories:

```
"%plesk_vhosts%\<domain_name>\anon_ftp"
"%plesk_vhosts%\<domain_name>\<subdomain_name>\anon_ftp"
```

On Linux, the size of anonymous FTP content is the total size of the following directories:

```
HTTPD_VHOSTS_D/<domain_name>/anon_ftp
```

On Windows, the size of web users' content is the total size of the following directories:

```
"%plesk_vhosts%\<domain_name>\web_users"
"%plesk_vhosts%\<domain_name>Error! Hyperlink reference not valid."
```

On Linux, the size of web users' content is the total size of the following directories:

```
HTTPD_VHOSTS_D/<domain_name>/web_users
```

Note: Starting with Panel 11.5, if the directories mentioned above contain hard links, Panel includes the size of each link in calculation only once, disregarding the number of the link instances.

We will refer to the total of website, FTP, and web users' content as *WEB_CONTENT* in the formula for calculation the total disk space usage.

Log Files and Statistic Reports

On Windows, the size of logs and reports is the total size of the following directories:

```
"%plesk_vhosts%\<domain_name>\.plesk\statistics"
"%plesk_vhosts%\<domain_name>\<subdomain_name>\.plesk\statistics"
```

On Linux, the size of logs and reports is the total size of the following directories:

```
HTTPD_VHOSTS_D/system/<domain_name>/statistics
```

We will refer to the total logs and reports size as *LOG_AND_STAT* in the formula for calculation the total disk space usage.

Databases

The size of databases is calculated per website and then summed to obtain the total size.

On Windows, the size of MySQL databases is the sum of data length and index length in the following query: *SHOW TABLE STATUS FROM <db_name>*.

To get the size of MS SQL databases, the system runs the query *exec sp_databases* for each database under a particular website. The results are summed and multiplied by 1024.

On Linux, the size of PostgreSQL databases is the total size of directories `PGSQL_DATA_D/base/db_oid`. Here *db_oid* stands for OID of a database under a certain website.

On Linux, the size of MySQL databases is the size of the directory `MYSQL_VAR_D/db_name`. Here *db_name* stands for a database name under a certain website.

We will refer to the total databases size as *DATABASES* in the formula for calculation the total disk space usage.

Mailboxes

The size of mailboxes per website is the total size of directories corresponding to mailboxes. The path to a mailbox depends on a message transfer agent (for example, MailEnable).

- (Windows, MailEnable) *mailbox_dir* \<domain_name>\MAILROOT*mailbox_name*. The *mailbox_dir* is stored in the Windows registry `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mail Enable\Mail Enable\Connectors\SF`.
- (Windows, SmarterMail) *mailbox_dir* \Users*mailbox_name*. The *mailbox_dir* is obtained by calling the *GetDomainSettings* method of the *svcDomainAdmin* web service.
- (Linux) `PLESK_MAILNAMES_D/<domain_name>`.

We will refer to the total mailboxes size as *MAILBOXES* in the formula for calculation the total disk space usage.

Java Applications

On Windows, the total size of Java applications is the size of the directory `CATALINA_HOME\psa-wars\domain_name`. Here *CATALINA_HOME* is the value of the *InstallPath* parameter in the Windows registry, in `HKLM\SOFTWARE\Apache Software Foundation\Tomcat\<Tomcat_version>`.

On Linux, the directory with Java content is `CATALINA_HOME/psa-wars/<domain_name>`.

We will refer to this total as *JAVA_APPS* in the formula for calculation the total disk space usage.

Backup Files

On Linux, the size of backups is obtained from the following utility call:

```
PRODUCT_ROOT_D/admin/bin/pmm-ras --get-domain-dumps-disc-usage
--domain-guid <domain_guid> --session-path
PRODUCT_ROOT_D/PMM/logs
```

If the administrator specifies to exclude website backups nested in server-level backups from user quota, the utility is run with an extra option, `--skip-server-dumps`.

On Windows, the size of backups is cached and is the sum of numbers that follow `size_` in file names `size_XXXXXX`. These `size_` files are stored in `"%plesk_dir%\Backup\backups_dir\<domain_name>\.discovered*\\"`.

The `backups_dir` is:

`/domains` – if the backups are owned by the administrator.

`/resellers/<reseller_username>/domains` - if a website is owned by a reseller.

`/resellers/<reseller_username>/clients/<customer_username>/domains` - if a website is owned by a customer of some reseller.

`/clients/<customer_username>/domains` – if a website is owned by a customer directly under the administrator.

If the file

`"%plesk_dir%\Backup\dumps_dir\<domain_name>\.discovered*\ownertype_server"` exists then the size of website backups nested in server-level backups is not added to the disk space usage.

We will refer to the backups size as *BACKUPS* in the formula for calculation the total disk space usage.

Calculating the Total Disk Space Usage

The formula for calculating the total disk space usage is as follows:

TOTAL = WEB_CONTENT

+ ***LOG_AND_STAT*** (if the **log files and statistic reports** option is selected in **Tools & Settings > Server Settings**)

+ ***DATABASES*** (depends on the **databases** option on Linux and **MySQL databases** and **Microsoft SQL databases**)

+ ***MAILBOXES*** (if the **mailboxes** option is selected)

+ ***JAVA_APPS*** (if the **Java applications** option is selected)

+ ***BACKUPS*** (if the **domain backup files** option is selected; the value depends on **backup files created by the administrator**)

Here placeholders (for example, *WEB_CONTENT*) stand for the totals of respective categories

Server Health Monitor

Generally, as time goes by, Panel server resources become more and more utilized: The number of Panel users grows; customers create new sites that use different system services, and so on. This means that at some point you can experience the lack of system resources, such as RAM, CPU performance, or disk space. To keep you notified about the server resources usage, we offer the component - Health Monitor. Based on its statistics, you can promptly decide what services should be adjusted to lower the system resources usage or what hardware components require an upgrade.

Health Monitor is an additional Panel component that tracks all main server health parameters, such as: Memory and CPU usage by different services, hard disk utilization, number of running processes, and so on. Besides, Health Monitor can be configured to make visual and e-mail notifications when a certain health parameter exceeds some threshold.

This section provides the detailed information on how to install and configure Health Monitor as well as to get statistics on a resources usage.

Next in this section:

Installing Health Monitor	266
Tracking Server Health.....	266
Accuracy of Health Monitor Values.....	268
Configuring Alarms, Trends, and E-mail Notifications.....	268
Updating Health Parameters After Hardware Change	268

Installing Health Monitor

Health Monitor is an additional component that is provided with Panel by default. You can install it during the Panel custom installation or add it later using the **Server Management > Tools & Settings > Updates**.

Tracking Server Health

Health Monitor displays the information on server resources usage in two ways:

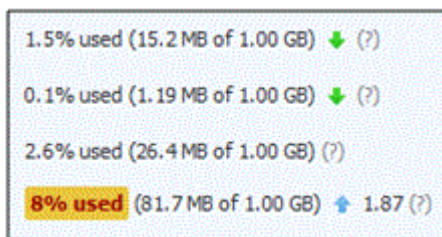
- A summary report on all main health parameters.
- A detailed report with graph of changes for each health parameter.

Summary Report

The summary report contains the information on all main server health parameters that are grouped for the sake of convenience. The report displays the status of each group, the instantaneous parameter values and their trends. To get the Health Monitor summary report, go to the **Server Administration Panel > Home > Server Health**.

Note that the summary report shows you *instantaneous* parameters values that are relevant only for the moment when the Home page was refreshed.

The example of summary report (random values) is shown below.



Yellow and Red Alarms

As you can see, one of the parameters exceeded some threshold and Health Monitor alarmed about it with the yellow highlighting. There are two types of alarms for each parameter:

- Yellow alarm - a parameter is close to its critical value.
- Red alarm - a parameter exceeds its critical value.

The threshold of these alarms can be set using the configuration file.

Trends

Health Monitor can also warn you if one of the parameters grows too fast. This is done with the help of trends. Trend is a way to show how a parameter value changes over time. In this example, the parameter, which was the source of the alarm increased (↑) for the last hour by 1.87 times comparing to the hour before (the default trend interval is one hour). If a parameter value is insignificant, its trend is not shown.

Detailed Report

Detailed report can help you find out the time periods when the resources usage is maximal (minimal). To view the report, go to the **Server Management > Health Monitoring**. To see how server health parameters have been changing over time, select the corresponding checkboxes. You can select a period for which the graph is generated: From the past 3 hours to a week.

Note that the parameters values behind the graph are also *instantaneous* and are relevant only for the moment when the page was refreshed.

Accuracy of Health Monitor Values

Note that Health Monitor shows *instantaneous* parameter values. These values are relevant *only* for the moment when the web page, which contains them, was refreshed. This means that if your server is permanently loaded, you will never see the conformity between Health Monitor and a system resource usage monitor (for example, **top** in Linux or **Task Manager** in Windows).

Configuring Alarms, Trends, and E-mail Notifications

After the installation, Health Monitor works with all parameters by default. If you want to adjust some of its options, such as alarm thresholds and e-mail notifications, you should perform the component configuration. Such configuration is available using the XML file.

➤ *To configure Health Monitor:*

1. Download the current configuration file by clicking the **Download Configuration File** button in **Server Management > Health Monitoring**.
2. Change the configuration file in any text editor. With the help of this file you can define:
 - Alarm threshold for each parameter.
 - Type of the alarm for each parameter: Exceeding of an absolute value, a relative value, or a trend value.
 - Trend calculation parameters.
 - E-mail notification parameters.
The detailed file structure and description for each of the file parameters is provided in the top of the configuration file.
3. Upload the file with changes to Panel by clicking the **Upload Configuration File** button in **Server Management > Health Monitoring**.

Updating Health Parameters After Hardware Change

Note that the hardware configuration of your Panel server is specified in Health Monitor just once - during component installation. Further changes in hardware parameters are not propagated to Health Monitor. For example, if you increase the amount of RAM from 1 GB to 2 GB, Health Monitor will continue to show that the total RAM is 1 GB. To update Health Monitor data on server configuration, use **Server Management > Health Monitoring > Detect Hardware Changes**.




Monitoring Connections to Panel

Next in this section:

Monitoring User Sessions.....	269
Monitoring FTP Users Sessions	270
Monitoring Terminal Connections (Windows)	271

Monitoring User Sessions

➤ *To find out who of your customers is logged in to Panel at the moment:*





1. Go to **Tools & Settings > Active Sessions**. All sessions including yours will be presented and the following details will be displayed:
 - **Type**. A type of Panel user who established the session:
 -  for server administrator.
 -  for reseller or customer.
 -  for mailbox owner.
 - **Login**. The login name the user is logged in as.
 - **IP address**. The IP address from which the Panel is accessed.
 - **Logon time**. The date and time when the user logged in to the Panel.
 - **Idle time**. The time that user was not doing anything in the Panel while being logged in.
2. To refresh the list of user sessions, click **Refresh**.
3. To end a user session, select the corresponding checkbox and click **Remove**, then confirm removal and click **OK**.

Monitoring FTP Users Sessions

Your Parallels Plesk Panel can show active FTP sessions only when any of the following FTP server programs is installed on the hosting server:

- Microsoft [FTP 7.0](#) (Windows hosting)
- Gene6 FTP Server (Windows hosting)
- Serv-U FTP Server (Windows hosting)
- ProFTPd (Linux/UNIX hosting)

➤ ***To find out who is connected to your server via FTP, in what directories they currently are and what files they are uploading to or downloading from the server:***

1. Go to **Tools & Settings > Active Sessions**.
2. Click the **FTP Sessions** tab. All sessions including yours will be presented and the following details will be displayed:
 - **Type**. The type of user who established the session:
 -  for users not registered with the Panel.
 -  for anonymous FTP users.
 -  for website administrators.
 -  for web users (owners of personal web pages without individual domain names).
 - **Status**. The current status of FTP connection.
 - **FTP user login**. The login name used for access to FTP account.
 - **Domain name**. The domain the FTP user is currently connected to.
 - **Current location**. The directory the FTP user is currently at.
 - **File name**. The file name being operated on.
 - **Speed**. Transfer speed in kilobytes.
 - **Progress, %**. The file transfer operation progress in percentage.
 - **IP address**. The IP address from which the FTP account is accessed.
 - **Logon time**. The time lapsed since the moment user logged in.
 - **Idle time**. The time that user was not doing anything while being connected to the server through FTP.
3. To refresh the list of FTP sessions, click **Refresh**.
4. To end a session, select the respective checkbox and click **Remove**.

Monitoring Terminal Connections (Windows)

➤ *To find out who of your customers is logged in to the server via Terminal Server session at the moment:*

1. Go to **Tools & Settings > Active Sessions**.
2. Click the **TS Sessions** tab. All sessions including yours will be presented and the following details will be displayed:

- **S.** The status of the terminal session:



- for server administrator.



- client is connected and logged in, using valid login and password.



- client is connected, but not logged in.



- client is disconnected.

- **Name.** The name of this terminal session.
- **User.** The name of the terminal session user.

You can see the session details by clicking the session name in the list.

3. To refresh the list of terminal sessions, click **Refresh**.
4. To disconnect a terminal session, select the respective checkbox and click **Disconnect**, then confirm disconnection and click **OK**.
5. To close a terminal session, select the respective checkbox and click **Log Out**, then confirm disconnection and click **OK**.

Backup and Restoration

With the data backup and restore functions provided by your Parallels Plesk Panel, you can perform the following operations:

- Back up the entire server. The backup archive will include your Panel license key, settings and configuration of system services, accounts, sites, databases and mailboxes.
- Back up individual user accounts with websites. The backup archive will include all settings and data related to user account and user's sites.
- Back up individual websites. The backup archive will include all data and settings related to a website.
- Schedule backups.
- Restore data from backup archives.

Storing Backups

Backups can be stored either in:

- The internal Panel repository - a backup storage located on your Panel server.
- An external FTP repository - a backup storage located on some external server in the Web or your local network. In this case, you should provide Panel with a server's hostname and FTP user credentials.

Backups Created by Your Customers

Your customers granted with the permission to use the backup and restore facilities can back up and restore their own account settings and websites through the Control Panel. Your customers, resellers and your resellers' customers will find shortcuts to their backup repositories in their Control Panel (**Websites & Domains** tab > **Backup Manager**).

The backup and restore functions are provided by optional Panel components that are not included in typical installations. You can install these components by using the web-based installation and update wizard: in Server Administration Panel, go to **Tools & Settings > Updates > Add Components**, and select **Plesk Backup Manager** in the **Server backup solutions** group.

Panel users are able to see the role of a user who created a backup (administrator, customer, or reseller) in the backup tasks list (**Tools & Settings > Backup Manager**). This lets customers differentiate between the backups they created by themselves and technical backups of their subscription. The technical backups happen when administrators or resellers back up customer subscriptions as a part of a larger backup. For example, when the Panel administrator creates a server-level backup, all customer subscriptions are backed up as well, and they are displayed to the customers as subscription backups created by the administrator.

If a certain backup task fails, Panel shows the detailed error description in a separate field of a backup task.

Creating Password-protected Backups

Since Panel 11.0, you are able to secure sensitive data in your backups by using password protection. This makes it impossible for an attacker to reveal backup data if the security of your external backup storage is compromised.

You can specify a backup password in the following circumstances:

- In your FTP repository settings (**Websites & Domains > Backup Manager > Personal FTP Repository Settings**).
- When downloading a backup file from the Panel internal repository to some external location.

When uploading these backups back to Panel and restoring them, you will be prompted to provide the password you used for protection.

In this chapter:

Configuring Global Backup Settings	274
Configuring Panel for Using FTP Repository	275
Backing Up the Entire Server	276
Backing Up Individual Accounts and Sites	276
Scheduling Backups	277
Restoring Data from Backup Archives	279
Downloading Backup Files from Server	281
Uploading Backup Files to Server	281
Removing Backup Files from Server	281
Backup Logs	282

Configuring Global Backup Settings

If you serve numerous websites, you may want to configure the backing up process so that it does not consume much server resources.

➤ ***To reduce the server load and set the disk space usage policy:***

1. Go to **Tools & Settings > Backup Settings**.
2. Specify the number of simultaneous backup processes in the **Maximum number of simultaneously running scheduled backup processes** box. The default value is 10. Type a lesser value.
3. To make the backup processes relinquish resources to other processes on the server, select one or both of the following settings:
 - **Run scheduled backup processes with low priority**
 - **Run all backup processes with low priority**

Note that these options increase the backup time. Other server tasks will not work slower during the backup.

4. Select the **Do not compress backup files** checkbox to disable compression.
5. Click **OK**.
6. To prevent the backing up processes from consuming all available disk space on the server, choose one of the following:
 - Set Panel to start a backup only if your server has enough free disk space to store it. Be aware that this option significantly increases the backup time as Panel additionally has to calculate the size of the future backup.

Note: Panel for Windows does not directly calculate object sizes but takes them from the database. As object sizes in Panel database are updated only once a day, the overall calculated backup size can differ from its real value.

 - Set Panel to start a backup only if your server has the specified free disk space. This option is convenient when you approximately know the size of the future backup and do not want Panel to waste time and resources on calculating it.

Configuring Panel for Using FTP Repository

If you are going to use an FTP server for storing backup files, you should specify its settings in **Tools & Settings > Backup Manager > Personal FTP Repository Settings**:

- FTP server's IP address or host name.
- Directory on the server where you want to store backup files.
- User name and password for access to the FTP account.
- Password that Panel will use for backup protection.

Note: Password protection secures only users' passwords included in backups. Other content, such as users' files, is not protected.

Backing Up the Entire Server

➤ *To back up the server configuration settings and all user data you have on your hosting machine:*

1. Go to **Tools & Settings > Backup Manager**.
2. Click **Back Up**.
3. Specify the following:
 - Backup file name prefix and description. You cannot specify an arbitrary file name, however, you can set the control panel to add a prefix to backup file names. Note that the control panel automatically adds the date and time of backup file creation (in Universal Time) to backup file names.
 - Splitting of the backup file. To create a multi-volume backup, select the respective checkbox and specify volume size in megabytes.
 - Location where to store the backup file. Select the repository where you would like to store the backup file.
 - E-mail notification on backup completion. If you want to be notified of the backup completion, type your e-mail address.
 - What data to back up. You can back up only the server settings, or server settings and all user data (including data in databases).
4. Click **Back Up**. The backup process will start and the progress will be shown under the **Current Back Up Tasks** tab. You can use the **Refresh** button to update the information on the screen.
5. When backing up is finished, the backup file will be saved to the repository you selected.

Note: Custom view settings (that are stored as the Simple plan) are included into server-level backups. However, the restoration of these settings is only possible if Panel has not been yet initially configured (either by the `init_conf` utility or from GUI). Learn more about Custom view (on page 25).

Backing Up Individual Accounts and Sites

➤ *To back up a user account with or without sites:*

1. Click **Customers**.
2. Locate the customer whose account you want to back up, and click the corresponding **Control Panel** link.
3. Click the **Account** tab.

4. Do any of the following:
 - To back up a user account with sites, click **Back Up My Account and Websites**.
 - To back up only websites with content, click **Back Up Websites**.
5. Click **Back Up**.
6. Specify the following:
 - Backup file name prefix and description. You cannot specify an arbitrary file name, however, you can set the control panel to add a prefix to backup file names. Note that the control panel automatically adds the date and time of backup file creation (in Universal Time) to backup file names.
 - Splitting of the backup file. To create a multivolume backup, select the respective checkbox and specify volume size in megabytes.
 - Location where to store the backup file. Select the repository where you would like to store the backup file.
 - E-mail notification on backup completion. If you want to send an e-mail notice on the backup completion, type the required e-mail address.
 - What data to back up. You can back up only the settings, or the settings and all data (including data in databases).
7. Click **Back Up**. The backup process will start and the progress will be shown under the **Current Back Up Tasks** tab. You can use the **Refresh** button to update the information on the screen.

When backing up is finished, the backup file will be saved to the repository you selected.

Scheduling Backups

➤ ***To schedule backing up of data:***

1. Go to **Tools & Settings > Backup Manager**.
2. Click **Scheduled Backup Settings**.
3. Select the **Activate this backup task** checkbox and specify the following:
 - When and how often to run the backup.
 - Backup file name.
 - Splitting of the backup file. To create a multivolume backup, select the respective checkbox and specify volume size in megabytes. Note that volume size cannot exceed 4095 megabytes.
 - Location where to store the backup file. Select the repository where you would like to store the backup file.
 - Maximum number of backup files stored in the repository. Type a number if you want to recycle backup files: When this limit is reached, the oldest backup files are removed.

- E-mail notification on backing up errors. If you want to send an e-mail notice when something goes wrong during backing up, type the e-mail address you need.
 - What data to back up. You can back up only settings, or settings and user data.
4. Click **OK**.

Restoring Data from Backup Archives

You can restore data from backup files kept in:

- *The Panel internal repository.*
To restore backup files from Panel repository, choose the backup file name you want to restore on the **Tools & Settings > Backup Manager > Server Repository** tab.
- *An external FTP repository (on page 275).*
To restore backup files from Panel repository, choose the backup file name you want to restore on the **Tools & Settings > Backup Manager > Personal FTP Repository** tab.

After you choose the backup file, Panel will start the restoration wizard. You will be prompted to specify the following restoration parameters:

- **Types of data to be restored.**
- **Suspend website until restoration task is completed.** Select this if you want to avoid possible conflicts that may occur when users modify site content or settings while they are being restored.
- **Send an e-mail notice when restoration task is completed.** Type your e-mail address if you want the control panel to notify you when restoring is completed.
- **Conflicts resolution policy.** Specify what to do if any conflicts occur during restoration.
- **Backup security settings.** If the backup was protected with a password, enter the password into the **Password** field.
If you have forgotten your password, clear the **Provide the password** option. Note that in this case, some sensitive data will not be restored properly. For example, user passwords will be replaced with random ones, the information about already installed APS apps will be lost, and so on.
- **Restore the modified backup file.** You will see this option in the following cases:
 - The selected backup file was modified after creation.
 - The selected backup file is corrupted.
 - The selected backup file was created on another Panel server.
 - The selected backup file was created on the same server before Panel upgrade to 11.5.

Panel will inform you in any of these cases with a warning. You will not be able to start the restoration until you select the **Restore the modified backup file** option. We strongly recommend that you do not restore such backups except in the following situations:

- The backup was created on the same server before Panel was upgraded to version 11.5. Earlier Panel versions did not sign backups, so Panel 11.5 is unable to check their signatures and shows such backups as potentially problematic.
- You are performing a *transfer through backup files*. Learn more in the section **Transferring Data Through Backup Files** of the **Installation, Upgrade, Migration, and Transfer Guide**.

Troubleshooting Restoration Errors

In case if any errors or conflicts occur during restoration of data, the wizard will prompt you to select an appropriate resolution. Follow the instructions provided on the screen to complete the wizard.

Note: The Overwrite data restoring mode means that all objects will be restored from the backup files regardless of their current presence in the system. The Overwrite mode works as follows:

- If an object or settings from the backup file are not present in Parallels Plesk Panel, then they are created or set in Parallels Plesk Panel.
- If an object or settings from the backup file are present in Parallels Plesk Panel, then the object or settings from the backup file replace the corresponding object or settings that are present in Parallels Plesk Panel.
- If an object or settings are present in Parallels Plesk Panel, but are missing from the backup file, then the object or settings currently present in Parallels Plesk Panel are not changed.

Downloading Backup Files from Server

To download a backup file from the Panel repository, choose the corresponding backup file name in **Tools & Settings > Backup Manager** and specify the location for the file.

In order to improve backup security, we recommend that you protect the backup with a password. This makes impossible for an attacker to obtain sensitive data in case the security of your backup storage is compromised.

Note: If you forget your password, it cannot be recovered. Therefore, it is strongly recommended to keep a list of your passwords and corresponding backup file names in a safe place.

Defining Location of Temporary Backup Files

When somebody downloads a backup from the server, Panel creates a temporary archive file with the backup on the server. By default, this file is located in the `/tmp` directory. If there is not enough disk space for storing the temporary file on the corresponding partition, downloading the backup file will be impossible. To avoid such situations, you can change the location of temporary backup files on the Panel server by editing the `DUMP_TMP_D` variable in the `/etc/psa/psa.conf` configuration file.

Uploading Backup Files to Server

You can upload a backup file to the Panel repository, by running the **Tools & Settings > Backup Manager > Upload Files to Server Repository** wizard. Before starting the upload, Panel will prompt you to enter the following backup parameters:

- *Backup file location.*
- *The password you used for protection.*
This is the password that you used for protecting the backup data.

Note: If you provide an incorrect password, Panel will warn you but will upload the backup to the server anyway. During the backup restoration, you will be prompted to enter the password again.

Additionally, if you want to upload a backup file created on another server or in a Panel version earlier than 11.5, you should allow uploading such backups by selecting the corresponding option on this page. In this case, Panel will upload the files and display a warning. If you do not select this option, Panel will display an error message and the files will not be uploaded.

Removing Backup Files from Server

➤ *To remove a backup file from the backup repository in the Panel:*

1. Go to **Tools & Settings > Backup Manager**.
2. Select a checkbox corresponding to the backup file you want to remove.
3. Click **Remove**.
4. Confirm removal and click **OK**.

Backup Logs

When Panel starts performing a backup, it reports the progress to a log. Backup logs contain only general errors such as syntax errors (no or wrong command specified, invalid input parameters), runtime errors and unhandled exceptions, low disk space for backup, and so on.

Backup logs are stored in `/usr/local/psa/admin/PMM/sessions` on Unix/Linux systems and `%plesk_dir%\admin\PMM\sessions` on Windows systems, where `%plesk_dir%` is an environment variable for the Panel installation directory on Windows systems. Each backup log is located in a separate folder that contains date and time of the backup in its name.

You can change the level of details included into logs. This feature is available only for scheduled backups and for backups made through command line. For more information on how to change level of details, see the **Advanced Administration Guide** for Linux and Windows.

Shared Files and Folders

If you use Panel to run your own websites within a webspace, you can set up file and folder sharing. Use sharing to achieve the following goals:

- Allow users within the organization to collaborate on the same documents or other files.
- Allow privileged customers or partners, after authorization in the system, to access documents such as product roadmaps, price lists with discounts, marketing presentations.

In this chapter:

File Sharing Settings	284
Sharing and Protecting Files	285

File Sharing Settings

You can access file sharing settings in both Service Provider (**Server Management > Tools & Settings > File Sharing Settings**) and Power User view (**Settings tab > File Sharing Settings**).

➤ ***To set up file sharing in your information system:***

1. Open the file sharing settings page.
2. **Web Folder root URL** defines the URL for accessing the root Web Folder used by file sharing services. If you want to change the root location of the Web Folder used for file sharing, select the host name, domain name or IP address and specify a folder name.

All other file sharing Web Folders are created inside the folder specified above. The resulting URL will be used for mounting the root Web Folder used by file sharing.
3. If you want the Panel to generate secure links to protect file transfers with SSL encryption, select the **Generate secure links to files and folders** check box.
4. If you want to grant Panel users the ability to publish uploaded files and make these files accessible to all website visitors, select the **Enable public files** check box.
 - If you want to change the folder for storing the public files, specify a new folder name in the **Folder for public files storage** field.
 - If you want to change the URL for read-only visitor access, specify a new folder name in the **URL for visitor access to public files** field.
5. If you want to allow uploading of files into a password-protected folder, that can be accessed by privileged partners or customers, select the **Enable password-protection of public files**, and provide the username and password for accessing the folder.
 - If you want to change the folder for storing the password-protected files, specify a new folder name in the **Folder for password-protected files storage** field.
6. Click **OK**.

Sharing and Protecting Files

When file and folder sharing is set up on the server, you can accomplish the following tasks:

- Share files with other users within your organization for collaboration purposes.
- Share files with privileged customers and partners. Files can be placed in a password-protected directory, and authorized users outside your organization will be able to access them.
- Place files in a private secured directory on the server for backup purposes, or to enable access them over the Internet.
- Transfer files that are too large to be sent by e-mail. You upload files to the server, generate a secret link, and send the link to the intended recipients so they can download the files.
- Access shared files and work with them:
 - Through a web browser, using File Manager built into your information system, or
 - By connecting the folder on the server to your computer's operating system as a Web Folder, and working as if the files are located on your computer.

Note that all operations described below are accessible *only in Power User view*.

Next in this section:

Sharing Files with Other Users Within the Organization	286
Publishing Files for Partners.....	287
Publishing Files for Your Customers	289
Uploading Your Files to a Private Directory on the Server	290
Transferring Large Files that Cannot Be Sent by E-mail.....	291
Accessing and Working with Files	292

Sharing Files with Other Users Within the Organization

➤ *To share files with other users within the organization, in Power User view:*

1. Go to the **File Sharing** tab and select the files that you want to share:

If you have to upload new files to the Panel:

- a. Go to **Shared Files** in the left navigation area and click **Upload Files**.
- b. Click **Browse** and select the files you need.
- c. Select the location inside the **Shared Files** folder where you want to upload files.

If you want to share the files from your **Personal Files** folder:

- d. Under the **Files** tab go to **Personal Files** in the left navigation area and browse to the directory where required files are located.
- e. Select the required files and click **Share**.
- f. Select the location inside the **Shared Files** folder where you want to upload files.

2. If you want to send an e-mail notice with links to shared files, select the check box **Send e-mail with links to uploaded files upon completion**, and click **Next**. Otherwise, click **Upload** without selecting this check box.

If you chose to send an e-mail notice, you will have to do the following on the next screen:

- a. Select whether authorization in the Panel should be required for accessing the files and whether those who have the links to files should be able to modify them.
- b. If you selected the linked files to be accessible for everyone, select the link expiration period. After this period has elapsed, the links will be no longer valid.
- c. Select the Panel user accounts who should receive the notice and type e-mail addresses of other notice recipients.
- d. Specify e-mail subject and body. Note that links to files will be inserted automatically in place of `<- [LINKS WILL BE INSERTED HERE - DO NOT REMOVE] -> text`.

3. Click **OK**.

Now the files are uploaded to the directory called `shared`, and all users registered in your information system will be able to view, modify, and delete them.

Publishing Files for Partners

If publishing to the password-protected directory called `protected` is allowed by the server policy, then authorized users of your information system will be able to upload files to this directory. After that, your partners or privileged customers will be able to download files from this directory after specifying the password that was sent to them.

➤ ***To publish files for your partners and privileged customers, in Power User view:***

1. Go to the **File Sharing** tab and select the files that you want to publish:

If you have to upload new files to the Panel:

- a. Under **Public Files** in the left navigation area go to **Password-protected files**.
- b. To view the credentials currently used for accessing password-protected files, click **Show Access Info** in the lower right corner of the screen. You will need to send these credentials to your partners who should have the access to files in the `protected` directory.
- c. Click **Upload Files** and select the location inside the **Password-protected files** folder where you want to upload files.
- d. Click **Browse** and select the files you need.

If you want to publish the files from **Personal Files** or **Shared Files** folder:

- e. To view the credentials currently used for accessing password-protected files, go to **Password-protected files** and click **Show Access Info** in the lower right corner of the screen. You will need to send these credentials your partners who should have the access to files in the partners directory.
 - f. Browse to the directory where required files are located, select the required files and click **Publish**.
 - g. Select the **Protect access to files with a password** check box.
 - h. Select the location inside the **Password-protected files** folder where you want to publish the files.
2. If you want to send an e-mail notice with links to published files, select the check box **Send e-mail with links to published files upon completion**, and click **Next**. Otherwise, click **Upload** without selecting this check box.
If you chose to send an e-mail notice, you will have to do the following on the next screen:
 - a. Select whether authorization in the Panel should be required for accessing the files and whether those who have the links to files should be able to modify them.

- b.** If you selected the linked files to be accessible for everyone, select the link expiration period. After this period has elapsed, the links will be no longer valid.
 - c.** Select the user accounts in the Panel who should receive the notice and type e-mail addresses of other notice recipients.
 - d.** Specify e-mail subject and body. Note that links to files will be inserted automatically in place of <- [LINKS WILL BE INSERTED HERE - DO NOT REMOVE] -> **text**.
- 3.** Click **OK**.

Now the files are published in the directory called `protected`, and only authorized users who know the password will be able to download and view these files.

Publishing Files for Your Customers

If publishing to the `public` directory is allowed by the server policy, then authorized users of the information system will be able to upload files to this directory, thus making them accessible to your customers who visit your website, and any Internet user who knows where these files are located.

➤ ***To publish files on the Web for your customers, in Power User view:***

1. Go to the File Sharing tab and select the files that you want to publish:

If you have to upload new files to the Panel:

- a. Go to **Public Files** in the left navigation area.
- b. Click **Upload Files** and select the location inside the **Public Files** folder where you want to upload files.
- c. Click **Browse** and select the files you need.

If you want to publish the files from **Personal Files** or **Shared Files** folder:

- d. Browse to the directory where required files are located, select the required files and click **Publish**.
 - e. Do not select the **Protect access to files with a password** check box.
 - f. Select the location inside the **Public Files** folder where you want to publish the files.
- 2. If you want to send an e-mail notice with links to published files, select the check box **Send e-mail with links to uploaded files upon completion**, and click **Next**. Otherwise, click **Upload** without selecting this check box.**

If you chose to send an e-mail notice, you will have to do the following on the next screen:

- a. Select whether authorization in the Panel should be required for accessing the files and whether those who have the links to files should be able to modify them.
- b. If you selected the linked files to be accessible for everyone, select the link expiration period. After this period has elapsed, the links will be no longer valid.
- c. Select user accounts in the Panel who should receive the notice and type e-mail addresses of other notice recipients.
- d. Specify e-mail subject and body. Note that links to files will be inserted automatically in place of `<- [LINKS WILL BE INSERTED HERE - DO NOT REMOVE] ->` text.

3. Click OK.

Now the files are uploaded to the directory called `public`, and your customers, including any Internet users who know where the files are located, will be able to download and view these files.

Uploading Your Files to a Private Directory on the Server

All authorized users of your information system can use private folders on the server to:

- Store backup copies of their files.
- Access files in their private directories over the Internet.

➤ ***To upload your files to the private directory through File Manager, in Power User view:***

1. Go to the **File Sharing** tab and click **Personal Files** in the left navigation area.
2. Click **Upload Files**.
3. Click **Browse** to select the files you need.
4. Select the folder where you want to upload files.
5. If you want to send an e-mail notice with links to the uploaded files, select the check box **Send e-mail with links to uploaded files upon completion**, and click **Next**. Otherwise, click **Upload** without selecting this check box.

If you chose to send an e-mail notice, you will have to do the following on the next screen:

- a. Select the link expiration period. After this period has elapsed, the links will be no longer valid. If you want to make the link permanent, so that it will not expire, select the option **never**.
 - b. Select user accounts in the Panel who should receive the notice and type e-mail addresses of other notice recipients.
 - c. Specify e-mail subject and body. Note that links to files will be inserted automatically in place of `<- [LINKS WILL BE INSERTED HERE - DO NOT REMOVE] ->` text.
6. Click **OK**.

Now the files are uploaded to the directory called `private/username`, and only the owner of this directory will be able to view, download, modify, and delete these files.

Transferring Large Files that Cannot Be Sent by E-mail

➤ *If you need to send someone a file that is too large to be sent by e-mail, in Power User view:*

1. Upload the file to the server, or select the file, if it has already been uploaded to the server:

If you have to upload new files to the Panel:

- a. Go to the File Sharing tab and click the **Upload Files** link.
- b. Select the folder where you want to upload files, for example, **Personal Files > admin**.
- c. Click **Browse** and select the files you want to send.
- d. Select the check box **Send e-mail with links to published files upon completion** and click **Next**.

If files are already uploaded to the Panel:

- e. Go to **Files** tab and browse to the directory where required files are located.
 - f. Select the required files and click **E-Mail Link**.
2. If you have chosen to send a file from locations other than a user's private directory (**Personal Folder**), then also select whether authorization in the Panel should be required for accessing the files and whether those who have the links to files should be able to modify them.
 3. Select the link expiration period. After this period has elapsed, the links will no longer be valid.
 4. Select user accounts in the Panel who should receive the notice and type e-mail addresses of other notice recipients.
 5. Specify e-mail subject and body. Note that links to files will be inserted automatically in place of <- [LINKS WILL BE INSERTED HERE - DO NOT REMOVE] -> text.
 6. Click **OK**.

The links to files will be sent to the intended recipients, and they will be able to download the files.

Accessing and Working with Files

There are two ways to work with shared files:

- If you need to work with the files frequently, connect a Web Folder on the server to your computer.
- If you occasionally need to access the files, use the Panel interface (Files tab).


➤ *To use the File Manager built into your information system for working with files:*

1. In the Panel, click the **Files** tab. The file manager opens.
2. Use the following icons and links to work with files and directories.

In the left area:

- **Upload Files.** This starts a wizard that allows you to upload files and directories to the server.
- **Personal Files.** This takes you to the private directory where you can place files that only you can access. If you need to use the storage space on the server for backup purposes, or if you need to access files over the Internet, place your files into this directory. For more information, refer to the section *Uploading Your Files to a Private Directory on the Server*.
- **Shared Files.** This takes you to the shared (or common) directory where you should place files that must be available to other users within your organization. When you need to collaborate with other employees, place files into this directory. For more information, refer to the section *Sharing Files with Other Users Within the Organization*.

The right area shows a list of files and directories located in the currently selected directory, and a toolbar with the following items:

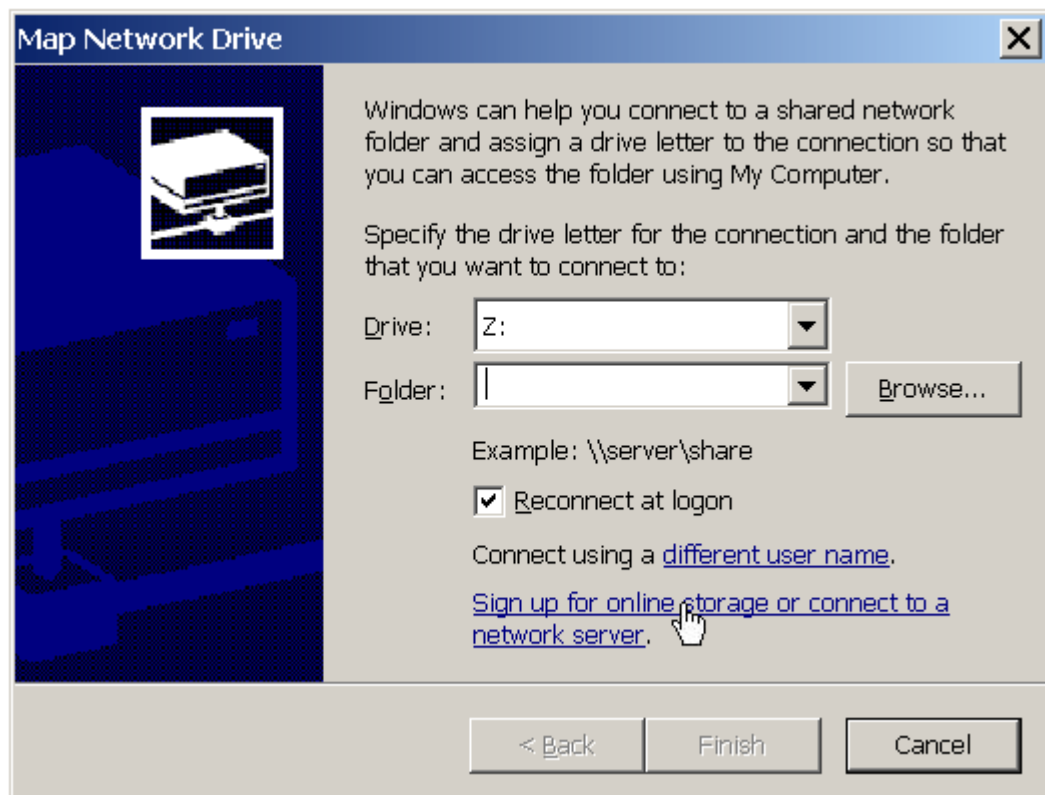
- **Share.** Select files in any directory and click this to move the files to the Shared Folder. This will make them accessible to all users authorized in your information system.
- **E-mail Link.** Select files in any directory and click this to send an e-mail message notifying users of files location, so that the users could download them.
- **Delete.** Select files and click this to permanently remove them.
- **More.** This menu provides access to the following operations: Create new folder, copy or move files and folders.
- The icon  (**Link to this Folder**). Click this to view or copy to clipboard the Internet address of the current folder.

Next in this section:

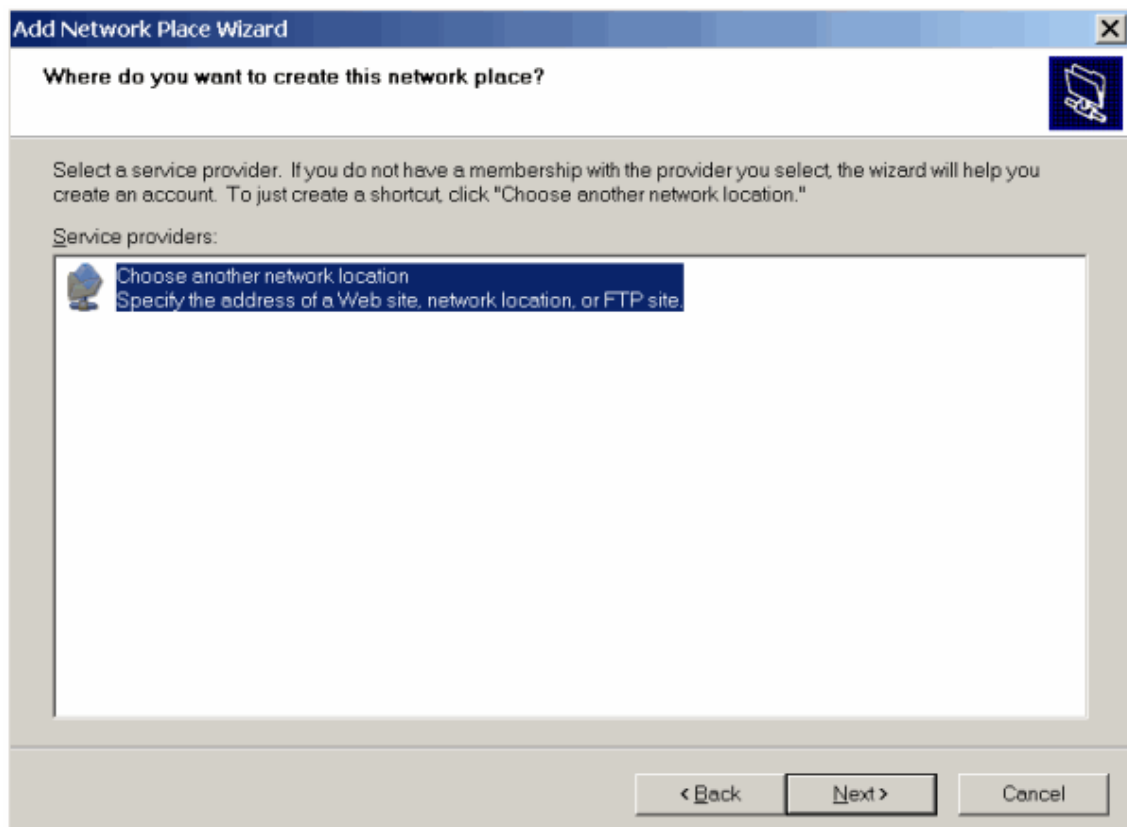
Connecting to Web Folders on Microsoft Windows Systems	293
Connecting to Web Folders on Linux Systems	301
Connecting to Web Folders on Mac OS	302


Connecting to Web Folders on Microsoft Windows Systems

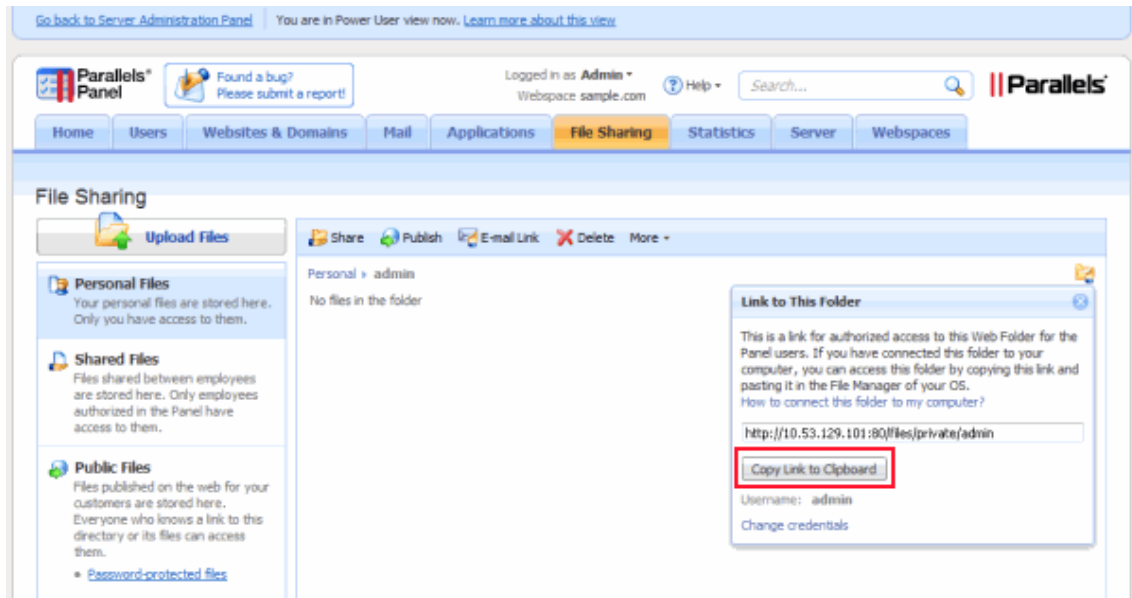
- *To connect a Web Folder to your computer running Microsoft Windows XP:*
1. Right-click the **Start** menu button, and select **Explore**.
 2. In the **Tools** menu, select **Map Network Drive**.
 3. Select the drive letter that will be assigned to the network drive and click **Sign up for online storage or connect to a network server**.



4. Click **Next**.
5. Make sure that the **Choose another network location** option is selected and click **Next**.

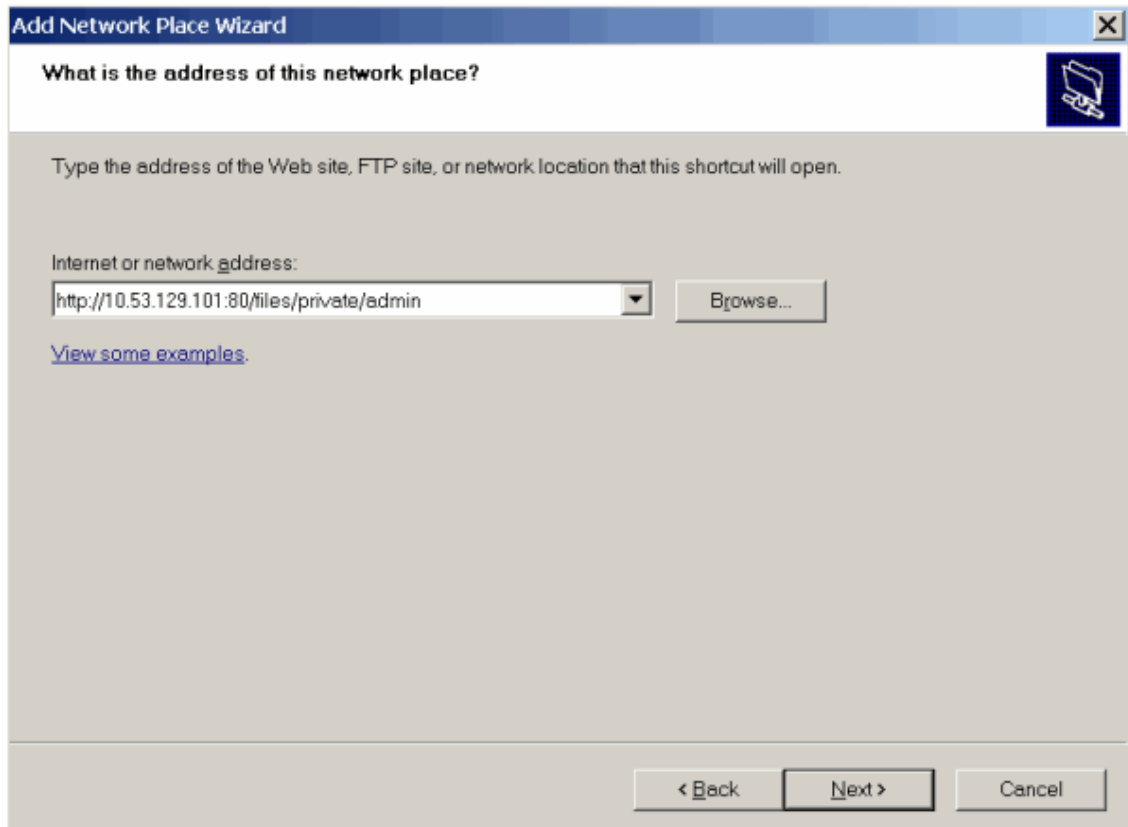


6. Go to Panel and find out the address of the required Web Folder. Log in to the Panel, go to **File Sharing**, find and enter the required folder and click the icon  in the upper right corner of File Manager. The link to the current Web Folder will be shown in the opened window. Click the **Copy Link to Clipboard** button.

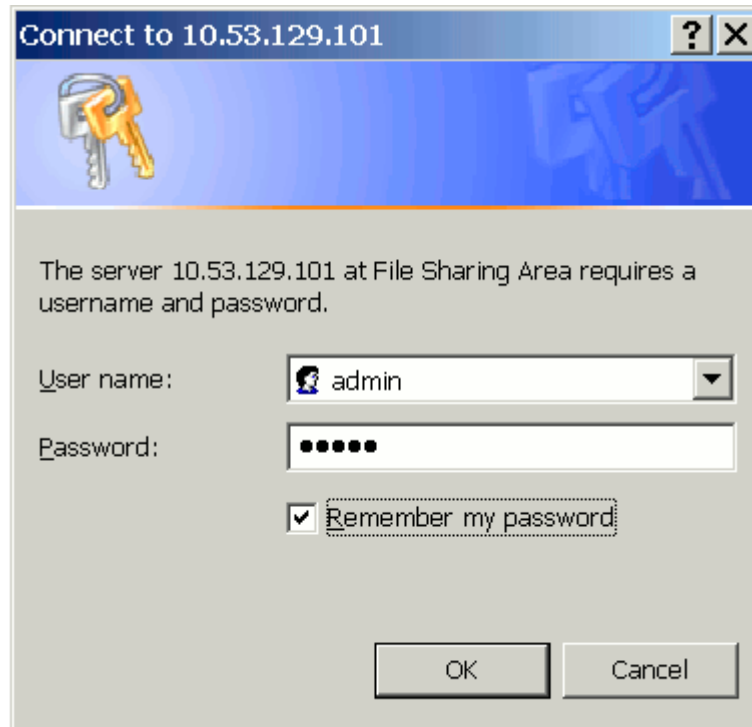


The screenshot shows the Parallels Panel interface. At the top, there is a navigation bar with tabs for Home, Users, Websites & Domains, Mail, Applications, File Sharing (selected), Statistics, Server, and Webspaces. The main content area is titled "File Sharing" and includes an "Upload Files" button and a toolbar with "Share", "Publish", "E-mail Link", "Delete", and "More" options. On the left, there are sections for "Personal Files", "Shared Files", and "Public Files". The main area displays "Personal > admin" and "No files in the folder". A "Link to This Folder" dialog box is open on the right, showing the URL "http://10.53.129.101:80/files/private/admin" and a "Copy Link to Clipboard" button highlighted with a red box. The dialog also shows the username "admin" and a "Change credentials" link.

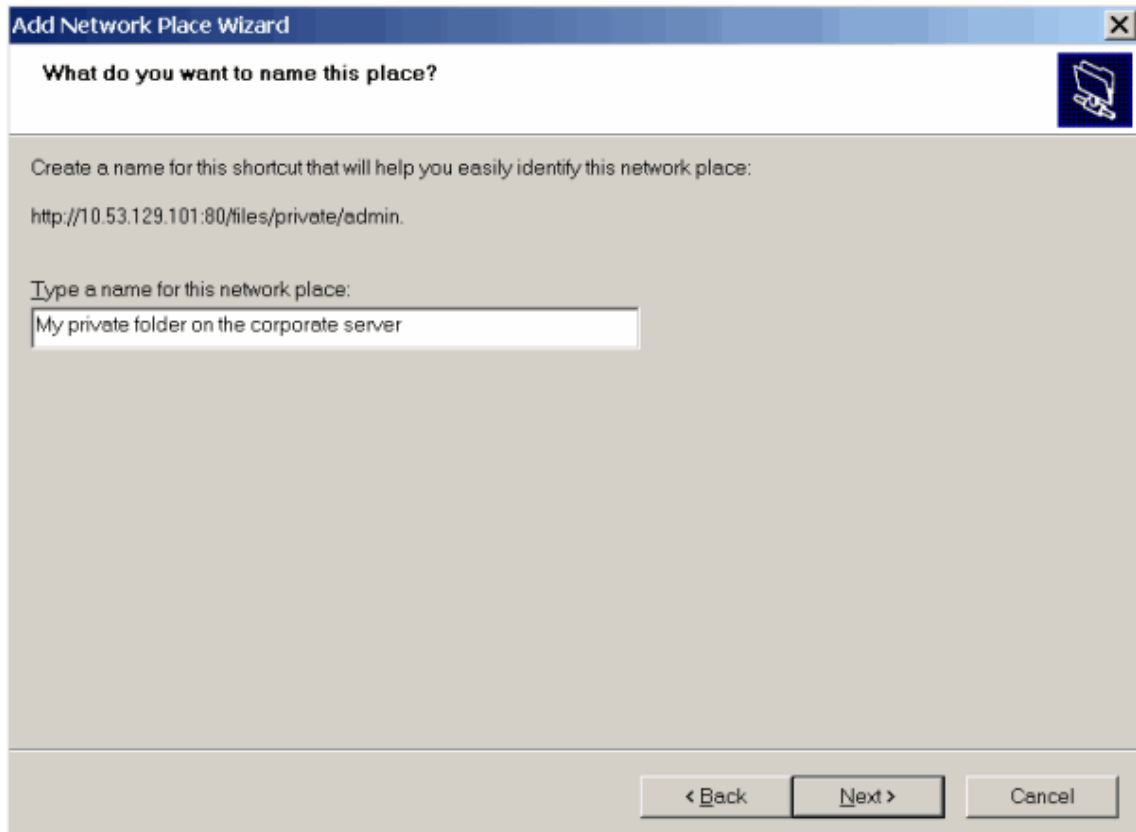
7. Return to the Add Network Place Wizard, specify the full URL to the required Web Folder and click **Next**.



8. In the window that opens, specify the username and password that you use for logging in to the Panel. Select the **Remember my password** check box and click **OK**.



9. Specify a name that you want to designate for this Web Folder in your operating system and click **Next**.



10. Click Finish.

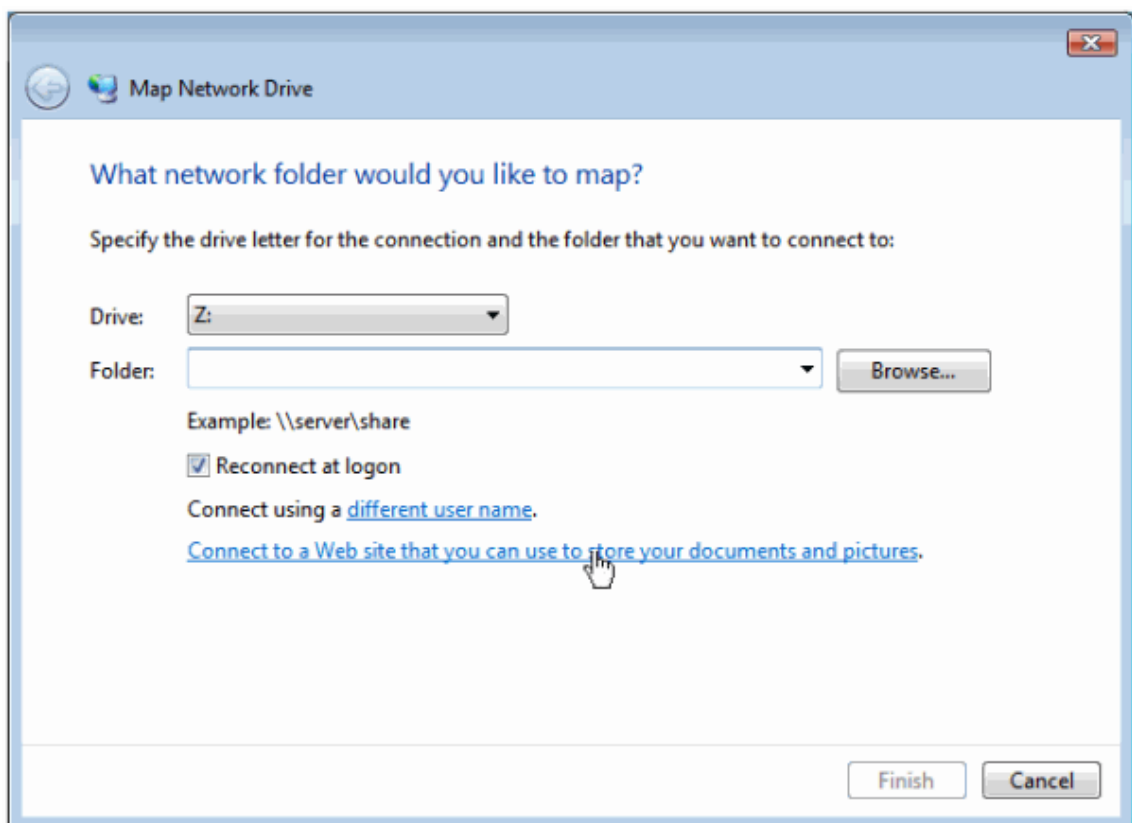
Now, every time you start your computer, this Web Folder will show in your Windows Explorer, under **My Network Places**.


Note for users of Microsoft Windows operating systems: If you experience problems with connecting to a Web Folder, make sure you have installed all available operating system updates and service packs. If you are using a 32-bit version of Windows XP, Windows Vista, or Windows 2003 Server, then also install the hotfix available at <http://www.microsoft.com/downloads/details.aspx?familyid=17C36612-632E-4C04-9382-987622ED1D64>.

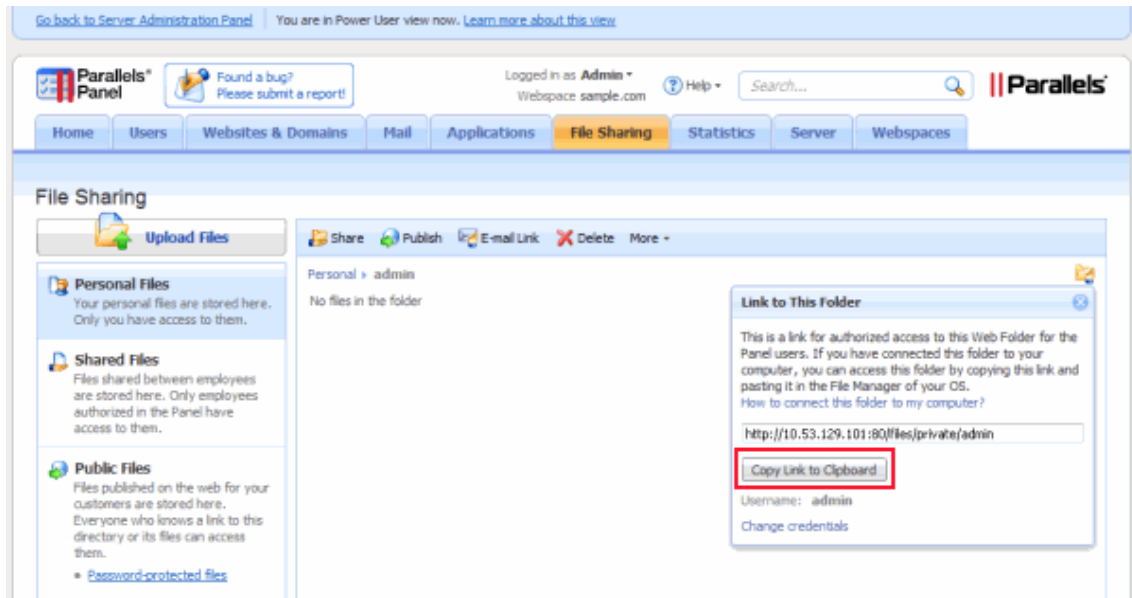


➤ *To connect a Web Folder to your computer running Microsoft Windows Vista or Microsoft Windows 7:*

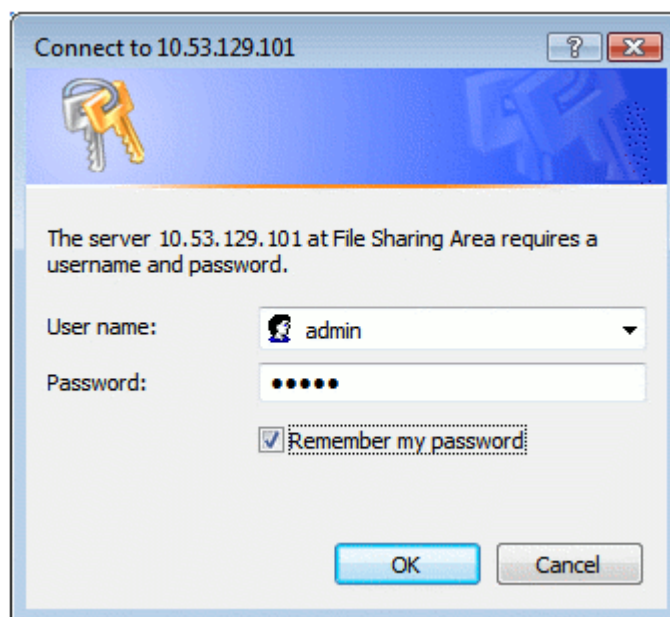
1. Click the **Start** menu button, and select **Computer**.
2. Click **Map Network Drive**.
3. Select the drive letter that will be assigned to the network drive and click **Connect to a Web site that you can use to store your documents and pictures**.



- Go to the Panel and find out the address of the required Web Folder. Log in to the Panel, go to **File Sharing**, find and enter the required folder and click the icon  in the upper right corner of File Manager. The link to the current Web Folder will be shown in the opened window. Click the **Copy Link to Clipboard** button.




- Return to the Map Network Drive Wizard, specify the full URL to the required Web Folder and click Finish.
- In the window that opens, specify the username and password that you use for logging in to the Panel. Select the **Remember my password** check box and click **OK**.




Now, every time you start your computer, this Web Folder will show in your Windows Explorer, under **Network Locations**.

Connecting to Web Folders on Linux Systems

➤ ***To connect a Web Folder as a network drive to your Linux-based computer using GNOME Nautilus file manager:***

1. Open the file browser.
2. In the **File** menu, select **Connect to Server**.
3. From the **Service type** menu, select either **WebDAV (HTTP)** or **Secure WebDAV (HTTPS)**.
To find out which option you need, ask your systems administrator.
4. In the **Server** field, type the host name or IP address of your server.
5. In the **Folder** field, type the path to your shared folder.
To learn the location of your Web Folder, log in to the Panel, go to **File Sharing**, find and enter the required folder and click the  icon in the upper right corner of File Manager. The link to current Web Folder will be shown in the opened window.
6. Click **Connect**.
7. The shortcut to the file share will be added to the **Places** pane. Click this shortcut.
8. Specify the username and password that you use for logging in to the Panel.
9. Select the option **Remember password forever** so that you would not have to type it every time you connect to the server.
10. Click **Connect**.


➤ ***To connect to a Web Folder using KDE Konqueror file manager:***

1. Open Konqueror, and type the address of the shared folder in the address bar. Use `webdav` or `webdavs` as the protocol, instead of `http` or `https`.
To learn the location of your Web Folder, log in to the Panel, go to **File Sharing**, find and enter the required folder and click the  icon in the upper right corner of File Manager. The link to the current Web Folder will be shown in the opened window.
2. Specify the username and password that you use for logging in to the Panel.

Connecting to Web Folders on Mac OS

➤ ***To connect a Web Folder as a network drive to your Mac OS X-based computer:***

1. Open Finder.
2. Click **Go**, and select the option **Connect to Server**.
3. Specify the location of your shared folder.

To learn the location of your Web Folder, log in to the Panel, go to **File Sharing**, find and enter the required folder and click the  icon in the upper right corner of File Manager. The link to the current Web Folder will be shown in the opened window.
4. Click **Connect**.
5. Specify the username and password that you use for logging in to the Panel.
6. Select the option **Remember this password in my keychain** so that you would not have to type it every time you connect to the server.
7. Click **OK**.

If you use SSL, you might receive an alert that the SSL certificate on the server is invalid. In such a case, just click through the SSL warning.

After the network drive is mounted, a shortcut to it will be placed on your desktop.
8. Open **System Preferences**, and select **Accounts**.
9. Select your user account and then click the **Login Items** tab.
10. Select the network drive shortcut on your desktop and drag it to the **Login Items** window (in **System Preferences > Accounts**).
11. If you do not want the mounted drive to automatically open in Finder every time you start your Mac, select the corresponding **Hide** check box.
12. Click **OK**.

Customers and Resellers

When you start your hosting business, you should define how you will offer hosting resources and services to customers. Parallels Plesk Panel lets you organize your business by means of *service plans* and *subscriptions*.

Serving Customers

A *service plan* is a combination of resources and services that you sell to your customers. For example, a hosting account with 1 GB of disk space and 50 GB of traffic is a hosting service plan. If you use Panel with the Business Manager solution, you can offer your customers service plans of other types, such as domain name plans and SSL certificate plans. For example, a 1024 bits SSL certificate for a year.

When customers want to host a website on a Panel server, they *subscribe* to a plan that offers hosting resources. In other words, a *subscription* is a set of resources and services defined by a plan that is available to a certain customer for a limited period of time.

The typical workflow to start serving hosting customers in Panel is as follows:

1. You create a hosting service plan in Panel (on page 308).
2. When a customer is ready to subscribe to the plan, you create the account and subscription for the customer (on page 312).
3. Panel grants the customer permissions to log in and use services provided with the subscription.

Using *add-on plans*, you can offer resources and services to customers in addition to those provided by their main service plan, for example, an additional gigabyte of disk space.

Learn more about hosting service plans and their relationship with subscriptions in the section **Hosting Plans and Subscriptions** (on page 305).

Serving Resellers

Reseller plans allow you to sell your services to a special category of customers - resellers. Resellers are people who sell hosting accounts on your servers to others. From a business perspective, resellers are similar to hosting providers: they have accounts in hosting panels, and their own online stores and customer management tools. The difference is that resellers do not have their own hosting servers. Learn how to start serving resellers in the section **Reseller Plans** (on page 322).

Business Automation with Business Manager

Organizing your offerings into plans is only one stage in getting your business ready to run. Before you can start serving customers, you should also think about how potential customers will find your offerings, how you will subscribe new customers and take payments, and other aspects of your business. To make it easier to start your business, we recommend that you use an integrated automation solution - Business Manager. This will allow you to completely automate all aspects of your business. Though you can decide to use another third-party automation tool, Business Manager provides the most complete integration with all Panel features. To learn more about Business Manager, refer to the **Administrator's Guide to Parallels Customer and Business Manager**.

Note: You can choose not to use any automation solution at all. In this case, you should control the money flow by yourself as well as perform a number of tasks manually in the Server Administration Panel, for example, create customer accounts and subscribe them to your offerings.

This chapter contains instructions on how to set up your hosting offer in Panel.

In this chapter:

Hosting Plans and Subscriptions	305
Reseller Plans	322

Hosting Plans and Subscriptions

A hosting plan is a set of hosting resources and services you offer to your customers. For example, the properties of a hosting plan define the server resources available in a plan subscription, such as disk space, traffic, number of mailboxes and so on. To learn more about how plan resources are allocated in the subscription, refer to the section **Relationship Between Plans and Subscriptions** (on page 306).

This section will guide you through the process of creating a hosting plan and starting to serve your customers.

The amount of resources and services provided with a subscription can be extended by associating the subscription with add-on plans. To learn how to create add-on plans, refer to the section **Setting Up Add-on Plans in Panel** (on page 311).

Next in this section:

Relationship Between Plans and Subscriptions.....	306
Setting Up Hosting Plans.....	308
Setting Up Add-on Plans	311
Subscribing Customers to Plans.....	312
Managing Customers	314
Managing Subscriptions	317
Serving Non-Technical Customers	321

Relationship Between Plans and Subscriptions

Normally, a subscription is associated with a service plan, and this association is reflected in a list of subscriptions: each subscription name contains the service plan name in brackets at the end. The amount of resources and services provided with a subscription can be extended by associating the subscription with add-on plans. A subscription can be associated with several add-ons, but each add-on can be added to the subscription only once.

It is also possible that a subscription may not be associated with a service plan, and so it cannot be associated with any add-on plans: add-ons are only added to a "main" service plan. We call such subscriptions *custom subscriptions*, and their names are extended with "(Custom)" in the list of subscriptions. Having a custom subscription may be useful if you want to provide services on specific terms that are different from the usual offerings in your business model.

You can change the association between a subscription and plans at any time as follows:

- Associate the subscription with another service plan.
- Add and remove add-on plans.
- Remove the subscription association with the service plan and add-ons.

States of Subscription

Subscriptions associated with a particular plan are synchronized, or *synced*, with it: any changes made to the plan are automatically applied to all its subscriptions. This is true for all kinds of plans: service plans, their add-ons, and reseller plans.

The Panel allows the following deviations from the default subscription state (active and synced with the service plans):

- **Locked** state, which means *locked for syncing*, indicates that a subscription is excluded from syncing with the associated plans.
A subscription gets locked if you change the parameters of the subscription, without changing the associated service plan. Such locking secures your customizations so that they are not overwritten the next time you change the plan and all its subscriptions are synced.
- **Unsynced** state indicates that some services or resources offered with the associated plans cannot actually be provided with the subscription.
- **Suspended** state. This state is not related to the synchronization of a subscription with the service plan, but it affects the behavior of websites. Panel suspends subscriptions automatically if their expiration date passes. In addition, you can suspend a subscription manually. To learn more, see **Managing Subscriptions** (on page 317).

Note: If a plan offers a privilege that makes it possible for a subscriber to change a particular resource or service, this resource/service allocation is ignored during a sync. For example, if the plan provides the privilege of PHP settings management and a customer changes some PHP setting, its subscription remains synced with the plan (even if a value of the PHP setting in the subscription differs from the corresponding one in the plan).

Unsynced Subscriptions

Panel does not check whether a service or a resource that a service plan should provide is actually available in the system. For example, when creating a plan, you can select to provide ColdFusion when ColdFusion is not installed on the server, and Panel will let you do it and will show no error or warning messages.

A subscription is automatically marked as **Unsynced** if Panel cannot provision the resources and/or services defined by the plan. This may happen in the following cases:

- When the subscription is created.
- When the properties of the associated plan are changed.
- When an add-on plan is added to or removed from the subscription.

➤ ***To know which of the subscription's resources or services are not synced with the plan:***

1. Go to **Subscriptions**, and click the unsynced subscription name.
2. Click **Sync**.

The Panel will retry syncing the subscription with associated plans, and will display the conflicting properties if syncing fails.

Be sure to take the note of the conflict report: which properties are affected, and what the **Plan value** and the **Available value** are.

Clicking **OK** at this page will initiate setting the subscription values according to the available values, **Cancel** will leave everything unchanged.

Once you have identified the problem, you can resolve it. There are two possible ways:

1. Fine-tune the plan to conform to the system actual state.
2. Fine-tune the system to provide resources and services offered with the plan.

➤ ***To change the plan properties to conform to the system:***

1. Go to **Service plans > <plan name>**.
2. Adjust values of the problem properties so that they correspond to the **Available values** (see above).
3. Click **Update & Sync**.

The subscriptions will be synced automatically.

➤ **To adjust the system and re-sync a subscription:**

1. Adjust your system: install missing components, add hard disks - whatever is indicated by the conflict report.
2. Go to **Subscriptions**, and click the unsynced subscription name.
3. Click **Sync**.

The Panel will retry syncing the subscription with associated plans.

Setting Up Hosting Plans

To create a hosting service plan in Panel, run the **Service Plans > Add New Plan** wizard in the Server Administration Panel.

During the plan creation process, you will be prompted to specify various plan parameters. Learn more next in this section.

If you already have service plans and want to create plans with similar settings, you can create copies of these plans by clicking **Clone Plans** on the **Service Plans** page and then edit the copies as described in this section.

Once the plan has been created, you are ready to start serving your customers. In other words, you can create customer accounts and subscriptions. Learn more in the section **Subscribing Customers to Plans** (on page 312).

Next in this section:

Specify Plan Properties	309
Offer Additional Services	309

Specify Plan Properties

When creating a plan, you are prompted to specify a number of service plan parameters. These parameters are grouped with a number of tabs:

Properties of a hosting plan and subscription are grouped as follows:

- **Resources**

These are hosting resources provided with a plan. Includes validity period, policy on overusing resources, system resources like disk space and traffic, and service resources like websites, subdomains, mailboxes, databases and so on. For example, the Domains resources sets the number of domains that a customer can register and manage in Panel.

- **Permissions**

Includes provided services and privileges.

Note: Some permissions prevent settings of the corresponding services from syncing (on page 306).

- **Hosting Parameters**

Includes parameters of the provided hosting service.

- **PHP Settings**

Includes the customizable PHP settings. The PHP settings have a great importance as they affect the work of the major part of web applications. Learn more about how to adjust PHP settings for service plans in the section **PHP Configuration** (on page 50).

- **Mail**

Includes parameters of the provided mail service.

- **DNS**

Specifies if the DNS zones of the subscription's domains should be master or slave.

Note: In case the **DNS zone management** privilege is provided, this parameter is not synced, and subscribers can set up this parameter on a per-domain basis.

- **Performance**

Includes parameters that affect performance of all services provided with the plan.

- **Logs & Statistics**

Includes settings of how statistics and logs of the plan's subscriptions should be stored

- **Applications**

Lets you select which applications should be available to subscribers.

Learn more about hosting plan properties in the **Appendix A: Properties of Plans and Subscriptions** (on page 558).

Offer Additional Services

In addition to the hosting services and features provided by your plan, you can expand the offering by using the following means:

- Install third-party applications packaged as Panel extensions and include the services they provide into your hosting plans.

When such an extension is installed, the service provided by it is registered in Panel and is made available for inclusion into hosting plans by the server administrator and resellers: The option corresponding to the new service is listed in hosting plan properties, on the **Additional Services** tab.

- Add custom options to plans.

If you, for example, run an online support service at `http://premium-support.example.com`, and want to include the support option into a service plan, you should set up a custom plan option:


1. Go to **Service Plans > Additional Services > Add Service**.
2. Specify service name (`Premium support`), service description, and select the option to place a button to Control Panel with the link to the online service (`http://premium-support.example.com`).

After this is done, a new tab called **Additional Services** appears in hosting plan settings. It shows your **Premium support** option which you or your resellers can select for provisioning to customers.

➤ *To add a service provided by an application packaged as an extension:*

Install the extension according to the instructions provided in the **Installation, Upgrade, and Migration Guide**, chapter **Installing Panel Extensions**, or use the instructions provided by the extension packager.

➤ *To add a service as a custom plan option:*

1. Go to **Service Plans > Additional Services** tab.
2. Click **Add Service**.
3. Specify the following:
 - **Service name**.
 - **Service description**.
 - **Use custom button for the service**. Select this checkbox to place a hyperlink to your online service or a web application to subscriber's Control Panel.
 - **URL attached to the button**. Specify the Internet address where the user should be directed after clicking the button. For example: `http://premium-support.example.com`.
 - **Background image for the button**. If you do not select an image, the Panel will use the default image .
 - **Open URL in the Panel**. Leave this checkbox cleared if you want the external web resource to open in a new browser window or tab.

- If you want the Panel to send the customer and subscription information with the HTTP request, specify what information should be included:
 - Subscription ID.
 - Primary domain name associated with a subscription.
 - FTP account username and password.
 - Customer's account ID, name, e-mail, and company name.
- 4. Click **OK**.
- ***If you do not want to let your resellers use an additional service and provision it to their customers:***
 1. Go to **Service Plans > Additional Services** tab.
 2. Select a checkbox corresponding to the service and click **Make Unavailable**.
- ***To let resellers use an additional service and provision it to their customers:***
 1. Go to **Service Plans > Additional Services** tab.
 2. Select a checkbox corresponding to the service and click **Make Available**.
- ***To remove a custom plan option from service plan properties:***
 1. Go to **Service Plans > Additional Services** tab.
 2. Select a checkbox corresponding to the service and click **Remove Service**.
- ***To remove an additional service provided by an extension:***

Remove the extension from the Panel.

Setting Up Add-on Plans

Add-on plans extend the amount of resources and services provided with a subscription (for example, additional gigabytes of disk space or Perl scripting language support). A subscription can be associated with several add-ons, but each add-on can be added to the subscription only once.

To create an add-on plan, start the wizard **Service Plans > Add New Add-on** and specify the plan properties (on page 558).

Subscribing Customers to Plans

If you do not use billing automation, then to start serving a customer in Panel, you should create a customer account and subscribe the customer to a service plan. Any user can be subscribed to several service plans simultaneously, meaning that they will have several service subscriptions, some of which may be custom, and some of which may be associated with different add-on and service plans.

Subscribing a new customer generally means creating the customer account together with their first subscription. However, starting from Parallels Plesk Panel 10.2, you can also create customer accounts without subscriptions. This can be useful if you do not need to set up a website for a customer at the moment, and want to transfer a subscription from another customer account, or set up a subscription later. Note that customers without subscriptions cannot log in to the Control Panel.

➤ ***To create a new customer account without a subscription:***

1. Go to **Customers**, and click **Add New Customer**.
2. Specify the customer's contact and billing information, Control Panel account user name and password.
3. Clear the **Create subscription for the customer** checkbox.
4. Click **OK**.

➤ ***To subscribe a new customer to a service plan and, optionally, add-ons:***

1. Go to **Customers**, and click **Add New Customer**.
2. Specify the customer contact/billing information, user name and password, attributes of the domain linked with the subscription.
3. Select a service plan with which the subscription should be associated.
4. Select add-on plans if you wish to add any.
5. Leave the **Proceed to customizing the subscription...** checkbox cleared.
6. Click **OK**.

➤ ***To subscribe a new customer to a service plan and add-ons on specific terms (customize subscription associated with plans):***

1. Go to **Customers**, and click **Add New Customer**.
2. Specify the customer contact/billing information, user name and password, attributes of the domain linked with the subscription.
3. Select a service plan and add-ons.
4. Select the **Proceed to customizing the subscription...** checkbox.
5. Click **OK**.

The customer account and the subscription will be created, and the Panel will offer to customize such subscription properties (on page 558) as resources and permissions. Customizing hosting, mail, DNS service parameters is not available in the Server Administration Panel.

6. Customize the subscription properties.

7. Click **Update & Lock**.

The customized subscription will get locked for syncing, it will not be synced with the service plan or add-ons in case they change. For details, refer to the section **Relationship Between Plans and Subscriptions** (on page 306).

➤ ***To subscribe a new customer to your services on specific terms (create custom subscription):***

1. Go to **Customers**, and click **Add New Customer**.

2. Specify the customer contact/billing information, user name and password, attributes of the domain linked with the subscription.

3. Select **None** next to the **Service plan**.

The subscription properties will be set according to the Panel default service plan.

4. Leave the **Proceed to customizing the subscription...** checkbox selected.

5. Click **OK**.

The customer account and their custom subscription will be created. For details on custom subscriptions, refer to the section **Relationship Between Plans and Subscriptions** (on page 306).

The Panel will offer to customize such subscription properties (on page 558) as resources and permissions. Customizing hosting, mail, DNS service parameters is not available in the Server Administration Panel.

6. Customize the subscription properties.

7. Click **OK**.

➤ ***To add a subscription to host your own websites and mail:***

1. Go to **Subscriptions**, and click **Add New Subscription**.

2. Specify attributes of the domain provisioned with the subscription, service plan and add-ons.

3. Optionally, select the **Proceed to customizing the subscription...** checkbox.

4. Click **OK**.

Managing Customers

Once you create a customer account, you can perform the following operations with it:

Changing Contact Information

➤ ***To change a customer's contact information:***

1. Go to **Customers**, and click the **<Customer Name>** in the list.
2. Click **Edit Contact Info**.
3. Update the information, and click **OK**.

Changing Username and Password

➤ ***To change username and password a customer uses to access Control Panel:***

1. Go to **Customers**, and click the **<Customer Name>** in the list.
2. Click **Change Login Info**.

Update password and username, and click **OK**.

Note: The Panel does not notify customers upon the login information change automatically. What is more important is that a customer must provide their username and e-mail address to retrieve their password. So be sure to update your customers on login information changes, especially if you change their username. Otherwise, they will not be able to use the Panel.


Suspending Accounts

Access to the Panel is blocked for suspended customers and Control Panel users that they created. The customer's subscriptions are suspended, too, meaning that their websites, FTP and mail services will no longer be accessible to the internet users.

➤ ***To suspend a customer's account:***

1. Go to **Customers**, and click the **<Customer Name>** in the list.
2. Click **Suspend**.

➤ ***To suspend several accounts at once:***

1. Go to **Customers**.
2. (Optional) Filter out active accounts:
 - a. Click the  button next to the search field above the list.
This will open the list filter.
 - b. Under the **Status** filter, select **Active**.
3. Select target accounts in the list.
4. Click **More Actions > Suspend**.


Activating Accounts

Once an account is activated, all its subscriptions are activated, too, and all the services start working properly.

➤ ***To activate a customer account:***

1. Go to **Customers**, and click the <Customer Name> in the list.
2. Click **Activate**.

➤ ***To activate several accounts at once:***

1. Go to **Customers**.
2. (Optional) Filter out suspended accounts:
 - a. Click the  button next to the search field above the list.
This will open the list filter.
 - b. Under the **Status** filter, select **Suspended**.
3. Select target accounts in the list.
4. Click **More Actions > Activate**.

Removing Accounts

Once a customer account is removed, all customer's subscriptions and websites are removed as well.

➤ **To remove customer accounts:**

1. Go to **Customers**, and select the accounts you want to remove.
2. Click **Remove**.
3. Click **Yes** at the confirmation box.

Managing Customers in Business Manager

If you installed the Customer and Business Manager component and configured it to work with your Panel, then the following additional links are available in Panel:

- **Business Manager.**
- **Billing Details.**
- **Invoices.**
- **Payment History.**
- **Generate Outstanding Invoices** (in the **More Business Operations** menu).
- **Create Invoice** (in the **More Business Operations** menu).
- **Credits** (in the **More Business Operations** menu).
- **Billing Accounts** (in the **More Business Operations** menu).

Use these links for managing customer accounts in Business Manager. Learn how to manage customer accounts in Business Manager in the section **Administering Customers in Business Manager**.

Managing Subscriptions

Once a customer is subscribed to a service plan, you can perform operations with their subscription. In order to perform operations on a subscription, you should first find it among other subscriptions. Naturally the information you have about a subscription in question is not full, for example, it may be only the domain name hosted on your server. Even in this situation, it is easy to find the required subscription using the **Domains** page in Server Administration Panel. The page provides facilities to find a domain, a subdomain, a domain alias, a customer account, or a company by name. On this page, you can find relations between domain names and subscriptions and also get the following valuable information:

- The hosting type associated with a domain name.
- The indication if a domain name is an alias.

Moreover, you can instantly view the content of each website from the list.

The following operations with subscriptions are available.

Changing Subscription's Hosting Settings

These include: the IP address on which the subscription's websites are hosted, database servers that the websites use by default, and credentials of a system user account linked with the subscription (used to manage files and folders of websites within the subscription, and to access the server via SSH or Remote Desktop).

➤ ***To change a subscription's hosting settings:***

1. Go to **Subscriptions**, and click the **<Subscription>** in the list.
2. Click **Change Hosting Settings**.
3. Update the information, and click **OK**.

Transferring Subscriptions to Another User

This means that you change owner of subscriptions, or, in other words, reassign subscriptions to another user: another customer, reseller, or yourself. In this case, the subscriptions are automatically unbound from their plans and become custom.

Note: Since Panel 10.4, customers can restrict auxiliary users to accessing only a specified subscription within their hosting account. For this purpose, user roles have the corresponding permission. When you transfer the subscription that has such an attached user role, the role with all its users is also transferred to the new subscriber.

➤ ***To transfer a subscription to another user:***

1. Go to **Subscriptions**, and click the <Subscription> in the list.
2. Click **Change Subscriber**.
3. Select a new subscriber and click **Next >>**.
4. Review the information about the changes to be made to the subscription settings and click **OK**.

➤ ***To transfer several subscriptions to another user:***

1. Go to **Subscriptions**.
2. Select the subscriptions you want to reassign.
3. Click **Change Subscriber**.
4. Select a new subscriber and click **Next >>**.
5. Review the information about the changes to be made to the subscription settings and click **OK**.

Suspending Subscriptions


Panel suspends subscriptions automatically if their expiration date passes. In addition, you can suspend a subscription manually. This may be useful, for example, in case a website hosted within the subscription gets attacked.

The behavior of websites in suspended subscriptions is defined by one of the statuses (active, suspended, disabled) that you select in a service plan or subscription settings (**Hosting Parameters > Status of websites in suspended subscriptions**). Websites, FTP and mail services of suspended subscriptions are no longer available to the Internet users, unless the **Active** status for websites was selected. For more information about websites in suspended subscriptions, see **Hosting Parameters** (on page 568) of service plans and subscriptions.

➤ ***To suspend a subscription:***

1. Go to **Subscriptions**, and click the <Subscription Name> in the list.
2. Click **Suspend**.

➤ ***To suspend several subscriptions at once:***

1. Go to **Subscriptions**.
2. (Optional) Filter out active subscriptions:
 - a. Click the  button next to the search field above the list.
This will open the list filter.
 - b. Under the **Status** filter, select **Active**.
3. Select target subscriptions in the list.
4. Click **Suspend**.

Activating Manually Suspended Subscriptions


Once a subscription is activated, all the services provided with it start working.

Note: Activating a subscription manually is good only for the subscriptions that were suspended manually. If you activate in such a way an expired subscription, it will be automatically suspended the next day. In such cases, renew the subscription as described further in this section.

➤ ***To activate a subscription:***

1. Go to **Subscriptions**, and click the <Subscription Name> in the list.
2. Click **Activate**.

➤ ***To activate several subscriptions at once:***

1. Go to **Subscriptions**.
2. (Optional) Filter out suspended subscriptions:
 - a. Click the  button next to the search field above the list.
This will open the list filter.
 - b. Under the **Status** filter, select **Suspended**.
3. Select target subscriptions in the list.
4. Click **Activate**.

Renewing Expired Subscriptions

The Panel does not renew subscriptions automatically, so it suspends a subscription when the subscription expiration date comes.

➤ ***To renew an expired subscription:***

1. Go to **Subscriptions**, and click the **<Subscription Name>** in the list.
2. Click **Activate**.
3. Click **Customize**.
4. On the **Resources** tab, set up a new expiration date, or select **Unlimited**.
5. Click **Update & Lock**.

Note: After this step, the system will not apply further changes of the plan settings to this subscription. If you try to sync this subscription with the plan, the subscription will expire again unless you set the **Unlimited** validity period for this plan.

Removing Subscriptions

➤ ***To remove subscriptions:***

1. Go to **Subscriptions**, and select the ones you want to remove.
2. Click **Remove**.
3. Click **Yes** at the confirmation box.

Managing Subscriptions in Business Manager

If you installed the Customer and Business Manager component and configured it to work with your Panel, then the following additional links are available in the Panel:

- **Business Manager.**
- **Billing Details.**
- **Upgrade.**
- **Downgrade.**
- **Add-ons**

Use these links for managing subscriptions in Business Manager. Learn how to manage subscriptions in Business Manager in the section **Managing Subscriptions**.

Serving Non-Technical Customers

Some of your customers may lack technical background in system administration, so it is natural for them to feel uncomfortable when they see the full set of tools that Control Panel offers. Even worse, they may corrupt configuration files and complicate troubleshooting if they attempt to use the tools. To avoid these situations and present your customers with a simple and lightweight Control Panel, we recommend that you subscribe them to the *Default Simple* hosting plan available in **Service Plans** > the **Hosting Plans** tab.

This plan allows customers to self service only simple routine operations leaving more complex tasks to your support service. Though it already contains only the most frequently used and popular tools, you are free to fine-grain the plan settings.

If you do not intend to create special plans for such audience, it is possible to limit the number of tools and settings on the per-subscription basis using the instructions we provide in this section. The instructions below explain how to achieve the successful user interface simplification: Practically, you should hide resources and tools your customers are not going to use.

Hiding Redundant Resources

The idea of this modification is straightforward: In hosting plan or subscription settings, the **Resources** tab, set all unused limits to 0. According to **Visibility of Hosting Features in the Control Panel** (on page 560), this will hide such resources in Control Panel.

For example, if you set the mailboxes limit to 0, the **Mail** tab will not be shown in Control Panel. Read more about the resources in the **Resources** section.

Hiding Redundant Tools

The set of tools available to customers in Control Panel is defined by the subscription or plan settings, the **Permissions** tab. For example, if you clear the **DNS zone management** option, the tools to manage DNS will not be shown in Control Panel. Read more about the permissions in the **Permissions** section.

Resources and Tools of Default Simple

Initially, the Default Simple hosting plan includes the following tools:

- Web Hosting Access
- Presence Builder
- File Manager
- Website Statistics
- Secure Your Site with SSL
- Applications
- Databases

Reseller Plans

If your business model employs *resellers*, plans and subscriptions work in almost the same way as for hosting service customers (on page 306). The differences are as follows:

- In this case, we use the terms *reseller plans* and *reseller subscriptions*.
- Reseller add-on plans are not implemented.
- A reseller subscription is not linked to a domain; a reseller subscription provides a set of resources and services that the subscribed resellers redistribute by means of service subscriptions belonging to their customers or to themselves.

Note that the Panel business model has some limitations. It is not possible to:

- Convert customer accounts into reseller accounts.
- Move customer accounts from one reseller to another. You can perform this operation indirectly by moving the customer subscription from one account to another. For more details on how to change a subscription owner, refer to the section **Managing Customers and Subscriptions**.

This section will guide you through the process of creating a reseller plan and starting to serve resellers.

Next in this section:

Setting Up Reseller Plans.....	323
Subscribing Resellers to Plans.....	323

Setting Up Reseller Plans

Serving resellers is quite similar to serving hosting customers.

If you use Panel without any automation solution, then to start serving resellers, you should:

1. Create a reseller plan by running the **Service Plans > Reseller Plans > Add New Plan** wizard in the Server Administration Panel or clone an existing reseller plan by clicking **Clone Plans**.
2. Define plan properties. Learn more about reseller plan properties in **Appendix B: Properties of Reseller Plans and Subscriptions** (on page 575).
3. When a reseller is ready to subscribe to the plan, create the reseller account and subscription. Learn more in the section **Subscribing Resellers to Plans** (on page 323).

Subscribing Resellers to Plans

If you do not use billing automation, then to start serving a reseller in Panel, you should create a reseller account and subscribe them to a reseller plan.

➤ ***To subscribe a new reseller to a reseller plan:***

1. Go to **Resellers**, and click **Add New Reseller**.
2. Specify the reseller contact/billing information, user name and password.
3. Select a reseller plan with which the subscription should be associated.
4. Leave the **Proceed to customizing the subscription...** checkbox cleared.
5. Click **OK**.

Website Management

As described in the chapter *How Panel Works*, one of the Panel's main functions is simplified administration of hosted websites, mailboxes, and other network resources. You can use hosting resources on your server for your own needs as well as for selling these resources to customers: For example, you can set up your corporate website or mailbox on the Panel server.

Setting Up Your Own Subscriptions (Webspaces)

To set up your own hosting account, create a webspace in the Server Administration Panel, **Home > My Webspaces** group. A *webspace* is a subscription to the **Unlimited** service plan (a plan with unlimited resources). During webspace creation, you will be prompted to specify a domain name for the webspace and access credentials. The webspace will appear in the list on the **Subscription** page together with your customers' subscriptions. To start creating your website or editing the subscription settings, click the **Open in Control Panel** link next to the subscription name. A list of operations available to you in the Control Panel is provided in the table below.

Each webspace opens in the Power User view. This view combines management of own hosting accounts and server administration capabilities. In turn, actions related to hosting plans, resellers, and customers are still performed in the Server Administration Panel.

To switch back to serving hosting customers and resellers, click **Go back to Server Administration Panel** at the top of Control Panel pages.

For more information about Power User view, see the section **The Panel GUI (on page 20)**.

Helping Customers Manage Their Subscriptions

Your customers have different levels of technical expertise and, therefore, may have problems with managing certain settings of their subscriptions. To assist your customers, you can log in to the Control Panel under a customer's account and edit their websites and subscription properties as your own ones. To start managing a customer's subscription in the Control Panel, find this subscription in the list on the **Subscriptions** page and click **Open in Control Panel**.

Operating in Control Panel

Operations related to managing hosting accounts, such as managing websites content, adding and removing mailboxes, changing hosting settings, and so on, are available to you in a separate interface called *the Control Panel*.

The sections of this chapter explain how to perform hosting operations in the Control Panel. The instructions are applicable to your own subscriptions and subscriptions of your customers. This means that when we say *your website*, *your subscription*, and so on, we imply both your own and your customers' websites or subscriptions. The table below lists the sections of this chapter and briefly describes what you can learn from them.

Section	Description
Quick Start with Parallels Panel	Explains the workflow of setting up a website and a mail account in the Control Panel.
Customer Account Administration	Explains how to view and manage account settings, subscriptions, invoices, and resources in the Control Panel.
Websites and Domains	Explains how to create websites, fill them with content, add applications, and configure subscriptions' properties related to websites and domain names.
Building Websites with Presence Builder	Provides instructions on creating websites using Presence Builder - a visual website editor coming in a bundle with Panel.
FTP Access to Your Websites	Explains how to set up access to websites over the FTP for subscribers and auxiliary users.
Mail	Describes how to set up mail accounts and configure mail settings under subscriptions.
Scheduling Tasks	Provides instructions on configuring Panel to automatically run scripts at specific time.
Website Databases	Explains how to use databases under subscriptions: create new databases, import existing ones, or access external databases.
Backing Up and Recovering Websites	Provides instructions on backing up and restoring data of certain customer subscriptions on behalf of subscribers.

In this chapter:

Quick Start with Parallels Panel..... 326
 Customer Account Administration 350
 Websites and Domains 377
 Creating Sites with Presence Builder 467
 FTP Access to Your Websites 521
 Mail Accounts..... 526
 Scheduling Tasks..... 537
 Website Databases 542
 Backing Up and Recovering Websites..... 547

Quick Start with Parallels Panel

According to the latest studies, the Internet has become the most popular source of information in the world, leaving far behind all traditional media such as TV or newspapers. Nowadays, the first thing people do when trying to find services is to searching for them on the web. Thus, a proper web presence is vital for every business. There are a number of ways you can present your company on the Web. A web presence may be as simple as a contacts page, or as complex as a large company website with access to an ERP system. In both cases, you should perform the same steps to get your business online.

Before proceeding any further, you will need to take the following two essential steps:

- *Purchase a customer account from a hosting provider.*
Your customer account provides access to the services that are vital for a web presence - Internet connectivity, disk space to store your website content, and so on. For more information about customer accounts in Panel, refer to the chapter **Customer Account Administration**.
- *Register a domain name.*
This is the name people will use to access your site from their browsers. For example, `www.example.com`.

These two elements - an account for web hosting management and a domain name make up your *website*.

In this chapter, we will explain how to create your first website, fill it with content, create mailboxes for users of the site, and, finally, view the site visits statistics.

Advanced Hosting Features

Once you are comfortable with basic Panel capabilities, try out some advanced hosting features: Expand website functionality by installing web applications (on page 421), secure your sites with SSL certificates (on page 430), employ databases, and much more.

Note: Hosting providers can turn off some of the advanced features to make your Control Panel look simple and user friendly. We have used the **(Advanced)** prefix to designate the sections about features that may be turned off. If you require one of the advanced options, contact your hosting provider.

Next in this section:

Set Up Your First Website	327
Set Up Mail Accounts	331
View Site Visit Statistics	350

Set Up Your First Website

Now that you have a customer account and a domain name, the first thing you will want to do is create a website. The information about the possible ways to do it is provided in the section **1. Create Your Site** (on page 327)

When your site is ready, you may want to take a look at the result in your browser. Learn how to do it in the section **2. Preview your Site** (on page 330).

Next in this section:

1. Create Your Site.....	327
2. Preview Your Site.....	330

1. Create Your Site

There are three general ways to create a website:

- Employ a web design studio to create a site for you, and then you will just maintain its content.
- Create a site by yourself using *Presence Builder* - the powerful tool that allows you to create professional-looking websites in a few mouse clicks. Learn more in the section **Presence Builder** (on page 328).
- Create your website in a third-party *Content Management System* - an editor that allows you to easily create and edit website content such as pages, scripts, applications, and so on. To learn more about creating sites in third-party content management systems, see the section **Content Management Systems** (on page 328).

If you have purchased a ready-made site or created it by yourself, you should upload the site content to your account to make the site visible on the web. There are two ways to upload content:

- *Using FTP*. Learn more in the section **Uploading Content Using FTP** (on page 330).
- *Using an integrated File Manager*. Learn more in the section **Uploading Content with File Manager** (on page 330).

Next in this section:

Presence Builder.....	328
Content Management Systems.....	328
Uploading Content.....	329

Presence Builder

Presence Builder is a tool that enables users with no knowledge of HTML markup or graphic design skills to create professional-looking sites. This tool provides a simple visual editor and a huge set of templates for different websites. The editor allows you to create web pages, add content of different types (text, images, video, scripts), and edit website settings such as website name, keywords, icons, and so on.

To create websites in Presence Builder, ensure that your hosting subscription includes this option. If it does not, choose another way or upgrade your subscription.

➤ **To create a website with Presence Builder:**

1. Go to the **Websites & Domains** tab and click your domain name.
2. Click the link **Launch Presence Builder**.
3. Select a topic that best suits your website.
4. Edit the website:
 - a. *Structure*: add more pages, remove the predefined pages that you do not need.
 - b. *Content*: change the predefined content to your own, add text, images, videos, scripts, and other required elements.
 - c. *Design*: change the layout and color scheme.
5. Publish the website.

Find more information about creating websites with Presence Builder in the section **Building Websites with Presence Builder** (on page 467).

Content Management Systems

Content Management Systems (or *CMS*) are applications that provide a graphical user interface for adding and editing website content: pages, scripts, files, multimedia content, and so on.

Before you can create a website in a third-party CMS, you should install the CMS on your hosting account. Note that you can install the CMS only if your hosting subscription allows it.

➤ **To create a website using a CMS:**

1. Go to the **Applications** tab.
2. Find the CMS you need in the list of available applications, and install it as described in the section **Using Website Applications** (on page 421).
3. Create your website in the CMS. For information about creating websites with your CMS, refer to the relevant documentation.

Uploading Content

If you already have a website created by yourself or a web design studio, just upload the website files and folders to your provider's server. You can do this in one of the following ways:

- *Using FTP.* This way is better when several people manage a website's content because it does not require access to your customer account. You can just create FTP users for them. Learn more about this method in the section **Uploading Content Using FTP** (on page 330).
- *Using Control Panel File Manager.* This way is more convenient since it uses the Control Panel GUI and provides a set of useful features, for example, a visual HTML editor and a file permissions manager. Find more information on the features of File Manager in the section **Uploading Content with File Manager** (on page 330).

Next in this section:

Uploading Content Using FTP.....	330
Uploading Content with File Manager	330

Uploading Content Using FTP

➤ *To publish a website using FTP:*

1. Connect to your webspace on the server with an FTP client program, using your FTP account username and password.

You can change your username and password in the Panel at the **Websites & Domains** tab > **Web Hosting Access**.

The FTP address should be `ftp://your-domain-name.com`, where `your-domain-name.com` is your site's Internet address.

Enable the passive mode if you are behind a firewall.

2. Upload the files and directories of your site to the `httpdocs` directory. If you use CGI scripts, place them in the `cgi-bin` directory.
3. Close your FTP session.

You can also set up additional FTP accounts if you need to collaborate on website content with other users. For more information, see the section **Adding FTP Accounts** (on page 522).

Uploading Content with File Manager

To upload a website from your computer to Panel server with File Manager, open the **Files** tab of Control Panel and drag the website folder to the central area of this tab. You can also upload your website as a compressed ZIP file and then extract the contents using the archiver integrated in File Manager.

With File Manager, you can also do the following:

- Edit HTML files in the visual editor.
- Preview website pages.
- Edit files in the text editor.
- Manage the files' access permissions.

Learn more about uploading and editing website files and folders with File Manager in the section **Managing Website Content** (on page 413).

2. Preview Your Site

After you uploaded website files to the webspace, you can check how your site will look in a web browser, even before the information about the new site has spread in the Domain Name System.

➤ *To preview a site:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, select the required webspace in the **Subscription** menu at the top of the screen.

2. Go the **Websites & Domains** tab.
3. Click **Preview** below the domain name of the website that you want to preview.
Your site will open in a new browser window.

Note: The contents of password-protected directories might be inaccessible in the Preview mode.

Sometimes, you may need to show your site to someone when your domain name is not registered yet. There are several ways to do it without giving a person access to your customer account. Learn more in the section **Previewing Websites** (on page 420).

Set Up Mail Accounts

Once your website is ready, you can start creating mail accounts. You can choose, for example, to create mail accounts for all users within your organization. Note that the number and size of mailboxes is limited by your hosting plan.

Next in this section:

1. Create Mail Account 332
2. Access Your Mailbox 333

1. Create Mail Account

➤ *To create an e-mail address:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Click the **Mail** tab.
3. Click **Create E-mail Address**.
4. Type the left part of the e-mail address before the @ sign, and, if you have several domain names on your account, select the domain name under which the e-mail address will be created.
5. Leave the **Mailbox** checkbox selected.
Clearing this checkbox makes sense only if you want to use this address as a mail forwarder, which will forward all incoming mail to another address.
6. Specify the mailbox size or use the default size defined by the provider's policy or your service plan.
7. Specify a password consisting of five or more Latin characters.
8. Click **OK**.

2. Access Your Mailbox

There are two ways to access a mailbox for sending and receiving e-mail messages:

- Set up and use an e-mail client program on your computer. Typically, in such programs you should specify the following settings:
 - **Username.** In this field, specify your full e-mail address. For example, `johndoe@example.com`.
 - **Password.** Most likely, the password to your e-mail account.
 - **Mail server protocol.** This property defines whether you want to keep copies of messages on the server or not. To keep the copies on the server, select the **IMAP** option. If you do not want to keep them on the server, select **POP3**. Selecting IMAP will also allow you to train the SpamAssassin spam filter on e-mail messages you receive, if SpamAssassin is enabled on the server.
 - **Incoming mail server (POP3/IMAP).** Type your domain name. For example, `example.com`. The POP3 port is 110. The IMAP port is 143.
 - **Outgoing mail server (SMTP).** Type your domain name. For example, `example.com`. The SMTP port is 25. This server requires authentication.

To get detailed instructions on configuring popular e-mail clients to work with your mailbox, see subsections of this section.

- Use a web browser to connect to the webmail interface.


Note: If you cannot access your mailbox following the instructions in this section, this might be caused by mail server settings. Contact your hosting provider to resolve the issue.

Next in this section:

Access from Webmail.....	333
Access from Microsoft Office Outlook.....	334
Access from Microsoft Outlook Express	338
Access from Mozilla Thunderbird	342
Access from Apple Mail.....	345

Access from Webmail

➤ **To access your mailbox through webmail, do any of the following:**

- In a Web browser, visit the URL `webmail.example.com`, where `example.com` is the Internet address of your website. When prompted, specify your full e-mail address as the username (for example, `mail@example.com`), and specify the password that you use for logging in to the Panel.
- When logged in to the Panel, click the **Mail** tab, and in the list of e-mail addresses, click an icon  corresponding to the e-mail address you need.

Access from Microsoft Office Outlook

➤ *To set up Microsoft Office Outlook 2010:*

1. Open Microsoft Office Outlook.
2. Go to **File > Info > Add Account**.
3. Select the checkbox **Manually configure server settings or additional server types**. Click **Next**.

Add New Account

Auto Account Setup
Connect to other server types.

E-mail Account

Your Name:
Example: Ellen Adams

E-mail Address:
Example: ellen@contoso.com

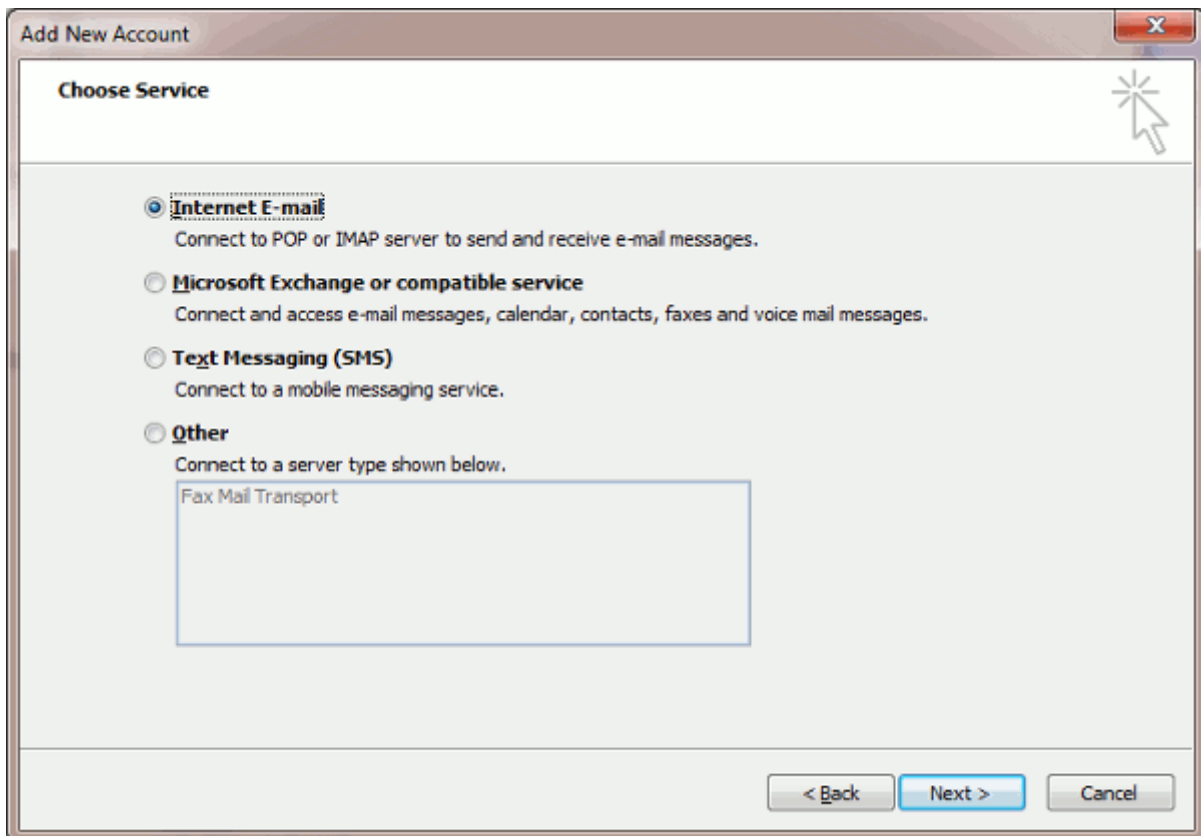
Password:
Retype Password:
Type the password your Internet service provider has given you.

Text Messaging (SMS)

Manually configure server settings or additional server types

< Back Next > Cancel

4. Select the **Internet E-mail** option and click **Next**.



5. Specify the following:

- Your name.
- Your e-mail address.
- **Account type.** If you want to keep copies of messages on the server, select the IMAP option. If you do not want to keep any messages on the server, select the POP3 option. Selecting IMAP will also allow you to train the SpamAssassin spam filter on e-mail messages you receive, if SpamAssassin is enabled on the server.
- Incoming mail server. Type your domain name. For example, example.com.
- **Outgoing mail server (SMTP).** Type your domain name. For example, example.com.
- **User Name.** Specify your full e-mail address. Example: johndoe@example.com.
- **Password.** Most likely, this password coincides with the password you use for logging in to Panel.
- **Require logon using Secure Password Authentication (SPA).** Leave this option cleared.

Add New Account

Internet E-mail Settings
Each of these settings are required to get your e-mail account working.

User Information

Your Name: John Doe

E-mail Address: mail@example.com

Server Information

Account Type: POP3

Incoming mail server: example.com

Outgoing mail server (SMTP): example.com

Logon Information

User Name: mail@example.com

Password: *****

Remember password

Require logon using Secure Password Authentication (SPA)

Test Account Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

Test Account Settings ...

Test Account Settings by clicking the Next button

Deliver new messages to:

New Outlook Data File

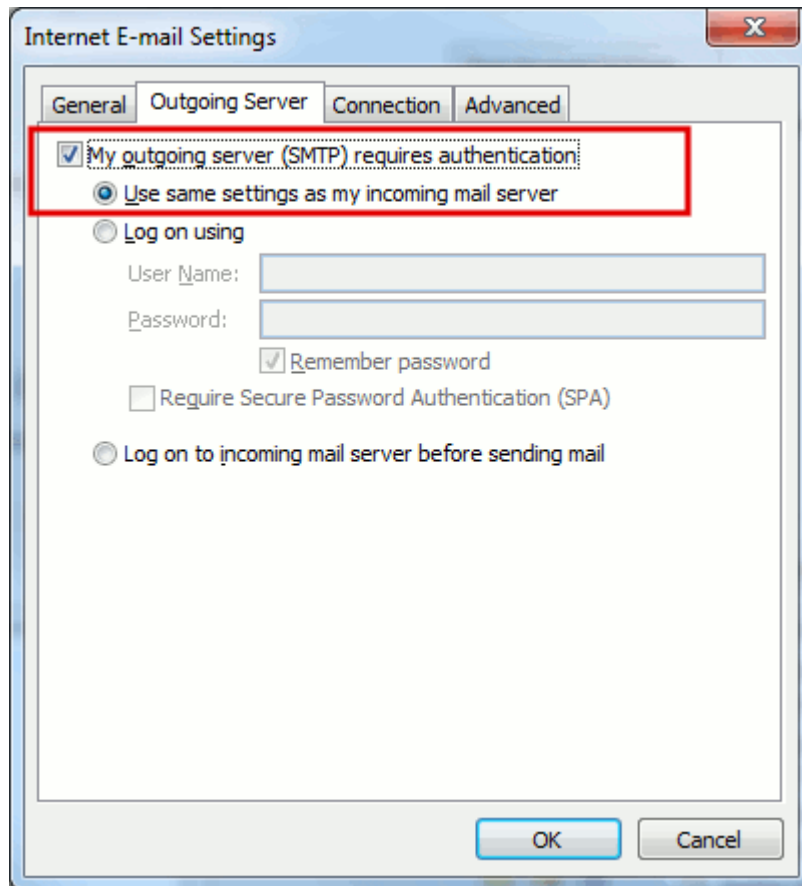
Existing Outlook Data File

Browse

More Settings ...

< Back Next > Cancel

6. Click **More Settings**, open the **Outgoing Server** tab and check **My outgoing server (SMTP) requires authentication**.



7. Click **Next**.
8. Click **Finish**.

Access from Microsoft Outlook Express

The instructions provided in this section were verified against Microsoft Outlook Express 6. They might not work with earlier or later versions of Microsoft Outlook Express.

➤ **To set up Microsoft Outlook Express:**

1. Open Microsoft Outlook Express.
2. Go to **Tools > Accounts**.
3. Click the **Add** button and select the **Mail** item.
4. Enter your name as you want it to appear in any messages you send, and click **Next**.

Internet Connection Wizard

Your Name

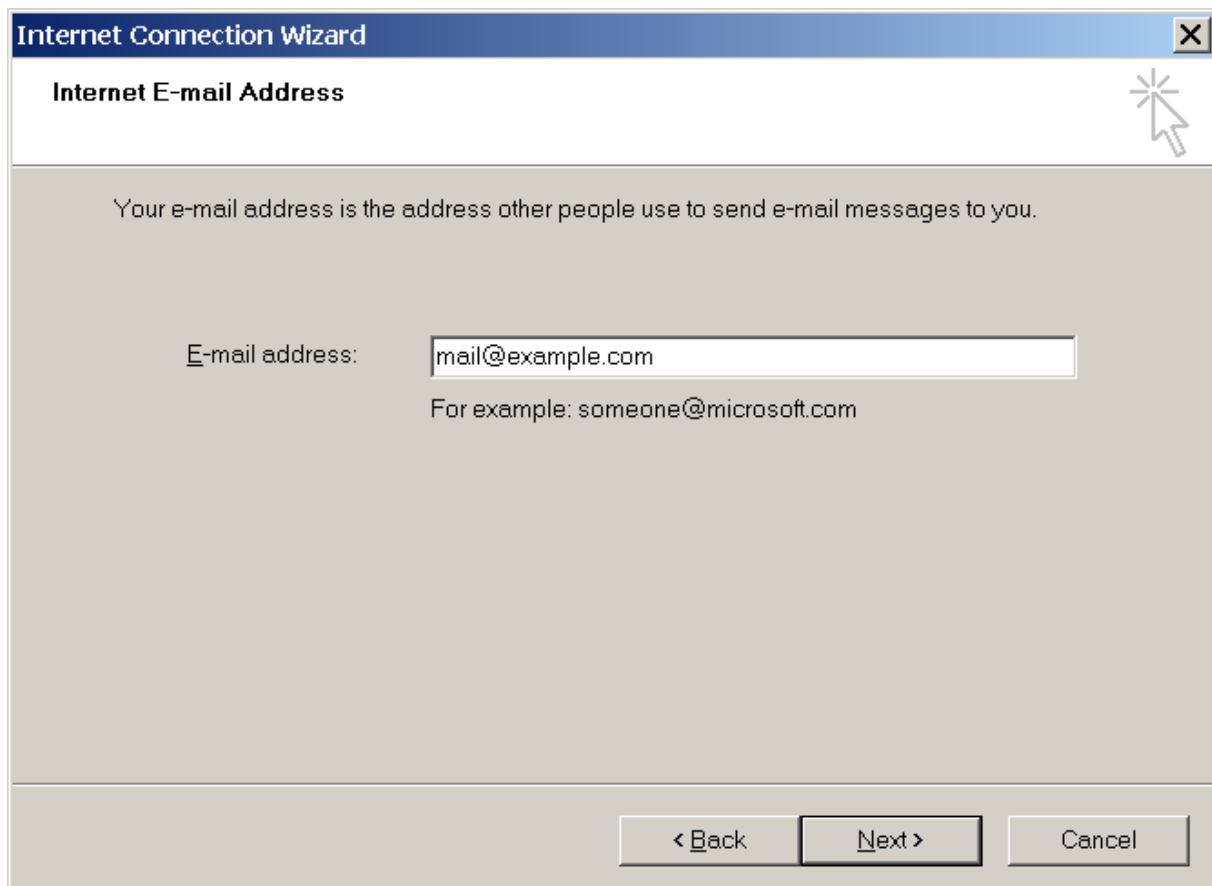
When you send e-mail, your name will appear in the From field of the outgoing message.
Type your name as you would like it to appear.

Display name:

For example: John Smith

< Back Next > Cancel

5. Type your e-mail address, and click **Next**.



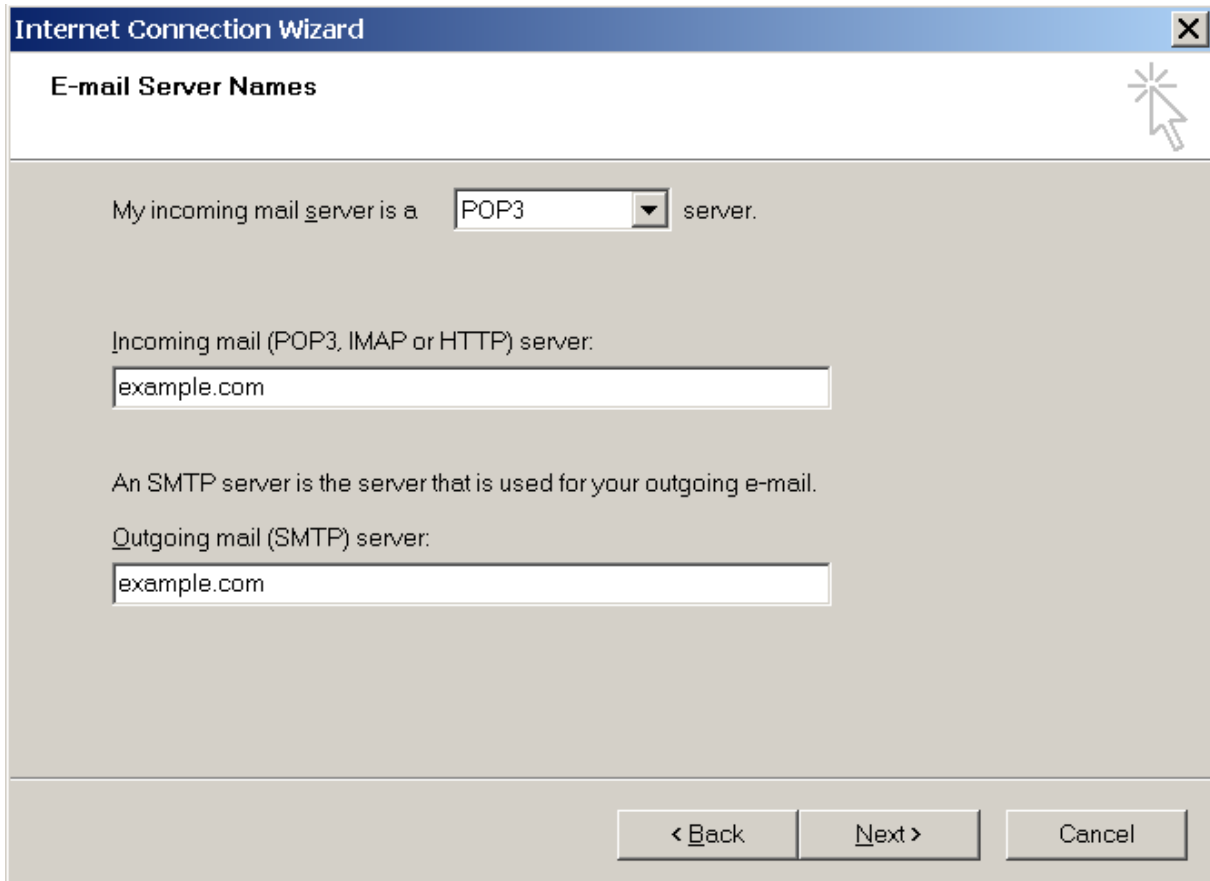
The screenshot shows a dialog box titled "Internet Connection Wizard" with a close button (X) in the top right corner. The main title of the dialog is "Internet E-mail Address". Below the title, there is a mouse cursor icon. The main text reads: "Your e-mail address is the address other people use to send e-mail messages to you." Below this text, there is a label "E-mail address:" followed by a text input field containing "mail@example.com". Underneath the input field, there is a hint text: "For example: someone@microsoft.com". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

6. Specify the following settings:

- Protocol of your incoming mail server.

If you want to keep copies of messages on the server, select the **IMAP** option. If you do not want to keep any messages on the server, select the **POP3** option. Selecting IMAP will also allow you to train the SpamAssassin spam filter on e-mail messages you receive, if SpamAssassin is enabled on the server.

- Incoming mail server. Specify your website's Internet address.
- Outgoing mail server. Specify your website's Internet address.



The screenshot shows a dialog box titled "Internet Connection Wizard" with a close button (X) in the top right corner. The main title of the dialog is "E-mail Server Names".

The dialog contains the following text and controls:

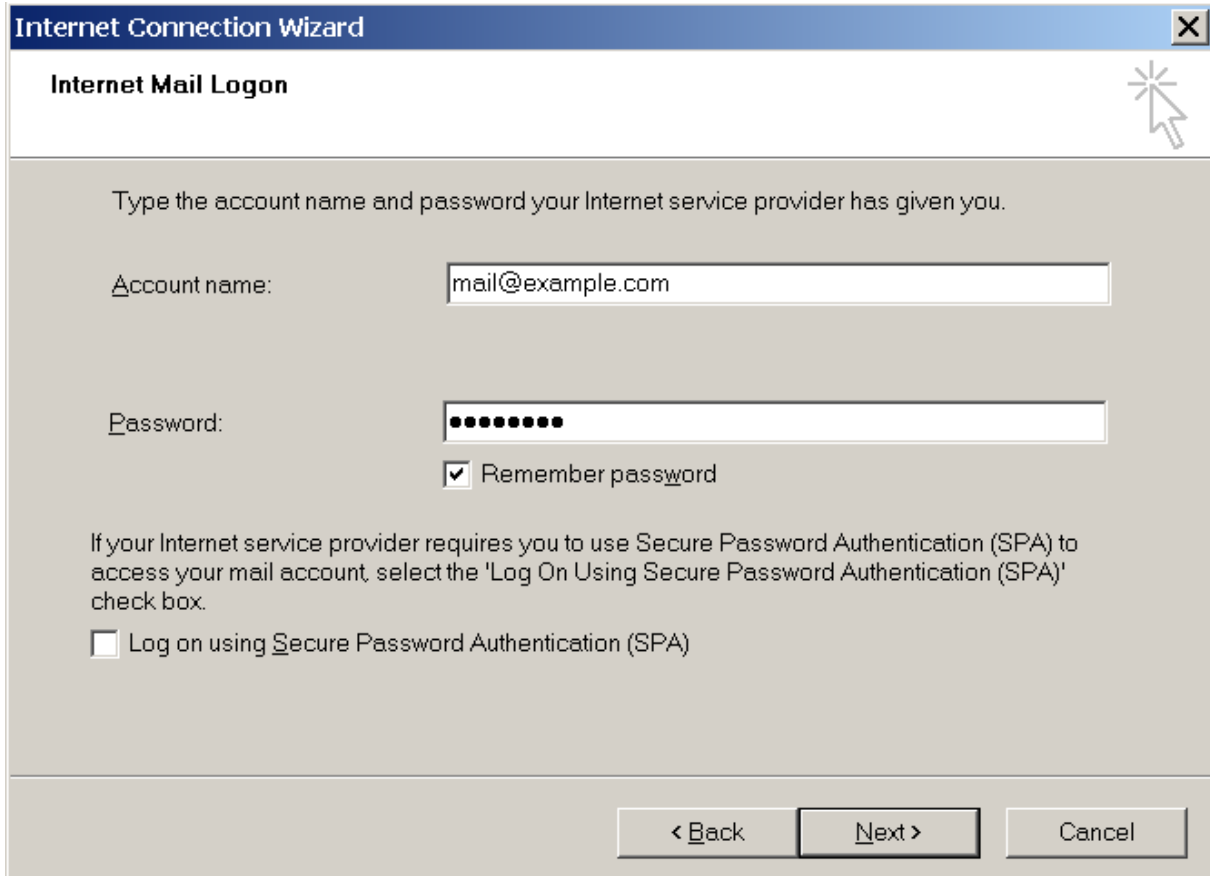
- "My incoming mail server is a server." (The dropdown menu is currently set to "POP3".)
- "Incoming mail (POP3, IMAP or HTTP) server:" followed by a text input field containing "example.com".
- "An SMTP server is the server that is used for your outgoing e-mail."
- "Outgoing mail (SMTP) server:" followed by a text input field containing "example.com".

At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

7. Click **Next**.

8. Specify the following:

- Your account name. Type your e-mail address in the **Account name** box.
- Your password. Most likely, this password coincides with the password you use for logging in to the Panel.
- **Remember password** checkbox. Leave it selected if you do not want to be prompted to enter password each time your e-mail program connects to the mail server to check for new mail, and click **Next**.



The screenshot shows a Windows-style dialog box titled "Internet Connection Wizard" with a close button (X) in the top right corner. The main title bar is blue. Below the title bar, the text "Internet Mail Logon" is displayed in a bold font, with a help icon (a mouse cursor pointing to a starburst) to its right. The main area of the dialog is light gray and contains the following text: "Type the account name and password your Internet service provider has given you." Below this text are two input fields. The first is labeled "Account name:" and contains the text "mail@example.com". The second is labeled "Password:" and contains a series of ten black dots. Below the password field is a checked checkbox labeled "Remember password". At the bottom of the main area, there is a paragraph of text: "If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your mail account, select the 'Log On Using Secure Password Authentication (SPA)' check box." Below this text is an unchecked checkbox labeled "Log on using Secure Password Authentication (SPA)". At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

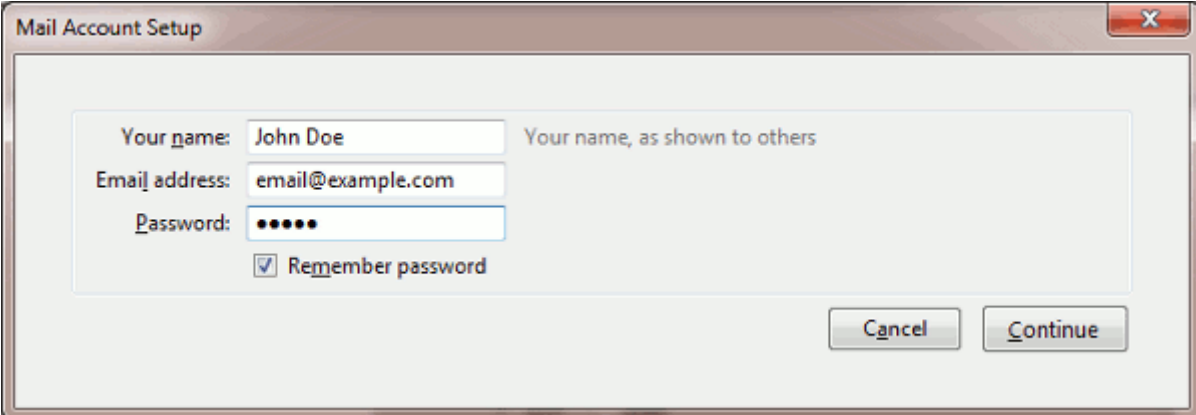
9. To complete setting up your e-mail program, click **Finish**.

Access from Mozilla Thunderbird

The instructions provided in this section were verified against Mozilla Thunderbird 12. They might not work with earlier or later versions of Mozilla Thunderbird.

➤ *To set up Mozilla Thunderbird:*

1. Open Mozilla Thunderbird.
2. Go to **Tools > Account Settings > Account Actions > Add Mail Account**.
3. Specify the following:
 - Your name, as you want it to appear in any messages you send.
 - Your e-mail address and password.



The screenshot shows a dialog box titled "Mail Account Setup" with a close button (X) in the top right corner. The dialog contains three input fields: "Your name:" with the text "John Doe" and a label "Your name, as shown to others" to its right; "Email address:" with the text "email@example.com"; and "Password:" with six dots. Below the password field is a checked checkbox labeled "Remember password". At the bottom right of the dialog are two buttons: "Cancel" and "Continue".

4. Click **Continue**.
5. If Thunderbird fails to find the settings automatically, specify the following:
 - Account type. If you want to keep copies of messages on the server, select the **IMAP** option. If you do not want to keep any messages on the server, select the **POP3** option. Selecting IMAP will also allow you to train the SpamAssassin spam filter on e-mail messages you receive, if SpamAssassin is enabled on the server.

Mail Account Setup

Your name: John Doe Your name, as shown to others

Email address: email@example.com

Password: ●●●●

Remember password [Start over](#)

Thunderbird failed to find the settings for your email account.

Username: email@example.com [Re-test Configuration](#)

Incoming: example.com POP 110 None

Outgoing: example.com SMTP 25 None

[Manual Setup...](#) [Cancel](#) [Create Account](#)

6. Click **Create Account**.

If you set up a mail account manually, please use the following typical combinations of connection security and authentication method settings. If the settings do not work for you, ask your hosting provider about the correct combination.

On Linux:

- **Connection security:** STARTTLS
- **Authentication method:** Encrypted password

On Windows, IMAP:

- **Connection security:** None
- **Authentication method:** Encrypted password

On Windows, POP3:

- **Connection security:** None

Authentication method: Password, transmitted insecurely Other parameters that you may need when configuring your account manually:

- **POP3 port:** 110
- **IMAP port:** 143
- **SMTP port:** 25
- **Username.** Your full e-mail address. For example: johndoe@example.com.
- **Incoming server address (POP3/IMAP).** Specify your website's Internet address. Example: *example.com*
- **Outgoing server address.** Specify your website's Internet address. Example: *example.com*

Access from Apple Mail

The instructions provided in this section were verified against Apple Mail 3.6 (Leopard). They might not work with earlier or later versions of Apple Mail.

➤ **To set up Apple Mail:**

1. Run Apple Mail.

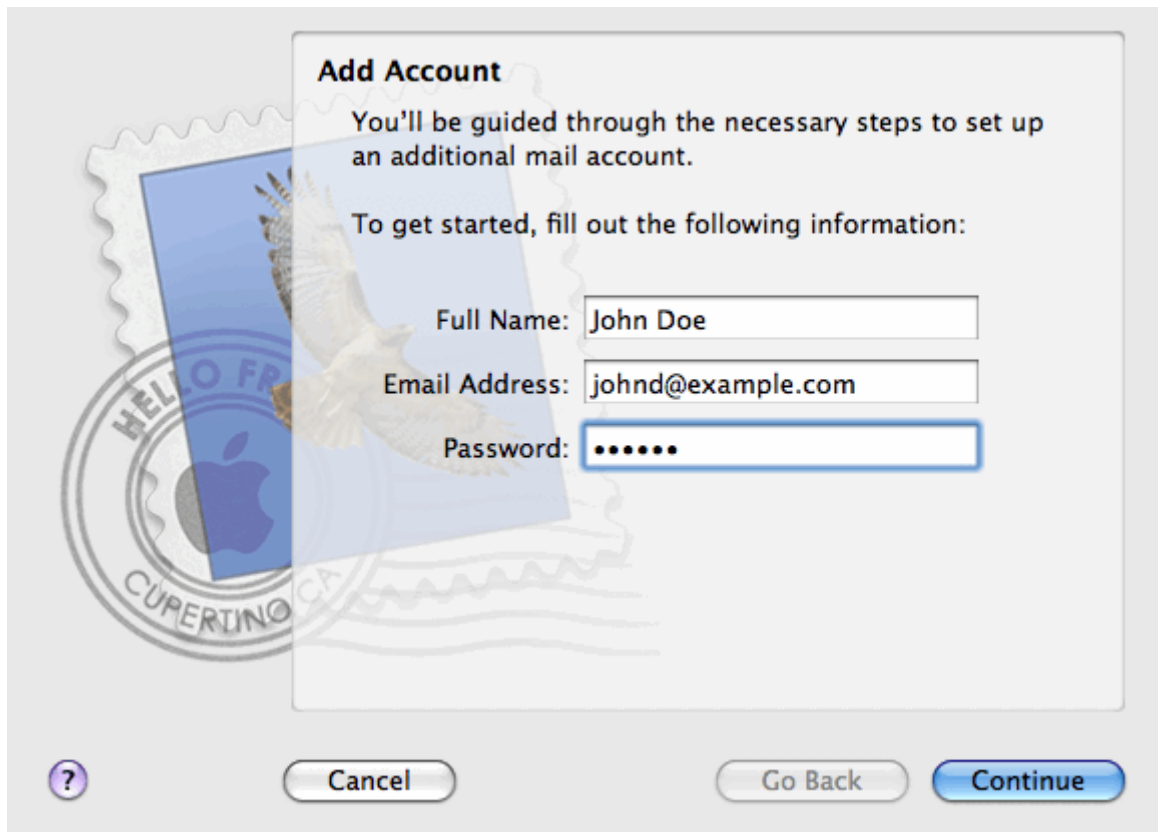
If you run it for the first time and do not have any mail accounts configured in it, skip the next step: Apple Mail will take you directly to creating one.

2. Open the Adding Mail Account wizard:

- a. Click **Mail > Preferences....**
- b. Select the **Accounts** tab.
- c. Click the **+** button at the bottom left corner.

3. Enter the account information:

- Your full name
- Your full e-mail address
- The password you use to log in to the Panel.



4. Click **Continue**.

5. Fill in the following incoming mail server information:

- **Account Type:** select whether you want to use IMAP or POP protocol.

We recommend selecting IMAP if you use SpamAssassin as a spam filtering solution: IMAP account is a requirement for SpamAssassin learning which messages are spam and which are not.

- **Incoming Mail Server:** type in the name of domain which serves your mail (which follows the @ sign in your e-mail address).
- **User Name:** enter your full e-mail address.
- **Password:** leave it auto-completed (Apple Mail takes it from the previous step).

Incoming Mail Server

Account Type:

Description:

Incoming Mail Server:

User Name:

Password:

? Cancel Go Back Continue

6. Click **Continue**.
7. (Optional) Specify the incoming mail security options:
 - a. Select the **Use Secure Sockets Layer (SSL)** checkbox.
 - b. Select the authentication method.

Keep the default method if you are not sure which to select.

Apple Mail displays this setup screen only if a mail server bundled with Panel supports SSL for the selected account type (POP or IMAP).



8. Click **Continue**.
9. Fill in the following outgoing mail server information:
 - **Outgoing Mail Server:** type in the name of domain which serves your mail (which follows the @ sign in your e-mail address).
 - **Use only this server:** selected.
 - **Use Authentication:** selected.
 - **User Name:** enter your full e-mail address.
 - **Password:** leave it auto-completed (Apple Mail takes it from the previous step).

Outgoing Mail Server

Description: (optional)

Outgoing Mail Server: example.com

Use only this server

Use Authentication

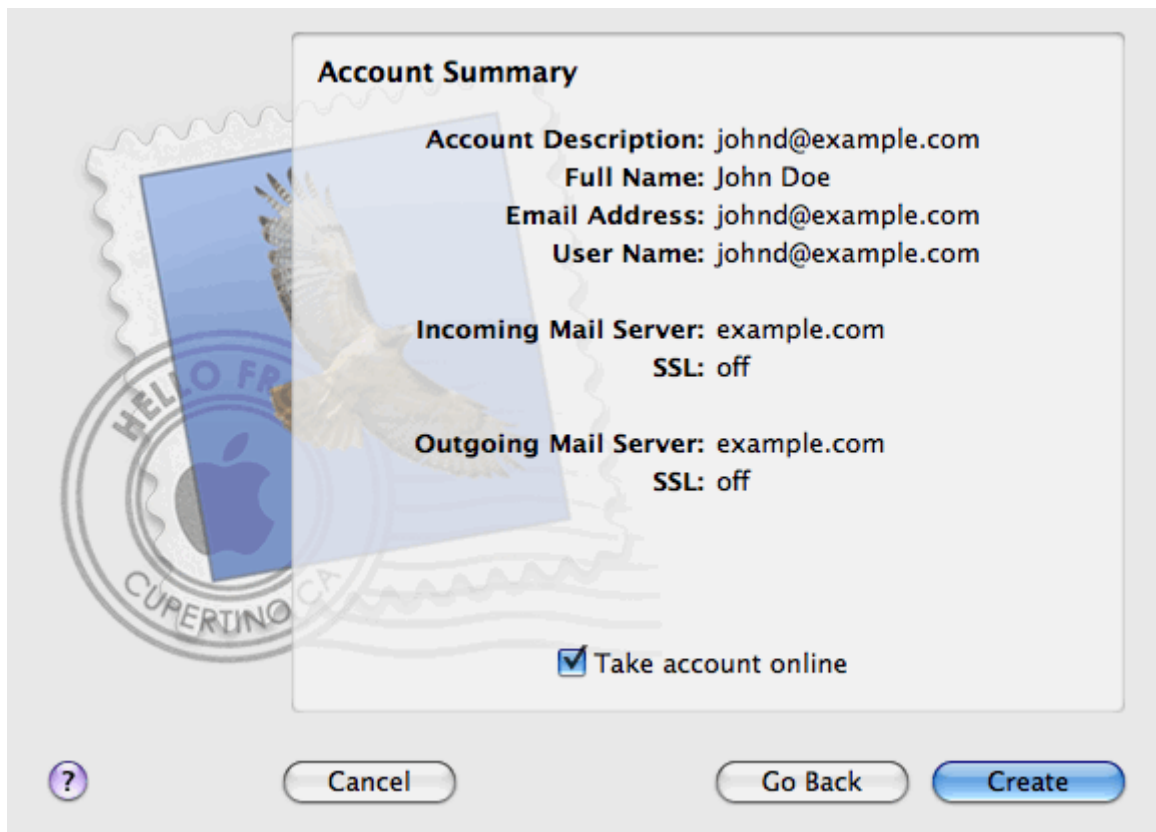
User Name: johnd@example.com

Password:

? Cancel Go Back Continue

10. Click Continue.

Apple Mail displays overall description of the mail account that is going to be created.

11. Select the Take account online checkbox and click Create.

View Site Visit Statistics

Finally, when your site works fine and search engines return it in search results, it is the best time to evaluate site efficiency by viewing the visits statistics.

➤ **To find out how many people visited a site, from what countries, and what pages of the site they viewed:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the domain name for which you want to view the statistics
3. Click **Web Statistics**.
The site visitor statistics will show in a new browser window.
4. To view statistics for web pages viewed from the SSL-secured area of your site, select **SSL Web Statistics** in the menu.
5. To view statistics for files downloaded over the file transfer protocol (FTP), select **FTP Statistics** in the menu.

Alternately, you can view the visits statistics for a site by visiting the following URL: <https://your-domain.com/plesk-stat/webstat>. When prompted for username and password, specify your FTP account username and password.

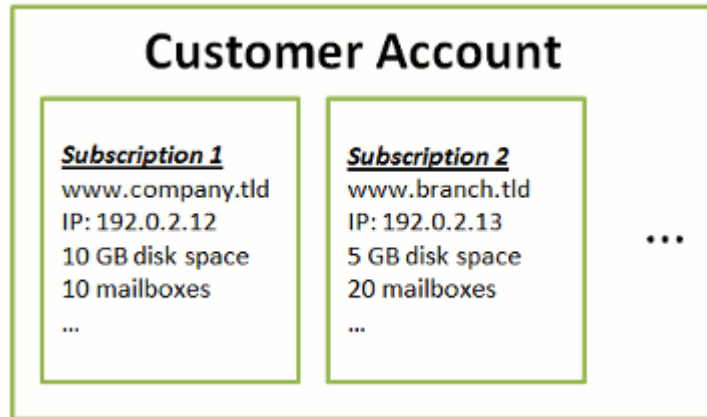
You have successfully completed the quick start part of the guide. Feel free to read about other features that are available to you in the Control Panel.

Customer Account Administration

As described in the section **Quick Start with Parallels Panel**, the first step in establishing your company's web presence is signing up to the services provided by a hosting company (hosting provider). After you subscribe to a hosting plan, a *customer account* in Panel is created to enable you to log in to Panel and use the hosting services and resources like mailboxes, disk space, and bandwidth.

Customer Account and Multiple Subscriptions

Panel allows you to subscribe to as many hosting plans as you need. For example, if you do not want your main site to share hosting resources with a company's branch site you can subscribe to another hosting plan under the same customer account. In other words, a customer account is a personalized access to all your subscriptions (see the picture below).



Another reason for using multiple subscriptions is that subscription is limited to *only one IPv4 and one IPv6 address*. Thus, all domains within a subscription share the same IP address (v4 or v6). If you need to host sites on different IP addresses, you should additionally order the same plan for as many IP addresses as you need. This can be useful, for example, if you want to secure connections to each of your sites with a separate SSL certificate. For information on how to purchase an additional subscription, refer to the section **Ordering More Resources** (on page 366).

If you have multiple subscriptions under a single customer account, you can easily switch among them from the **Account** tab. To be more specific, the **Account** tab provides access to operations that apply to *all your subscriptions*. All other tabs (like **Mail**, **Users**, or **Domains & Websites**) are, on the contrary, *subscription-wide*. This means that to change mail settings on a particular subscription, *you should first switch to it* before clicking **Mail**.

System Users

For each hosting subscription, Panel creates a *system user* - a user account in the Panel server operating system. Customers obtain their system users' access credentials from their service providers and use these credentials for connecting to the server through FTP, SSH, and so on. In addition, all operations with files and directories in Panel are performed on behalf of system users. For example, when a customer adds a new file in File Manager, the subscription's system user becomes the owner of the file.

Adding Resources to a Subscription

Purchasing a new subscription for extending hosting resources is not always necessary. You can always improve just one of your subscriptions. For example, add extra disk space or SSL support. This can be done by switching to another hosting plan or by purchasing hosting plan add-ons. Learn more in the section **Ordering More Resources** (on page 366).

Managing Customer Account

In Panel, you can perform a number of administrative operations on your customer account:

- Change an account password and personal information. Learn more in the section **Changing Your Password and Contact Information** (on page 354).
- View the list of services and resources provided by subscription on the **Account** tab. For detailed information about all subscription features, refer to the section **Viewing Subscription Summary** (on page 355).
- Make payments to renew your subscription. Learn more in the section **Managing Account Balance and Invoices** (on page 362).
- View statistics on your account: For example, disk space or traffic usage. Learn more in the section **Viewing Statistics** (on page 368).

Allowing Other Users to Access Your Account

If the number of hosting maintenance operations is too large to be handled by one person, you can delegate some of them to other people. For this purpose, you can create auxiliary user accounts grouped by means of user roles. For example, you can create a group that is allowed to only upload content to websites. Users in this group will not be able to perform any operations except for managing website content. For more information about auxiliary users, refer to the section **(Advanced) Managing Auxiliary User Accounts** (on page 370).

Next in this section:

Changing Your Password and Contact Information	354
Viewing Subscription Summary	355
Managing Account Balance and Invoices	362
Ordering More Resources	366
Viewing Statistics	368
(Advanced) Managing Auxiliary User Accounts	370

Changing Your Password and Contact Information

➤ *To change your password for access to the Control Panel:*

1. Click a link with your name at the top of the screen.
2. Type a new password, and click **OK**.

➤ *To change a username or password that you use for connecting to your subscription over FTP or SSH:*

1. Click the **Websites & Domains** tab.
2. Click **Web Hosting Access**.
3. Type the new username or password, and click **OK**.

➤ *To change your contact information:*

1. Click a link with your name at the top of the screen.
2. Click the **Contact Details** tab.
3. Update your contact information and click **OK**.

Viewing Subscription Summary

When you subscribe to hosting services, a user account is created in the Panel to allow you to manage your websites and mailboxes on your own.

You can view the following information about your account:

- Current subscriptions to service plans.
You can be subscribed to a number of service plans at once, and, therefore, can have several subscriptions associated with your account. If a billing system is connected to the Panel, then you can also purchase additional subscriptions, upgrade or downgrade them, and pay your invoices.
- Allocated and consumed resources.
- Hosting features available for your websites.
- Operations you can perform in your Panel.
- Account balance, unpaid invoices, and monthly fee for your hosting package.

➤ ***To view the information about your account and your current subscriptions:***

1. Click the **Account tab.**

A list of your current subscriptions is shown.

2. If the billing system is integrated with the Panel, then the following information is shown:

- **Account credit balance.** This is how much money is available in your billing account.
- **Due invoices balance.** This is how much money you owe to your provider. Here, you can pay all invoices at once by clicking **Pay All Outstanding Invoices**, or pay one of invoices by clicking a **Pay Now** link in the list titled **Latest Outstanding Invoices**. You can also view all invoices by clicking the link **Show all invoices**, or print an invoice by clicking an invoice number and then clicking **Print**.
- **Latest to-do items.** This shows reminders from the system about the actions you need to take.
- List of all your subscriptions. You can use links in the list to perform the following operations:
 - View subscription properties by clicking a link with subscription name.
 - Select a subscription that you want to manage through the Control Panel by clicking the corresponding link **Switch to Subscription**.
 - Order an SSL certificate for a site by clicking **Request SSL Certificate**. This operation is described in the section **Ordering SSL Certificates**.
 - View properties of already ordered SSL certificates by clicking **Show Certificate Info**.
 - View or change domain information, contact information, and DNS settings specified at a registrar's site, by clicking **Show Domain Info**. These operations are described in the section **Registrar's DNS Settings in Panel** (on page 392).

3. To view detailed information about resource allotments, available hosting options, and permissions for operations, click a subscription's name.
4. Do any of the following:
 - To view a list of allocated and consumed resources, click the **Resources** tab.
 - To view a list of hosting features available for your account, click the **Hosting Options** tab.
 - To view a list of operations that you can perform in your Hosting Panel, click the **Permissions** tab.

Next in this section:

Allocated and Consumed Resources.....	357
Hosting Features Available for Your Websites.....	359

Allocated and Consumed Resources

If you are subscribed to a number of service plans at once, then you have several subscriptions. For each subscription, the following types of allocated resources are listed in the Panel at the **Account** tab > *subscription name* > **Resources** tab:

- **Disk space.** This is the total amount of disk space allocated to your account with subscription. This amount includes all data related to your websites, e-mail accounts, applications, backups, and log files.
- **Traffic.** This is the total amount of data in megabytes that can be transferred monthly from all your websites.
- **Domains.** This is the number of websites that can have separate second-level domain names, such as, for example, example.com.
For information about setting up websites, refer to the sections **Set Up Your First Website** (on page 327) and **Adding Domains** (on page 379).
- **Subdomains.** This is the number of additional websites that can have third-level domain names, such as, for example, news.example.com.
For information about setting up subdomains, refer to the section **Adding Subdomains** (on page 381).
- **Domain aliases.** This is the number of additional domain names that can be set up to point to one of your sites. For example, example.fr and example.de can both point to example.com.
For information about setting up domain aliases, refer to the section **Adding Domain Aliases** (on page 383).
- **Mailboxes.** This is the number of mailboxes that can be created under all your websites.
For information about creating mailboxes, refer to the chapter **Mail**.
- **Mailbox size.** This is the amount of disk space that can be occupied by a mailbox.
- **Total mailboxes quota.** This is the total amount of disk space that can be used by all mailboxes under all your domains. This option is available only on Windows-based customer accounts.
- **Mailing lists.** This is the total number of mailing lists that can be set up under all your websites. Note that there are mailing lists and mail groups, which serve the same purpose, but are slightly different in functionality. Mailing lists support archiving and pre-moderation of messages, while mail groups can only be used for sending one message to a number of recipients at once.
For information about setting up and using mailing lists, refer to the section **Using Mailing Lists** (on page 536).
- **Additional FTP accounts.** This is the number of FTP accounts that can be set up for accessing the webspace, in addition to the main FTP account that was created when your subscription was activated.
For information about setting up FTP accounts, refer to the sections **Changing FTP Access Credentials** (on page 521) and **Adding FTP Accounts** (on page 522).
- **Databases (Linux).** This is the number of databases that can be hosted for all your websites. Databases are a standard means of organizing data storage that allows dynamic websites, web applications, and their users to store, search, and retrieve information.
For information about working with databases, refer to the chapter **(Advanced) Using Databases**.

- **MySQL databases and Microsoft SQL Server databases (Windows).** This is the maximum number of MySQL and Microsoft SQL Server databases respectively that can be created on the Panel database servers and used by the subscription's websites.
- **MySQL databases quota and Microsoft SQL databases quota (Windows).** This is the maximum amount of disk space (in megabytes) that the subscription's MySQL and Microsoft SQL Server databases respectively can occupy.
- **Java applications.** This is the number of Java applications packaged in WAR format that you can install on your sites.
- **Sites published with Presence Builder.** This is the number of sites that you can create and publish using Presence Builder, if Presence Builder option is included in your hosting package.
- **Mobile sites.** This is the total number of websites that you can host with the UNITY Mobile online service, which optimizes sites for viewing on mobile devices.
- **Web users.** This is the number of user accounts that you can create for hosting web pages for other users under your domains.
- **FrontPage accounts.** This is the number of Microsoft FrontPage user accounts that you can create for collaboration on site content using FrontPage. This option is available only for Windows-based customer accounts.
- **Shared SSL links.** This is the number of websites that you can secure with an SSL certificate shared by your provider. This option is available only for Windows-based customer accounts.
- **ODBC DSN connections.** This is the number of connections to external databases that you can create for web applications running on your customer account. This option is available only for Windows-based customer accounts.
- **ColdFusion DSN connections.** This is the number of connections to external databases that you can create for web applications written in Adobe ColdFusion, which are running on your customer account. This option is available only for Windows-based customer accounts.

Hosting Features Available for Your Websites

Depending on your service plan, the following hosting features may be available for your websites (listed at the **Account** tab > *subscription name* > **Hosting Options** tab):

- **SSL support.** This allows you to secure connections to websites with SSL encryption. For information about securing sites with SSL, refer to the section **Securing Connections with SSL Certificates** (on page 430).
- **Web statistics.** This allows you to view website visits statistics presented in diagrams and charts. For information about viewing website visits statistics, refer to the section **Viewing Statistics** (on page 368).
- **Custom error documents.** This allows you to create custom HTML pages and configure web server to show them instead of typical error messages, such as `404 Not Found`. For information about setting up custom error documents, refer to the section **Setting Up Custom Error Pages** (on page 439).
- **Support for programming and scripting languages**, such as PHP, CGI, Perl, Python, Microsoft ASP, ASP.NET, Adobe ColdFusion, SSI.
- **Microsoft FrontPage support and Microsoft FrontPage over SSL support.** These allow you to use Microsoft FrontPage to create and edit website content. These options are available only for Windows-based customer accounts.
- **Remote Microsoft FrontPage authoring (Windows).** This allows you to use Microsoft FrontPage to create and edit website content directly on the server. This option is available only for Windows-based customer accounts.
- **Dedicated IIS application pool (Windows).** This provides isolation and improved stability for web applications working on sites.
- **Additional write/modify permissions (Windows).** This option allows the web applications to use a file-based database (like Jet) located in the root of `httpdocs` folder.
- **Allow web users to use scripts.** This allows scripting at web pages available at URLs like `http://example.com/~<username>/<webpage>`, where *<username>* refers to a web user. Web users are individuals who do not need their own domain names. This service is popular with educational institutions that host non-commercial personal pages of their students and staff.

The following is a list of permissions for operations that you can perform in your Panel (shown at the **Account** tab > *subscription name* > **Permissions** tab):

- **DNS zone management.** Manage resource records in the DNS zones of websites. DNS stands for Domain Name System. It is a service that enables web browsers to locate websites by domain names. For information about configuring DNS settings for your websites, refer to the section **(Advanced) Configuring DNS for a Domain** (on page 386).
- **Hosting settings management.** Manage web hosting settings, such as custom web server settings or support for scripting languages.

- **PHP safe mode management.** This option is available only for Linux-based customer accounts. It allows you to switch PHP safe mode on or off for websites. Safe mode is a security restriction that does not allow scripts written in PHP to perform potentially dangerous operations on the server. You might need to switch off the safe mode for PHP if you use some web applications written in PHP and if they do not function properly.
- **Management of access to the server over SSH and Management of access to the server over Remote Desktop.** Securely upload web content to the server through Secure Shell (Linux) or a Remote Desktop connection (Windows).
- **Anonymous FTP management.** Set up a folder on the server which should be accessible to the Internet users over FTP protocol. This folder can have an address like, for example, ftp://downloads.example.com. This feature is called anonymous FTP because the users will not need to specify a username and password to browse, download, or upload files. For information about setting up FTP folder with unrestricted access, refer to the section **Setting Up Anonymous FTP Access** (on page 524).
- **Scheduler management.** Schedule execution of programs or scripts in the server's operating system.
For information about scheduling tasks, refer to the chapter **Scheduling Tasks**.
- **Spam filter management.** Set custom settings for protection from unsolicited commercial e-mail, also known as spam.
For information about setting up spam filtering, refer to the section **Protecting Mailboxes from Spam**.
- **Antivirus management.** Set custom settings for protection from viruses and other malicious software that spreads itself through e-mail.
For information about setting up virus protection, refer to the section **Protecting Mailboxes from Viruses**.
- **Data backup and restoration using the server repository.** Use the backup and restore functions of the Panel to back up and restore websites, mail accounts, settings, and keep your backup files on the server.
For information about backing up and restoring data, refer to the chapter **(Advanced) Back Up and Restore Data**.
- **Data backup and restoration using a personal FTP repository.** Use the backup and restore functions of the Panel to back up and restore websites, mail accounts, settings, and save your backup files to an FTP folder on another server.
For information about backing up and restoring data, refer to the chapter **(Advanced) Back Up and Restore Data**.
- **Web statistics management.** Set custom preferences for visitor statistics reports.
For information about configuring and viewing website visitor statistics, refer to the section **Viewing Statistics** (on page 368).
- **Log rotation management.** Set custom preferences for recycling (rotation) of web server logs. Web server records information about connections to your sites and errors occurred on attempts to retrieve missing files. You can use these log files for website debugging purposes.
For information about working with web server access logs, refer to the section **Log Files** (on page 369).
- **Access to Application Catalog.** View and install applications on websites. For information about applications, refer to the section **Employing Website Applications** (on page 421).
- **Setup of potentially insecure web scripting options that override provider's policy.** This allows you to override the hosting security policy, if it is applied by the provider.

- **Domain creation.** Set up and manage new websites.
For information about setting up websites, refer to the sections **Set Up Your First Website** (on page 327) and **Adding Domains** (on page 379).
- **Subdomains management.** Set up and manage new websites with addresses like forum.example.com.
For information about setting up subdomains, refer to the section **Adding Subdomains** (on page 381).
- **Domain aliases management.** Set up and manage additional domain names for a site.
For information about setting up domain aliases, refer to the chapter **Adding Domain Aliases** (on page 383).
- **Additional FTP accounts management.** Set up and manage additional FTP accounts. To enable collaboration on website content, you can set up FTP accounts for other users and specify which directories of the site should be accessible to them.
For information about setting up FTP accounts, refer to the section **Adding FTP Accounts** (on page 522).
- **Java applications management.** Install and manage Java applications distributed in WAR archives and obtained separately from third-party vendors or application developers.
For information about installing Java applications, refer to the section **Installing Java Applications**.
- **Mailing lists management.** Set up and manage mailing lists.
For information about setting up and using mailing lists, refer to the section **Using Mailing Lists** (on page 536).
- **Hosting performance settings management.** Limit the bandwidth and number of connections to websites.
For information about restricting bandwidth usage for sites, refer to the section **Limiting Bandwidth and Number of Connections to Websites** (on page 446).
- **IIS application pool management.** Set custom preferences for IIS application pool (available only on Windows-based customer accounts).
For information about setting up IIS application pool, refer to the section **Setting Up IIS Application Pool (Windows)** (on page 465).
- **Additional write/modify permissions management.** Set additional write/modify permissions for websites that use file-based databases (available only on Windows-based customer accounts).
- **Shared SSL management.** Secure connections to your sites with SSL protection by using an SSL certificate shared by your provider.
For more information, refer to the section **Using Shared SSL Certificates (Windows)** (on page 434).
- **Hard disk quota assignment.** Adjust hard quotas on disk space if that is supported by your customer account.
- **Database server selection.** Select a database server for creating databases, if multiple database servers are available.

Managing Account Balance and Invoices

The operations described below are available if your Control Panel is integrated with Parallels Parallels Customer and Business Manager.

➤ **To view your account balance and pay for hosting services:**

1. Click the **Account** tab.
2. The following information is shown:
 - *Account credit balance.* This is how much money is available in your account.
 - *(Optional) Usage charge.* If your subscription allows consuming hosting resources over the plan limit, this number shows how much money you should pay for these resources in addition to your subscription price. To view the detailed information about how much resources you used over limits, click the link **See details** below the charge amount. To learn how the system calculates usage charges, see the section **Calculating Usage Charges** (on page 364).
 - *Due invoices balance.* This is how much money you owe to your provider. Here, you can pay all invoices at once by clicking **Pay All Outstanding Invoices**, or pay one of invoices by clicking a **Pay Now** link in the list titled **Latest Outstanding Invoices**.
 - *Latest to-do items.* This shows reminders from the system about actions you need to take.
 - *(Optional) Affiliate programs.* Your provider may let you earn money for promoting their plans. To start earning, you should join their *affiliate programs*. Here you can find the link to join affiliate programs or the info about your money you earn if you already joined the programs. To learn how to get profit from affiliate programs, see the section **Earning Money by Promoting a Provider's Plans** (on page 364).
 - *List of all your subscriptions.* You can use links in the list to perform the following operations:
 - To view subscription properties, click a link with subscription name.
 - To select a subscription that you want to manage through the Control Panel, click the corresponding link **Switch to Subscription**.
 - To order an SSL certificate for a site, click **Order a Certificate**. For more information about this operation, see the section **Ordering SSL Certificates**.
 - To view properties of already ordered SSL certificates, click **Show Certificate Info**.
 - To view or change domain information, contact information, and DNS settings specified at a registrar's site, click **Show Domain Info**. For more information about these operations, see the section **Registrar's DNS Settings in Panel** (on page 392).

➤ **To choose a payment method that you would like to use for paying for services:**

1. Go to the Account tab > Billing Accounts.

A record about the payment method that you used for purchasing the services for the first time is shown.

2. Do any of the following:

- To view or change settings for a billing account, click the corresponding link in the **Billing account name** column, specify the information about your bank card or account, and select the subscriptions that should be paid by it. Click **OK**.
- To add a new billing account, click **Add New Billing Account**, select the payment method, and click **Next**. Then choose the account owner (you or an auxiliary user that will be able to use this account), specify the required information about your bank card or account, and select the subscriptions for which you will pay with it. Click **OK**.
- To remove a billing account, click the corresponding **Remove** link.

Next in this section:

Calculating Usage Charges	364
Earning Money by Promoting a Provider's Plans	364

Calculating Usage Charges

If the pay-as-you-go web hosting is allowed for a plan, Business Manager calculates *usage charges* - total costs of hosting resources overage - for the plan's subscribers basing on resource usage statistics that Business Manager collects from the connected Panels on a daily basis. No matter what billing mode and billing cycles you use, this happen on the first day of each month: The system finds the average daily overage of each resource except traffic and multiplies it by the month length and the monthly usage price of this resource.

Traffic

The traffic usage charge is calculated in the following way: Business Manager counts the total traffic overage for a month and multiplies it by the monthly traffic usage price. For example, if subscribers download 10 GB of files during a month while the plan limit is 5 GB, then the traffic overage is 5 GB. Assuming that the traffic usage price is \$1 for a 1 GB, such subscribers will pay $(10 \text{ GB} - 5 \text{ GB}) * \$1 = \$5$ traffic usage fee.

Other Resources

For calculation usage charges for other resources, Business Manager uses the average daily usage values. For example, if a customer uses 500 MB of disk space over the subscription quota for 15 days and then uses extra 700 MB for other 15 days, the average overage will be $(500 * 15 + 700 * 15) / 30 = 600$ MB. If the disk space usage price is \$1 for 1 GB, then the customer will pay \$0.6 for disk space overage this month.

Calculating Usage with Add-ons

If a customer purchases additional resources in the middle of a month, then the system subtracts the resource amount provided by the add-on from the daily resource usage of each day starting from the add-on purchasing day.

For example, if a customer uses 500 MB of disk space over the plan limit for a whole month and purchases the add-on that provides an additional 1 GB of disk space on the 7th day of the month, then the usage charge will include the payment for only 7 days of 500 MB of disk space overage.

Earning Money by Promoting a Provider's Plans

Panel lets you earn money for promoting your provider's service plans. Particularly, you can get a certain commission for each subscription ordered in the provider's online stores by people who signed up using your referral link.

Participants of affiliate programs (*affiliates*) distribute links to their provider's online stores. Each link is unique, so the system defines who brought a new customer and adds the commission to the link owner's *affiliate balance*. This commission is defined by the terms of the affiliate program and may vary depending on an online store. The commission consists of two different elements:

- *Initial rate* - a percentage that the affiliate earns from the price of each order placed using the affiliate's link.
- *Recurrent rate* - a percentage that the affiliate earns from each invoice issued for subscriptions that were ordered using the affiliate's link.

Affiliates can use money they earn only after the provider pays out the money to them. Depending on the affiliate program conditions, the provider can pay out the commission either to the affiliate's account credit balance or transfer the money outside the system, for example, by check or cash. Normally, the provider pays out affiliates' commissions when they exceed the affiliate program's *payment threshold*. When the threshold is exceeded, affiliates can request the provider to pay out the commission by using the button in the Control Panel. Alternatively, affiliates can delay payments in order to earn a larger amount.

Becoming an Affiliate

To start earning money, click the link **Become an Affiliate** on the **Account** tab. Once became an affiliate, you will get the access to the list of the provider's affiliate programs and your affiliate links. To see the programs list and your links, click the **Affiliate Programs** list on the **Account** tab.

Tracking Your Earnings

To see your current affiliate balance, go to the **Account** tab and find the balance in the **Affiliate Programs** group. If you want to see detailed information about your earnings, click the link **Revenue from Referrals**.

To request a payout after exceeding a payment threshold, go to the **Affiliate Programs** page, select the programs and click **Request Payout**.

Note: If none of your affiliate balances exceed the corresponding thresholds, you will not see the **Request Payout** button.

Example

For example, your provider offers you an affiliate program with 10% commission rate and \$20 payment threshold. You share your affiliate link with your friends, and three of them subscribe to a web hosting plan which costs \$50. The total commission that you get to your affiliate balance is $\$50 * 3 * 10\% = \15 . This amount is less than the program's payment threshold, so to receive credits, you should bring more customers to the online store with your link. When you do this and your balance exceeds the payment threshold which is \$20, the provider will add this balance to your credits. When you receive them, you can use them to pay for your subscriptions or subscribe to new services in the provider's online stores.

Participating in Multiple Programs

Your hosting provider may have multiple online stores with different currencies. If the provider offers affiliate programs for stores with different currencies, you will receive separate commissions in the corresponding currencies. For example, if you distribute links to stores with *USD* and *EUR* currencies, your affiliate balance contains two separate affiliate balances, one for each currency. Your provider pays out the commissions separately as well. For example, your affiliate balance is USD 50 and EUR 40 and the payment thresholds of the corresponding programs are USD 40 and EUR 45, your provider will pay out USD 50 to your credits and your affiliate balances will be USD 0 and EUR 40.

Ordering More Resources

The operations described below are available if your Control Panel is integrated with a billing system.

➤ *To add more resources to your subscription or upgrade to another service plan:*

1. Click the **Account** tab.
2. In the list of subscriptions, locate the subscription that you want to upgrade to another service plan, and click a link with the currently used plan's name.
3. Click **Upgrade**.

If there is no **Upgrade** link, then it means that you cannot upgrade to another hosting plan from your Control Panel, and you need to contact your provider.

4. Do any of the following:
 - To add resources to your subscription without upgrading to another plan, select the options you would like to add and click **Adjust Add-ons**.
 - To upgrade to another service plan, click **Order Upgrade**.

➤ *To reduce the amounts of resources or downgrade to another service plan:*

1. Click the **Account** tab.
2. In the list of subscriptions, locate the subscription that you want to downgrade to another service plan, and click a link with the currently used plan's name.

3. Click Downgrade.

If there is no **Downgrade** link, then it means that you cannot downgrade to another hosting plan from your Control Panel, and you need to contact your provider.

4. Do any of the following:

- To reduce the amounts of allocated resources without downgrading to another plan, select the options you would like to reduce and click **Adjust Add-ons**.
- To downgrade to another service plan, click **Order Downgrade**.

➤ To subscribe to a hosting plan in addition to your main plan:

1. Go to the **Account** tab and click the **Add Subscription** link.
2. Select the hosting plan to which you want to subscribe, and click **Buy Now**. Follow the instructions on the screen to complete the order.

Viewing Statistics

➤ *To view the reports on disk space and traffic usage by your account:*

1. If you have several subscriptions associated with your account, in the **Subscription** menu at the top of the screen, select the required subscription.
2. Click the **Statistics** tab.

The following information is presented in charts:

- Disk space used by the following files and directories in the subscription:
 - Websites
 - Mail accounts
 - Databases
 - Logs
 - Backups
 - Chroot directories
 - Configuration files
 - Anonymous FTP directory
- Traffic used by FTP, web, and mail services during the current month.

FTP field shows the information about the total size of files transferred to and from the webspace over the file transfer protocol.

HTTP field shows the information about the total amount of data transferred from all of your websites over HTTP protocol, that is, retrieved by web browsers.

POP3/IMAP field shows the total amount of data received by all mail accounts under your domains.

SMTP field shows the total amount of data sent by all mail accounts under your domains.

3. Do any of the following:

- To view a report on the amount of data transferred to and from your sites over FTP, click **FTP Statistics**.
- To view a report on the amount of data transferred to and from your FTP directory, which is accessed without authorization, click **Anonymous FTP statistics**.
- To view a report on the amount of traffic used by services during a certain month, click **Data Transfer Statistics**, and select the required month from the menu.

Next in this section:

Log Files 369


Log Files

All connections to the web server and requests for files that were not found on the server are registered in log files. These log files are analyzed by the statistics programs running on the server, which then present graphical reports on demand. You may want to download these log files to your computer for processing by third-party statistics programs, or view their contents for web server debugging purposes.

➤ ***To prevent these log files from growing too large, you should enable automatic cleanup and recycling of log files:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Logs** > **Log Rotation**.
3. Click **Switch On**. If you see only the **Switch Off** button there, this means that log recycling is already switched on.
4. Specify when to recycle log files and how many copies of each log file to store on the server. Also specify whether they should be compressed and sent to an e-mail address after processing.
5. Click **OK**.

➤ ***To view the contents of a log file or download it to your computer:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Logs**. A list of log files opens.
3. Do any of the following:
 - To view all entries in a log file, click the log file name. If you want to view only a few last lines from the log file, type the number of lines into the input box under the **Settings** group, and then click the log file name.
 - To download a file to your computer, click the corresponding icon .
 - To remove a processed log file from the server, select the corresponding checkbox and click **Remove**. Confirm removal and click **OK**.

➤ ***To download log files to your computer via FTP:***

1. Connect to the Panel server via FTP.
2. Go to the `/var/www/vhosts/<domain_name>/logs` directory and copy the log files to you computer.

(Advanced) Managing Auxiliary User Accounts

If you want to allow other users to access the Panel for managing websites and installed applications, or to use e-mail services under your domains, then you need to create user accounts for them.

Auxiliary Users and User Roles

Auxiliary user accounts are created based on user roles. The roles include privileges to access certain areas of the Panel and perform operations in the Panel. There are several predefined user roles, namely: Accountant, Application User, Owner, and Webmaster. You can review and modify the Accountant, Application User, and Webmaster roles to suit your needs, or you can create your own custom roles. For more information on user roles and user account creation, refer to the sections **User Roles** (on page 371) and **Auxiliary User Accounts** (on page 373) correspondingly.

After auxiliary user accounts are created, the users will be able to log in to their accounts in Panel and use shortcuts in their Panels to access their mailboxes and work with applications. In addition, you can extend the list of links available to your auxiliary users with your custom links. These can be links to corporate resources, sites on the web, and so on. Learn more in **Custom Links** (on page 375).

Auxiliary Users and Multiple Subscriptions

Since Panel 10.4, if your customer account includes more than one subscription, you can allow auxiliary users to access only a specified subscription. If the **Access to subscriptions** property of a user account is set to a certain subscription, the user will always log in to this subscription and will not be able to switch to other subscriptions.

Next in this section:

User Roles	371
Auxiliary User Accounts.....	373
Custom Links	375

User Roles

➤ *To create a user role:*

1. Go to the **Users** tab > **User Roles** tab > **Create User Role**.
2. Specify the following:
 - **User role name.**
 - **Access to Panel services.** Grant the required permissions for operations to the user:
 - **Manage users and roles.** Add, modify, and remove user accounts and roles. Note that even if this permission is not granted to a user, the user will be able to browse contact information of other users after logging in to the Panel.
 - **Create and manage sites.** Set up, modify, remove domain names and subdomains, host websites and change web hosting settings.
 - **Configure log rotation.** Manage settings for recycling of web server access and error log files. View, download, and remove log files.
 - **Configure anonymous FTP service.** Set up a directory accessible to all Internet users over FTP without authorization.
 - **Create and manage scheduled tasks.** Schedule execution of scripts or programs on your customer account.
 - **Configure spam filter.** Set up spam protection for mailboxes.
 - **Configure antivirus.** Set up virus protection for mailboxes.
 - **Create and manage databases.** Add, modify, and remove databases stored on your customer account.
 - **Configure and perform data backup and restoration.** Back up and restore data related to your customer account, websites, and mailboxes under your domains.
 - **View statistics.** View reports on disk space and traffic usage by your websites, and website visits.
 - **Install and manage applications.** Install applications on websites and manage them.
 - **Design sites in Presence Builder.** Create websites using Presence Builder.
 - **Upload and manage files.** Manage files and directories located in the web space by using the Panel's file manager.
 - **Create and manage additional FTP accounts.** Set up additional FTP accounts for other users.
 - **Manage DNS settings.** Manage DNS settings for domains.
 - **Install and manage Java applications.** Install on websites third-party Java applications.
 - **Create and manage mail accounts.** Create, modify, and remove e-mail accounts.
 - **Create and manage mailing lists.** Create, modify, and remove mailing lists.

- **Access to apps.** Select the applications that the user should be able to access and use. All web applications installed on the server are listed in this area.

For more information about installing applications and providing access to users, refer to the section **Granting Auxiliary Users Access to Apps** (on page 423).

- **Access to the billing operations.** Grant these permissions if you want users of this role to view and pay invoices for your subscriptions.

3. Click **OK**.

➤ ***To modify user role properties:***

1. Go to the **Users** tab > **User Roles** tab.
2. Click a link with the role name that you want to change.
3. Change the role properties as required and click **OK**.

➤ ***To remove a user role:***

1. Go to the **Users** tab > **User Roles** tab.
2. Select a checkbox corresponding to the role you want to remove and click **Remove**. Note that it is impossible to remove the **Owner** role and other roles that are assigned to one or more users.
3. Click **Yes** to confirm the removal.

Auxiliary User Accounts

➤ *To create a user account:*

1. Go to the **Users** tab > **Create User Account**.
2. Specify the following:
 - **Contact name.**
 - **E-mail address.** The e-mail address will be used as a user name for logging in to Panel, unless you specify another name in the **Username** box.
 - To create a new e-mail address for the user, select the option **Create an e-mail address under your account**, type the desired left part of the address which goes before the @ sign, and, if you have a number of domains on your account, select the domain name under which the e-mail address should be created.
 - To associate with this user account an external e-mail address, select the option **Use an external e-mail address**, and specify an existing external e-mail address.
 - **User role.** Select the required user role from the menu.
 - **Access to subscriptions.** Allow a user to access only a specified subscription. The **All** value grants them access to all subscriptions within your customer account.
 - **Username.** The user name for access to Panel.
 - **Password.** The password for access to Panel.
3. Leave the **User is active** checkbox selected. Otherwise, the user will not be able to access the Panel and use applications on your customer account.
4. Click **OK**.
5. Now, if you want to add contact information for the user, click a link with the user's name, and then click the **Contact Details** tab, and specify the user's contact information.
6. Click **OK**.

Now you can notify the user about creation of his or her account and ability to access Panel. Provide the user with the address to open in his or her browser, the username (which is the user's e-mail address), and the password that you specified in the account settings.

➤ *To change user account properties:*

1. Click the **Users** tab.
2. Click a link with the user's name.
3. Make the required changes and click **OK**.

➤ ***To suspend or activate a user account:***

1. Click the **Users** tab.
2. Click a link with the user's name.
3. Do any of the following:
 - To suspend a user account, clear the **User is active** checkbox. The user will no longer be able to log in to the Panel and access applications.
 - To activate a user account, select the **User is active** checkbox.
4. Click **OK**.

➤ ***To remove a user account:***

1. Click the **Users** tab.
2. Select a checkbox corresponding to the user account you want to remove, and click **Remove**. Note that you cannot remove your own account.
3. Click **Yes** to confirm the removal.

Custom Links

You can add custom hyperlinks to the Panel and make them visible for your users. The links may lead to web resources, such as your corporate site, or to a web application that can process online requests and accept additional information about the users who click these links.

You can specify what information about users should be passed:

- Subscription ID.
- Primary domain name associated with a subscription.
- FTP account username and password.
- Customer's account ID, name, e-mail, and company name.

You can place the links in the following locations of the Control Panel, and decide who should be able to see them:

- On the **Websites & Domains** page in the Control Panel, visible only to you. This is achieved by selecting the **Customer's Home page** option in the link properties.
- On the **Websites & Domains** page in the Control Panel, visible to you and your users who are allowed to log in to the Control Panel. This is achieved by selecting the **Common access** option in the link properties.
- On the **Websites & Domains** tab in the Control Panel, visible to you and your users who are allowed to log in to the Control Panel. This is achieved by selecting the **Websites & Domains page of Subscription** option in the link properties.

➤ *To add a custom hyperlink to the Control Panel:*

1. Go to the **Account** tab > **Additional Services**, and click **Add Link to Service**.
2. Specify the following settings:
 - Type the text that will show on your button in the **Button label** box.
 - Choose the location for your button.
 - Specify the priority of the button. Your custom buttons will be arranged in the Panel in accordance with the priority you define: the lower the number, the higher the priority. Buttons are placed in the left-to-right order.
 - To use an image for a button background, type the path to its location or click **Browse** to browse for the desired file. It is recommended that you use a 16x16 pixels GIF or JPEG image for a button to be placed in the navigation pane, and 32x32 pixels GIF or JPEG image for buttons placed in the main frame or desktop.
 - Type the hyperlink of your choice to be attached to the button into the **URL** box.
 - Using the checkboxes, specify whether you want the customer information and other data to be transferred within the URL. These data can be used for processing by external web applications.
 - In the **Tooltip text** input field, type in the help tip that will be displayed when the users place the mouse pointer over the button.

- Select the **Open URL in Parallels Panel** checkbox if you want the destination URL to be opened in the main frame of the Panel, otherwise, leave this checkbox cleared to open the URL in a separate browser window or tab.
- If you want to make this button visible only to you, select the **Show to me only** checkbox.

3. Click **Finish** to complete creation.

➤ ***To remove a hyperlink button from the Panel:***

1. Go to the **Account** tab > **Additional Services**.
2. Select a checkbox corresponding to the link that you want to remove and click **Remove**.

Websites and Domains

As described in the chapter **Quick Start with Parallels Panel**, creating your web presence always starts with purchasing a domain name. The *domain name* (or simply, *domain*) is the name people use to access your site from their browsers, for example, `www.example.com`. The domain registration is carried out by authorized companies - domain name registrars. Hosting providers often carry out this function. For detailed information about how to manage domains in Panel, refer to the section **Domains and DNS** (on page 378).

However, a domain is not a website. To make it accessible from the web and fill it with content, you should subscribe to hosting services (obtain a customer account). That is to supplement your domain with Internet connectivity, some disk space to store your content, mail services, and so on. Thus, *a website is a domain with provided hosting services*.

Panel provides a full range of operations in regard to domains and websites:

- Adding and removing domains, subdomains, and aliases.
- Managing the content of your websites.
- Installing various web apps.
- Securing connections to your websites and much more.

This chapter provides detailed information on all the possible operations on websites and domains in Panel. Note that some of these operations may be unavailable according to your hosting plan.

Next in this section:

Domains and DNS.....	378
Hosting Settings.....	395
Website Content.....	413
(Advanced) Restricting Access to Content.....	418
Previewing Websites.....	420
Web Applications.....	421
(Advanced) Website Security.....	429
(Advanced) Extended Website Management.....	435

Domains and DNS

As described above, a domain name is the name that people type in their browsers to access your website.

A domain name is hierarchical and can consist of a number of parts called labels:

- The label furthest to the right is called the *top-level domain*. For example, `com` is the top-level domain of `www.example.com`. The number of top-level domains is limited and all of them are managed by separate international authorities.
- *The second-level domain* is the label that we mainly use to imply the purpose of our website. In `www.example.com` it is the `example` part. The combination of the second-level and top-level domain names specifies the exact location of your website.
- Each label to the left is a subdomain of the domain to the right. For example, `www` is the subdomain of `example.com`. Subdomains can be convenient when you want to isolate some content from the main site, e.g. you can organize your personal blog on `myblog.example.com`. For information on how to add subdomains in Panel, refer to the section **Adding Subdomains** (on page 381).

If you want to host more than one website under your subscription, you can register more domains and add them to your subscription. Registering new domains may be available to you in the Control Panel if your hosting provider allows this. For information on how to purchase and add domains in Panel, refer to the section **Adding Domains** (on page 379).

In fact, domain names exist only for convenience; the real communication between browser and web servers uses IP addresses - the numerical host identifiers. For example, the real address of `www.example.com` may be `192.0.2.12` (IPv4). To resolve domain names into IP addresses, web hosts use DNS technology. For more details about how DNS is implemented in Panel, refer to the section **(Advanced) Configuring DNS for a Domain** (on page 386).

DNS allows several domains to be resolved into one IP address. Such additional names are called domain aliases. This is convenient when you have purchased several domains that you want to point to the same website. For information on how to add aliases to existing domains, refer to the section **Adding Domain Aliases** (on page 383).

Next in this section:

Adding Domains	379
Adding Subdomains	381
Adding Domain Aliases	383
Adding Wildcard Subdomains (Linux)	384
Adding a Domain Forwarder	385
(Advanced) Configuring DNS for a Domain	386

Adding Domains

If your hosting package includes more than one domain name (website), then you can easily add new domains to the server. Before you start adding a new domain that will use a second-level domain name, like *example.com*, be sure to register this domain name. If your hosting provider provides the domain name registration service, you can do this from the Control Panel as described below. Otherwise, you should register your domain name with another domain name registration authority.

You can set up the following types of site configurations through Panel:

- **Website addressed by a second-level domain name.** The following services are available for websites:
 - A unique Internet address (domain name), like *example.com*.
 - Additional domain names (domain aliases).
 - Subdomains - divisions of a site accessible by easy-to-remember addresses that are added to the main site, like *mail.example.com*.
 - Separate FTP accounts for collaboration on the site content. For every FTP account, you can specify which directories can be accessed.
 - Creating content using Presence Builder.
 - Simplified deployment of applications, such as content management systems, photo galleries, shopping carts, blogging platforms, and many more.
 - Secure data exchange implemented by SSL protocol. This requires that a site be hosted on a dedicated IP address, which is not shared among other users and sites.
 - Mailboxes and mailing lists.
 - Viewing statistics on site visits.
- **Website or a division of a website addressed by a third-level domain name (subdomain).** This is usually a division of an existing site. It has an Internet address comprising of three parts separated by dots. The following services are available for subdomains:
 - Separate document root from the main site. Document root is a directory on the server where web pages of a site are stored.
 - Access over FTP for content management.
 - Creating content using Presence Builder.
 - Simplified deployment of applications.
 - Secure data exchange implemented by SSL protocol.
 - Viewing statistics on site visits.

Adding More Domains

➤ **To host a new website with a second-level domain name:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, select the required workspace in the **Subscription** menu at the top of the screen.
2. Click the **Websites & Domains** tab, click **Add New Domain** and follow on-screen instructions.

Note: If you select the recommended option, you should connect the DNS settings related and your domain name with the domain name at the registrar's side. To achieve this, enter the Panel name server IP address into the respective NS record of the registrar. The instruction on how to obtain the IP is as follows: go to **Websites & Domains > <domain name> > DNS Settings**, find the NS record, and then find the A record corresponding to the NS record value.

For example, if your NS record is
`example.com. NS ns.example.com,`
find the A record with `ns.example.com`, for example,
`ns.example.com. A 192.0.2.12`

The resulting value, `192.0.2.12`, is the Panel name server IP you need.

3. Click **OK**.
The new domain name is now shown in the list at the bottom of the screen.
4. If the operation of changing hosting settings is available for your account, then you can click the domain name of the new website to view or change the hosting settings, as described in the section **Changing Hosting Settings** (on page **395**).

You can now start creating your website with Presence Builder or upload your web content to the workspace of the new website, as described in the section **Managing Website Content** (on page 413).

Registering Domains

If your service provider offers the domain name registration service as well as web hosting, you can initiate a domain registration directly from Panel. To register a domain name, add it as described above and then click the link **register it now** beside the new domain name on the **Websites & Domains** tab. This will redirect you to the provider's online store where you can complete the registration.

After you register a domain name, it appears in the **Registered domain names** list on the **Websites & Domains** tab. To get information about a domain name registration, for example, the registration price and next renewal date, click the domain name in this list.

Removing Domains

When you delete a domain from Panel, all data related to the corresponding site are deleted from the server. The first domain name (default domain) that was created for your account cannot be deleted; however, it can be renamed.

➤ **To remove a domain:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, select the required workspace in the **Subscription** menu at the top of the screen.
2. Go to the **Websites & Domains** tab and click the name of the domain or subdomain you want to remove.
3. Click **Remove Website** or **Remove Subdomain**.
4. Confirm removal and click **OK**.

Note: Removing domain names from the Control Panel does not cancel the registration of these names. If you registered these domains name, you still can use them for your websites.

Adding Subdomains

If your hosting package includes subdomains, which are additional third-level domain names, then you can use them to:

- Organize logically the structure of your site.
- Host additional websites or parts of a website on the same server without the need to pay for registration of additional domain names.

An example of using subdomains:

You have a website `your-product.com` dedicated to promoting and selling your product. For publishing information related to customer service and online order tracking, you can organize the subdomain "orders" so that your users will be able to access this information directly by visiting the Internet address "orders.your-product.com".

As subdomains have the same status with the additional domains, you can use the same set of tools and services for working with subdomains. For example, SSL protection, Presence Builder, web statistics, and so on.

➤ **To set up a subdomain for a site division or a separate site:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, select the required workspace in the **Subscription** menu at the top of the screen.
2. Click the **Websites & Domains** tab.
3. Click **Add New Subdomain**.

4. Specify the following:
 - a. In the **Subdomain name** box, type the portion of address that will be added to the domain name of your main site.
 - b. In the **Document root** box, type the desired location of the directory where all files and subdirectories of this site will be kept. You can use the default directory of the main site, called `httpdocs`, or specify another directory.
5. Click **OK**.

The new subdomain name is now shown in the list at the bottom of the screen.

You can now upload your web content to the subdomains web space (directory on the server), as described in the section **Uploading Content over FTP**.

Wildcard Subdomains

If you enter the asterisk (*) symbol as a subdomain name, Panel will create a so-called *wildcard subdomain*. When site visitors enter *any* subdomain name that is not registered in Panel, they will be redirected to this wildcard subdomain. You can create wildcard subdomains on any domain name level. For example, you can create the **.mystore.example.com* subdomain. Learn more about wildcard subdomains in the section **Adding Wildcard Subdomains (Linux)** (on page 384).

Adding Domain Aliases

Domain aliases allow you to point several domain names to the same website. This can be useful, for example, for branding purposes.

➤ *To set up a domain alias in Panel:*

1. Run the **Add New Domain Alias** wizard in the **Websites & Domains** tab.
2. Specify the domain for which you are creating an alias (the *primary domain*) and the alias's domain name, for example `alias.tld`, and set up the following:

- **Synchronization of DNS zone with the primary domain**

If this option is enabled, the DNS zone of the domain alias will be in sync with the zone of the primary domain. Any changes made in the DNS zone of the primary domain will be automatically applied to the DNS zone of the alias. For example, if you create the CNAME record like `blog.primary_domain.tld`, the corresponding `blog.alias.tld` record will be added to the zone of the alias.

Note: If a domain alias's DNS zone is synced with the primary domain, you cannot modify resource records in the alias's DNS zone.

- **Mail service**

Panel does not allow creating mailboxes under domain aliases. Instead, the mailboxes of the primary domain are used. If you select the **Mail service** option, the mailboxes created under the primary domain will also be available under the alias. To enable users to read mail sent to mailboxes under the alias, Panel redirects it to the corresponding mailboxes under the primary domain.

For example:

You have an email address `mail@domain.tld`. Then you set up an alias for `domain.tld`, for example, `alias.tld`. If you select the **Mail service** option, all mail sent to `mail@alias.tld` will be available at `mail@domain.tld`. Otherwise, the mailbox `mail@domain.tld` will not receive mail sent to `mail@alias.tld`.

- **Web service**

If this option is turned on, the website will open in the browser at the alias's URL. If you clear the **Web service** check box, the alias will be used for mail only provided that **Mail service** is selected.

- **Redirect with the HTTP 301 code**

By default, Panel uses web server internal redirection for aliases. In this case, the alias appears to be a separate website for visitors and for web search engines. This causes the problem because search engines index the content of the alias separately, so your primary domain loses search engine rankings.

To avoid this, you can use redirection with the HTTP 301 code (Moved permanently) by selecting **Redirect with the HTTP 301 code**. In this case, only the primary domain will rank in search engines. Learn more at

<http://support.google.com/webmasters/bin/answer.py?hl=en&answer=93633>

- **Java web applications**

If you use hosting services based on a Linux platform, and you have Java applications installed on your site that you want to make accessible through the domain alias, select the **Java web applications** option.

Adding Wildcard Subdomains (Linux)

Use wildcard subdomains to redirect visitors from *non-existent subdomains* to one of your websites, commonly, to your main website. The typical use cases of this feature are:

- Improve website organization and run marketing campaigns.
For example, you do not have the *vps-limited-offer* subdomain but wish to forward users from *limited-vps-offer.example.com* to *example.com*.
- Help users reach your website even if they mistyped a subdomain name.
It is a widespread mistake to mistype a website name if it has the leading *www* prefix (for example, typing *ww.example.com*).
- Finally, some website applications (WordPress) use wildcard subdomains to create dynamic subdomains for convenience and better user experience.

Note: Traffic to existent subdomains will not be affected in any way if you add a wildcard subdomain.

How to Add Wildcard Subdomains

You can add one wildcard subdomain per each of domain names under a subscription. For this, go to the **Websites & Domains** tab and add a new subdomain which name is "*" to one of your domain names. Example: **.example.com*. If you wish this subdomain to have a custom set of scripts or website content, specify a custom document root for this subdomain.

Limitations of Wildcard Subdomains

Wildcard subdomains act like typical subdomains with the following exceptions:

- *Linux-only feature*. Currently, wildcard subdomains are supported only on Panel for Linux.
- *Renaming is not available*. It is not possible to rename such subdomains.
- *No DNS zone*. This type of subdomains does not have own zone record in the Panel's DNS server. Instead, they have the A record that points to the IP address associated with a corresponding domain name.
- *Installation of APS apps is not allowed*. Panel users are unable to install APS apps to wildcard subdomains.
- *No Presence Builder sites*. Panel users are unable to edit and publish sites to these subdomains.

Adding a Domain Forwarder

➤ *To create a domain forwarder in Panel:*

Start creating a new domain in **Websites & Domains > Add New Domain** and specify the following:

- In the **Domain name** box, type the domain name that you have registered with your service provider or a domain name registration company and from which you want to redirect visitors.
- Under **DNS server configuration**, select the option **Use our DNS settings**.
- Under **Hosting type**, select the **Forwarding** option.
- In the **Destination address** box, type the URL address to which you want to redirect visitors.
- Under **Forwarding type**, select standard or frame forwarding. To learn more about forwarding types, see **Forwarding**. (on page 399)

➤ *To make an existing domain a domain forwarder:*

On the **Websites & Domains** tab, click **Hosting Settings** beside the name of the domain you want to make a forwarder, and click the **Change** link next to the **Hosting type** field and specify the following:

- Under **Hosting type**, select the **Forwarding** option.
- In the **Destination address** box, type the URL address to which you want to redirect visitors.
- Under **Forwarding type**, select standard or frame forwarding. To learn more about forwarding types, see **Forwarding**. (on page 399)

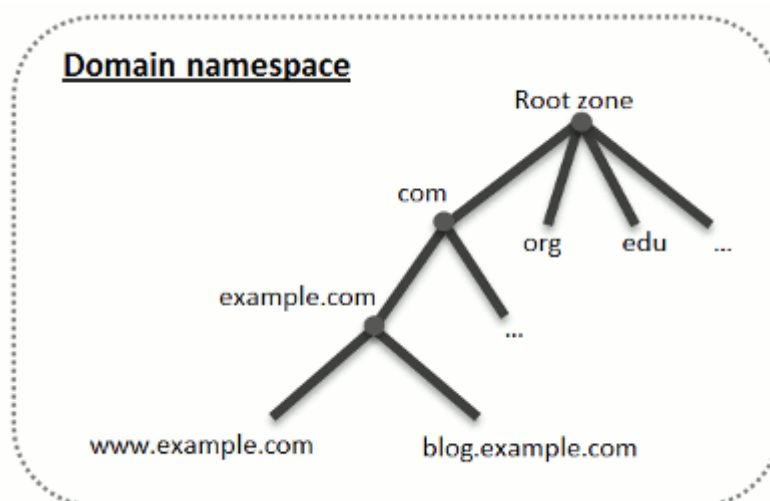
(Advanced) Configuring DNS for a Domain

The Domain Name System (DNS) is a hierarchical naming system that translates understandable domain names into the numerical identifiers (IP addresses) associated with web hosts. Such translation is called *resolving*. When you add a domain name (using **Websites & Domains > Add New Domain**), you should choose the role of Panel in resolving your resources: It can directly process all translation requests, be a backup server, or pass the translation requests to a remote server. This role can be changed for existing domain names (**Websites & Domains > domain name > DNS Settings**). We discuss details about each of the roles and provide instructions how to assign them next in this section.

Note: If your Panel does not use its own DNS service and does not allow configuring DNS settings on a remote DNS server, you can only view the information about your registered domain name. The link **DNS Settings** in **Websites & Domains** will be replaced with **Whois Information**.

DNS Name Resolving

DNS is based on a hierarchical tree structure called the domain namespace. This global namespace contains all possible domain names and is divided into logical parts - domain zones (see the picture below). A domain zone is a part of the namespace that contains the addresses of particular domains. Addresses are stored in a file on a separate name server with authority for that zone. For example, when a browser tries to access `www.example.com`, it gets the site's IP address from a server with authority for the `example.com` zone. For more information about how DNS works, refer to the respective documentation. You can find it in numerous sources on the Internet, for example, Microsoft TechNet.



When you purchase a domain, a registrar gives you access to the settings for the DNS zone responsible for your domain and its subdomains. You can either allow the registrar to manage the zone, or delegate the zone to Panel. The latter option gives you the ability to manage a zone directly from your customer account. For information about how to delegate your zone to the Panel, refer to the section **Panel as a Master DNS Server** (on page 388).

If you are an advanced user and already have a DNS server that you want to give authority for your zone, you can set up Panel to be a slave (also called secondary) DNS server. In this case, Panel just stores a copy of your zone and you do not have the option to manage it from the Control Panel. The Panel DNS server will be used only if your primary name server becomes inaccessible or inoperable. For information about how to make Panel act as a secondary DNS server, refer to the section **Panel as a Slave DNS Server** (on page 392).

If you decide *not* to use Panel as a DNS server, all zone management should be performed on a domain registrar's site. Some registrars provide support for remote DNS zone management. If your hosting provider uses this feature, you will still be able to modify the DNS zone from the Control Panel regardless of where your authoritative name server is located. For information about how to switch off the Panel's DNS server and manage your zone remotely, refer to the section **Registrar's DNS Settings in Panel** (on page 392).

Next in this section:

Panel as a Master DNS Server.....	388
Panel as a Slave DNS Server.....	392
Registrar's DNS Settings in Panel	392

Panel as a Master DNS Server

For each new domain name, the Panel automatically creates a DNS zone in accordance with the settings configured by your service provider. The domain names should work fine with the automatic configuration, however, if you need to perform custom modifications in the domain name zone, you can do that through your Panel.

➤ *To view the resource records in a DNS zone of a domain:*

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to view.
2. Click **DNS Settings**.

➤ *To add a new resource record to the zone:*

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage..
2. Click **DNS Settings**.
3. Click **Add Record**.
4. Select a resource record type, and specify the appropriate data:
 - For an NS record, which specifies the domain name of a name server that is responsible for a DNS zone of a domain, you need to specify the domain name (or a subdomain), and then the corresponding name server's domain name. If you are defining an NS record for your main domain, then you should leave the domain name field empty. If you are defining a name server for a subdomain, then type the subdomain into the **domain name** field. After that, type the appropriate name server's domain name into the **name server** field. For example: ns1.mynameserver.com.
 - For A and AAAA records, which associate IP addresses with domain names, you need to specify the domain name and IP address. If you are simply defining a record for your main domain, then you should leave the **domain name** field empty. If you are defining a record for a name server, then type ns1 or ns2 into the **domain name** field. Then specify the appropriate IP address with which to associate the domain name.
 - For a CNAME record, which specifies which subdomains (or domain aliases that look like subdomains, for example, www) should be associated in the Domain Name System with the main domain address, you need to type the subdomain name or www alias, and then, the main domain name.
 - For an MX record, which specifies the host name of the preferred mail server for the given domain, you need to specify the mail domain (or subdomain), the domain name of the mail exchange server responsible for receiving e-mail, and the server's priority. For the main domain, you would simply leave the available field blank. Then type the domain name of your mail server. If you are running a remote mail server named 'mail.myhostname.com', then simply type 'mail.myhostname.com' into the **Mail exchange server** field. After that, specify its priority: 0 is the highest and 50 is the lowest.
 - For a PTR record, which is required for reverse DNS lookup (an IP address is translated to domain name), you need to enter the IP address/mask, and then type the appropriate domain name for this IP address to be translated to.

- For a TXT record, which is used for specifying arbitrary human-readable text, you can type an arbitrary text string, or an SPF record.
- For an SRV record, which is used for specifying location of services other than mail, you will need to enter the service name, protocol name, port number, and target host. You can also specify the priority of the target host, and relative weight (for records with the same priority) in the appropriate fields.

4. Click **OK**, and then click **Update**.

➤ ***To modify the properties of a resource record:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click the hyperlink in the **Host** column corresponding to the resource record you want to modify.
4. Modify the record as required, click **OK**, and then click **Update**.

In addition to the resource records described above, there is also a Start of Authority record. This record indicates that this DNS name server is responsible for the domain's DNS zone. It also contains settings that affect propagation of information about the DNS zone in the Domain Name System.

➤ ***To modify the entries in the Start of Authority (SOA) record for a domain:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **SOA Record**.
4. Specify the required values:
 - **Refresh interval.** This is how often the secondary name servers check with the master name server to see if any changes have been made to the domain's zone file. The Panel sets the default value of three hours.
 - **Retry interval.** This is the time a secondary server waits before retrying a failed zone transfer. This time is typically less than the refresh interval. The Panel sets the default value of one hour.
 - **Expire interval.** This is the time before a secondary server stops responding to queries, after a lapsed refresh interval where the zone was not refreshed or updated. The Panel sets the default value of one week.
 - **Minimum TTL.** This is the time a secondary server should cache a negative response. The Panel sets the default value of three hours.
 - **Default TTL.** This is the amount of time that other DNS servers should store the record in a cache. The Panel sets the default value of one day.
5. Click **OK**, and then click **Update**.

Usage of serial number format recommended by IETF and RIPE is mandatory for many domains registered in some high-level DNS zones, mostly European ones. If your domain is registered in one of these zones and your registrar refuses your SOA serial number, using serial number format recommended by IETF and RIPE should resolve this issue.

The Panel-managed servers use UNIX timestamp syntax for configuring DNS zones. UNIX timestamp is the number of seconds since January 1, 1970 (Unix Epoch). The 32-bit timestamp will overflow by July 8, 2038.

RIPE recommends using YYYYMMDDNN format, where YYYY is year (four digits), MM is month (two digits), DD is day of month (two digits) and NN is version per day (two digits). The YYYYMMDDNN format will not overflow until the year 4294.

➤ ***To change the Start of Authority (SOA) serial number format to YYYYMMDDNN for a domain:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **SOA Record**.
4. Select the **Use serial number format recommended by IETF and RIPE** checkbox.

Note: See the sample of SOA serial number generated with the selected format. If the resulting number is less than the current zone number, the modification may cause temporary malfunction of DNS for this domain. Zone updates may be invisible to the Internet users for some time.

5. Click **OK**, and then click **Update**.

➤ ***To remove a resource record from the zone:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Select a checkbox corresponding to the record you want to remove.
4. Click **Remove**.
5. Confirm removal, click **OK**, and then click **Update**.

➤ ***To restore the original zone configuration in accordance with the default DNS template settings used on the server:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **Restore Defaults**.

4. In the **IP address** menu, select the IP address to be used for restoring the zone.
5. Specify whether a **www** alias is required for the domain.
6. Select the **Confirm the restoration of the DNS zone** checkbox, and click **OK**.

➤ ***To restore the default Start of Authority (SOA) serial number format (UNIX timestamp) for a domain:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **SOA Record**.
4. Clear the **Use serial number format recommended by IETF and RIPE** checkbox.

Note: See the sample of SOA serial number generated with the selected format. If the resulting number is less than the current zone number, the modification may cause temporary malfunction of DNS for this domain. Zone updates may be invisible to the Internet users for some time.

5. Click **OK**, and then click **Update**.

By default, transfer of DNS zones is allowed only for the name servers designated by NS records contained within each zone. If you are using a Windows-based account, then you can change zone transfer settings.

➤ ***If your domain name registrar requires that you allow transfer for all zones you serve:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **Zone Transfers**. A screen will show all hosts to which DNS zone transfers for all zones are allowed.
4. Specify the registrar's IP or network address and click **Add Network**.

Panel as a Slave DNS Server

If you host websites on your account and have a standalone DNS server acting as a primary (master) name server for your sites, you may want to set up the Panel's DNS server to function as a secondary (slave) name server.

➤ ***To make the Panel's DNS server act as a secondary name server:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **Switch DNS Service Mode**.
4. Click **Add Record**.
5. Specify the IP address of the primary (master) DNS server.
6. Click **OK**, and then click **Update**.
7. Repeat steps from 2 to 6 for each website that needs to have a secondary name server on your server.

➤ ***To make the Panel's DNS server act as a primary back:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **Switch DNS Service Mode**.
The original resource records for the zone will be restored.

Registrar's DNS Settings in Panel

If you have external primary and secondary name servers that are authoritative for some of your websites, switch off the Panel's DNS service for each of these sites.

➤ ***To switch off the Panel's DNS service for a site served by external name servers:***

1. Go to the **Websites & Domains** tab and click the domain name whose DNS settings you want to manage.
2. Click **DNS Settings**.
3. Click **Switch Off the DNS Service**.

Turning the DNS service off for the zone will refresh the screen, so that only a list of name servers remains. Note that the listed name server records have no effect on the system. They are only presented on the screen as clickable links to give you a chance to validate the configuration of the zone maintained on the external authoritative name servers.

4. If you want to validate the configuration of a zone maintained on authoritative name servers, do the following:
 - a. Add to the list the entries pointing to the appropriate name servers that are authoritative for the zone: Click **Add Record**, specify a name server, click **OK**, and then click **Update**.
 - b. Repeat the step a for each name server you would like to test. The records will appear in the list.
 - c. Click the records that you have just created.

The Panel will retrieve the zone file from remote name servers and will check the resource records to make sure that domain's resources are properly resolved. The results will be interpreted and displayed on the screen.

If your Control Panel is integrated with a billing system, then the following operations on domains might be available from the Panel:

- Setting a password for access to domain management panel at a registrar's site.
- Locking and unlocking domain name for transferring to another provider.
- Changing domain registrant and other contact information.
- Changing DNS settings for domain zones served by a domain registrar.
- Configure automatic renewal of the domain account at the domain name registration company.

➤ ***To set a new password for access to your domain management control panel at a registrar's site:***

1. Go to the **Account** tab.
2. Locate the domain name for which you want to change settings, and click the link **Show Domain Info** next to it.
3. Click **Change Domain Password**.
4. Type a new password and click **OK**.

➤ ***To lock or unlock domain name for transferring to another provider:***

1. Go to the **Account** tab.
2. Locate the domain name for which you want to change settings, and click the link **Show Domain Info** next to it.
3. Click **Change Registrar Lock Setting**.
4. To allow domain name transfer, clear the **Lock** checkbox and click **OK**.

➤ ***To change domain owner's contact, technical, administrative, or billing information:***

1. Go to the **Account** tab.
2. Locate the domain name for which you want to change settings, and click the link **Show Domain Info** next to it.
3. Click **Edit Contact Info**.
4. Make the necessary changes and click **OK**.

➤ ***To change DNS settings for a domain:***

1. Go to the **Account** tab.
2. Locate the domain name for which you want to change settings, and click the link **Show Domain Info** next to it.
3. Click **Edit DNS Settings**.
4. Specify the domain name servers that serve the DNS zone for your website and IP address of the server where the website is hosted.
5. If the DNS zone of your website is served by your domain name registrar, then you can also specify other resource records that affect how your website's services are accessible over the Internet.
6. To save your changes, click **OK**.

➤ ***To configure automatic renewal of the domain name:***

1. Go to the **Account** tab.
2. Locate the domain name for which you want to change settings, and click the link **Show Domain Info** next to it.
3. Click **Automatic Domain Renewal**.
4. To allow auto renewal of the domain registration, select the **Turn on auto renewal** checkbox and click **OK**.

Hosting Settings

The website's hosting settings are available on the **Websites & Domains** tab of the Control Panel. All per-website hosting settings form the following groups:

- *General.*
Hosting type, security, scripting and statistics settings. See **General Settings** (on page 396).
- *PHP.*
PHP scripting language settings. See **PHP Settings** (on page 402).
- *Web Server.*
Web server settings (*Apache* (with *nginx*) or *IIS*). Web server type depends on Panel version: Apache with nginx is used on Panel for Linux, and IIS on Panel for Windows. See **Apache Web Server Settings** (on page 408) and **IIS Web Server Settings** (on page 410) correspondingly.
Note that in the IIS web server settings you can configure basic website security settings, such as anonymous access, ssl usage, and directory browsing.

On Windows, you can also set up custom ASP.NET settings in **Websites & Domains** > select a domain > **ASP.NET Settings**. For details, see **ASP.NET Settings (Windows)** (on page 406).

Next in this section:

General Settings.....	396
Web Scripting Settings	401
Web Server Settings	408

General Settings

To view a website's general hosting settings, click **Hosting Settings** beside its name on the **Websites & Domains** tab. The general website hosting settings are divided into groups:

Basic Settings

- **Domain name.** The domain name that you register with a domain registrar and will use for this website.
- **Hosting type.** The hosting type (**Website hosting**, **Forwarding**, and **No hosting**) defines the website behavior. By default, all websites belong to the **Website hosting** type as they are physically hosted on the server.

To change the hosting type, use the **Change** link. To learn more about hosting types, see **Hosting Types** (on page 397).

To suspend the website with all mailboxes and mailing lists hosted under the website's domain name use the **Suspend** option.

Note: Other basic settings depend on the selected hosting type. See **Hosting Types** (on page 397).

- **Website status.** The website status defines the site's accessibility in browsers and available hosting services. Apart from working as usual, the site can be suspended so it will not open in browsers, and even more, the hosting features of the site (such as the mail service and DNS service) can be disabled. You should change the status if you want the site to be temporarily unavailable, for example, for maintenance purposes. See **Website Status** (on page 400).
- **Document root.** Displayed for domains with the **Website** hosting type. See **Website Hosting** (on page 398).
- **Preferred domain.** Displayed for domains with the **Website** hosting type. See **Website Hosting** (on page 398).

Security Settings

- **Enable SSL support.** Secure Sockets Layer encryption is generally used for protecting transfer of sensitive data during online transactions on e-commerce websites that run on dedicated IP addresses. SSL certificates that participate in the encryption process are usually applied to a single domain name on a single IP address, therefore, each site that needs SSL protection must be hosted on a dedicated IP address. An exception to this is subdomains, which you can protect with a wildcard certificate. Installing an SSL certificate on a web server that hosts several websites with different domain names on a single IP address is technically possible, however, it is not recommended: the encryption will be provided, but users will get warning messages on attempt to connect to the secure site. To allow SSL encryption for the website, select the **Enable SSL support** checkbox.

Web Scripting and Statistics

- **Scripting languages.** Specify programming and scripting languages you want the website to support. For PHP, you can also select the custom PHP version and handler type. More PHP settings are available on the **PHP** tab. To learn more about PHP handlers and PHP configuration, see **PHP Settings** (on page 402).
- **Microsoft FrontPage settings.** Microsoft FrontPage is a popular website authoring tool. To enable content creation and publishing through Microsoft FrontPage, select the options **Microsoft FrontPage support**, **Microsoft FrontPage over SSL support**, and **Remote FrontPage authoring allowed**.
- **Web statistics.** Select the web statistics software that you want to use for viewing graphical reports and charts on website visitors. Also, select the corresponding checkbox if you want to be able to access the statistical reports by visiting the password-protected directory `http://your-website/plesk-stat/webstat`.
- **Custom error documents.** When visitors coming to a site request pages that the web server cannot find, the web server generates and displays a standard HTML page with an error message. If you want to create your own error pages and use them on the web server, select the **Custom error documents** checkbox.
- **Additional write and modify permissions** (available only for Windows hosting). This option is required if web applications on the site will be using a file-based database (like Jet) located in the root of the `httpdocs` directory. Note that selecting this option will seriously compromise the website security.

Next in this section:

Hosting Types	397
Website Status	400

Hosting Types

The hosting type defines the website's behavior. Panel supports three types of hosting: **Website hosting**, **Forwarding**, and **No hosting**.

Next in this section:

Website Hosting	398
Forwarding	399
Domains Without Web Hosting	399

Website Hosting

The **Website** hosting means that a website is physically located on the server.

For the website hosting type you can specify:

- **Document root.** The location of the directory where all files and subdirectories of the site will be kept. You can use the default directory `htdocs` or specify another directory.
- **Preferred domain.** Typically, any website is available on two URLs: with the `www` prefix (like in `www.example.com`) and without it (like in `example.com`). We recommend that you always redirect visitors to one of these URLs (typically to the non-`www` version). For example, after you set the Preferred domain to the non-`www` version (`example.com`), site visitors will be redirected to this URL even if they specify `www.example.com` in their browsers.

Panel uses the search engine friendly HTTP 301 code for such a redirection. This allows preserving search engine rankings of your site (preferred domain). If you turn off the redirection by choosing **None**, search engines will treat both URL versions (`www` and non-`www`) as URLs of different sites. As a result, rankings will be split between these URLs.

Forwarding

You can make one or more registered domain names to point to the same physical website, by using the domain name forwarding. This allows automatic redirection of visitors from the URL they specify in a browser to a site with a different URL. For example, visitors of the site `www.example.com` can be redirected to www.somedomain.tld. There are two types of forwarding in Panel: the standard and frame forwarding.

Standard Forwarding

With the **Standard forwarding**, users who have been redirected to another URL can see the destination URL in the browser address bar.

Depending on how long you intend to use the redirection, you can select the type of redirection – Moved permanently (code 301) or Moved temporarily (code 302). These are HTTP response codes which Panel sends to browsers to perform the redirection. From visitors' point of view, the response code does not matter: in both cases they will be simply redirected to the destination URL. For search engines, the code defines how they should treat the redirected site and affects search engine rankings.

- **Moved permanently (code 301).**

Use this redirection type if you want to keep search engine rankings of your site after moving it permanently to another address.

For example, if `example1.com` has been moved permanently to the domain `example2.com`, the rankings will not be split between `example1.com` and `example2.com` – search engine crawlers will treat them as a single website.

- **Moved temporarily (code 302).**

Use this redirection type when the destination domain is used temporarily, for example, when you are testing a new version of your site with real visitors while keeping the old version intact. If you set this redirection for a newly created destination domain, this domain will not be indexed by search engines.

Frame Forwarding

With the **Frame forwarding**, when visitors are redirected to another site, the address bar of their browsers continues to show the source URL. Thus, visitors remain unaware of the redirection. This is called frame forwarding as the index page of the source site contains a frame with the destination site.

Domains Without Web Hosting

You can switch off web service and use only email services under that domain (**Websites & Domains** tab > domain name > the **Change** link > the **No web hosting** option).

Website Status

The *website status* defines whether a website is available over the Internet and what hosting services are provided for it. The hosting provider may need to change the status of a site if the client does not pay for the services. Site owners can change the status of their sites if they want the sites to be temporarily unavailable.

Panel supports three website statuses: **Suspended**, **Disabled**, and **Active**.

Suspended Sites

If you want to shut down a site for maintenance and let your visitors know that it is temporarily unavailable, you can suspend the website so that it will not open in browsers (**Websites & Domains** > domain name > the **Suspend** link). Visitors will be redirected with the search engine friendly 503 HTTP code (Service Unavailable) to the "503 Service Unavailable" error page. The site's search engine rankings will not be affected, and the hosting services such as mail will still be available and manageable by means of Panel.

You can customize the error page using the link **Edit maintenance error page** in **Control Panel** > **Websites & Domains** > domain name.

Note: The link **Edit maintenance error page** is displayed only if your hosting plan provides the option to customize web server error documents (the **Custom error documents** is **On** in the domain settings in **Websites & Domains** > domain name > **Edit**).

Disabled Sites

If you stop supporting a website, you can disable it using **Websites & Domains** > domain name > the **Disable** link. Visitors will see the *web server's default page* set by the hosting provider, and the site's search engine rankings will drop.

Disabled websites stop being hosted on the server: They are excluded from the web server configuration. However, the physical directories and files of disabled sites can be accessed by FTP clients and File Manager. The hosting services such as mail will be unavailable.

Note: In Panel versions earlier than 11.5 this status was called **Suspended**.

Active sites

To bring the website back online, use **Websites & Domains** > domain name > the **Activate** link. The website will start working as usual.

Web Scripting Settings

For each website in your subscription you can specify which of the following programming and scripting languages should be supported by the web server: Active Server Pages (ASP), Microsoft ASP.NET, Server Side Includes (SSI), PHP hypertext preprocessor (PHP), Common Gateway Interface (CGI), Fast Common Gateway Interface (FastCGI), Perl and Python. Since Panel 10.4, you are able to configure PHP settings individually for each website (or subdomain) in your subscription. This is possible only if your subscription has the corresponding permissions. To get the details about custom PHP configuration, refer to the section **PHP Settings**.

Next in this section:

PHP Settings.....	402
ASP.NET Settings (Windows)	406

PHP Settings

PHP is one of the most popular scripting languages for creating dynamic web pages. The majority of today's websites and web applications are based on PHP scripts. This is why site administrators should clearly understand how they can control the execution of PHP scripts.

How PHP scripts are executed for a certain website is fully defined by two aspects: PHP handler and PHP settings for the site. You can set up these parameters for a certain website in the Control Panel as described below.

PHP Handler

When a visitor accesses a site based on PHP scripts, a web server interprets site scripts to generate a page that will be shown to the visitor. PHP handler calls PHP libraries needed for this interpretation. You can choose from a number of PHP handlers: ISAPI (Windows), Apache module (Linux), FastCGI, CGI, or PHP-FPM (Linux). The decision on what PHP handler to choose should depend on a number of factors like security considerations, script execution speed, and memory consumption.

➤ *To choose a PHP handler for your website:*

1. Go to **Websites & Domains**.
2. Click **Hosting Settings** near the domain name of a website for which you want to choose the PHP handler.
3. Choose one of the following PHP handlers as the value of the **Run PHP as** parameter (beside the **PHP support** option):

Run PHP as	Performance	Memory Usage	Security
------------	--------------------	---------------------	-----------------

<p>Apache module (Linux only)</p>	<p>High. Runs as a part of the Apache web server.</p>	<p>Low</p>	<p>This handler (also known as mod_php) is the <i>least secure option</i> as all PHP scripts are executed on behalf of the <code>apache</code> user. This means that all files created by PHP scripts of <i>any plan subscriber</i> have the same owner (<code>apache</code>) and the same permission set. Thus, a user has a theoretical possibility to affect files of another user or some important system files.</p> <hr/> <p>Note: You can evade some security issues by turning the PHP <code>safe_mode</code> option on. It disables a number of PHP functions that bring potential security risk. Note that this may lead to inoperability of some web apps. The <code>safe_mode</code> option is considered to be obsolete and is deprecated in PHP 5.3.</p>
<p>ISAPI extension (Windows only, <i>not supported since PHP 5.3</i>)</p>	<p>High. Runs as a part of the IIS web server.</p>	<p>Low</p>	<p>The ISAPI extension can provide site isolation in case a dedicated IIS application pool is switched on for subscriptions. Site isolation means that sites of different customers run their scripts independently. Thus, an error in one PHP script does not affect the work of other scripts. In addition, PHP scripts run on behalf of a system user associated with a hosting account.</p> <hr/> <p>Note: The ISAPI extension handler is not supported since PHP 5.3.</p>
<p>CGI application</p>	<p>Low. Creates a new process for each request and closes it once the request is processed.</p>	<p>Low</p>	<p>The CGI handler provides PHP script execution on behalf of a system user associated with a hosting account. On Linux, this behavior is possible only when the suEXEC module of the Apache web server is on (default option). Otherwise, all PHP scripts are executed on behalf of the <code>apache</code> user.</p> <p>We recommend that you use the CGI handler only as a fall-back.</p>
<p>FastCGI application</p>	<p>High (close to Apache module and ISAPI extension). Keeps the processes running to handle further incoming requests.</p>	<p>High</p>	<p>The FastCGI handler runs PHP scripts on behalf of a system user associated with a hosting account.</p>

PHP-FPM application (Linux only)	High	Low	<p>The PHP-FPM is an advanced version of FastCGI which offers significant benefits for highly loaded web applications.</p> <p>The PHP-FPM handler is available only if it was installed by hosting provider and if the option Process PHP by nginx in the website's settings is turned on (Websites & Domains > select a domain > Web Server tab).</p>
--	------	-----	---

Note: Switching PHP from **Apache module** to **FastCGI application** may break functionality of existing PHP scripts. Switching to **PHP-FPM** by selecting **Process PHP by nginx** in the website's web server settings may do the same.

PHP Version

Panel supports different versions of PHP. For each handler, one or more PHP versions can be available. The list of available versions is defined by your hosting provider and available to you in the same location where you select the PHP handler: **Websites & Domains** tab > **<domain_name>** > **Edit**.

Note: Always use PHP 5.x except the cases when you need PHP 4.x to host some old PHP apps.

PHP Settings

PHP behavior is defined by a number of configuration settings. These settings specify various script execution aspects, like performance (for example, the amount of memory a script can use), security (for example, access to file system and services), and so on. You may adjust these settings for a number of reasons:

- Preventing a memory leak or server hang-up by poorly written scripts.
- Protecting data from malicious scripts.
- Meeting the requirements of a certain web app.
- Testing own scripts and other.

PHP settings are located in the Control Panel, **Websites & Domains** > select a website > **PHP Settings**. For convenience, all PHP settings are divided into two groups:

- **Performance settings.**
These settings define how scripts work with system resources. For example: Use the `memory_limit` parameter to limit the amount of memory for a script to prevent a memory leak. In addition, you can prevent scripts from tying up the server by limiting the maximum time scripts are allowed to run using `max_execution_time`.
- **Common settings.**
This group contains other commonly used PHP settings. Generally, these are: Security settings (for example, the PHP safe mode toggle or the permission to register global variables), error reporting settings (for example, the directive to log errors), and others.

You can set the value of each parameter in **PHP Settings** either by selecting a value from a preset, typing a custom value, or leaving the **Default** value. In the latter case, *Panel* uses the values defined by the server-wide *php.ini* file. For information about certain PHP settings, refer to the respective documentation. For example, <http://php.net/manual/en/ini.list.php>.

It is possible to use three placeholders in parameter values:

- {DOCROOT} for the document root directory of a domain that gets custom PHP configuration.
- {WEBSACEROOT} for the root directory of a subscription (webpace).
- {TMP} for the directory which stores temporary files.

Note: Default values of PHP settings in Panel differ from the ones suggested by the official PHP documentation at <http://php.net/manual/en/ini.list.php>.




Note: Custom PHP configuration of a website acts as a preset for all subdomains of this site. You can perform further per-subdomain PHP configuration in the same way as for the websites.

ASP.NET Settings (Windows)


➤ *To configure ASP.NET Settings for a site:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Websites & Domains** tab and click your website's domain name.
3. Click **ASP.NET Settings**.
4. Set up the strings that determine database connection data for ASP.NET applications that use databases. This option is available only for ASP.NET 2.0.x.

When you open the ASP.NET configuration screen for the first time, sample connection parameters with common constructions are displayed. You can delete them and specify your own strings.

- To add a string, enter the required data into the **Name** and **Connection Parameters** input fields and click  next to them.
 - To remove a string, click  next to it.
5. Set up custom error messages that will be returned by ASP.NET applications in the **Custom Error Settings** field:
 - To set the custom error messages mode, select an appropriate option from the **Custom error mode** menu:
 - **On** - custom error messages are enabled.
 - **Off** - custom error messages are disabled and detailed errors are to be shown.
 - **RemoteOnly** - custom error messages are displayed only to remote clients, and ASP.NET errors are shown to the local host users.
 - To add a new custom error message (which will be applied unless the **Off** mode was selected), enter the values in the **Status Code** and **Redirect URL** fields, and click .
 - **Status Code** defines the HTTP status code resulting in redirection to the error page.
 - **Redirect URL** defines the web address of the error page presenting information about the error to the client.

Due to possible conflicts, you cannot add a new custom error message with an error code that already exists, but you can redefine the URL for the existing code.

 - To remove a custom error message from the list, click  next to it.
 6. Configure compilation settings in the **Compilation and Debugging** field:
 - To determine the programming language to be used as default in dynamic compilation files, choose an entry from **Default web page language** list.
 - To enable compiling retail binaries, leave the **Switch on debugging** checkbox empty.

- To enable compiling debug binaries, select the **Switch on debugging** checkbox. In this case, the source code fragments containing error will be shown in a diagnostic page message.

Note. When running applications in debug mode, a memory and/or performance overhead occurs. It is recommended to use debugging when testing an application and to disable it before deploying the application into production scenario.

7. Configure encoding settings for ASP.NET applications in the **Globalization Settings** section:

- To set an adopted encoding of all incoming requests, enter an encoding value into the **Request encoding** field (default is utf-8).
- To set an adopted encoding of all responses, enter an encoding value into the **Response encoding** field (default is utf-8).
- To set an encoding which must be used by default for parsing of `.aspx`, `.asmx`, and `.asax` files, enter an encoding value into the **File encoding** field (default is Windows-1252).
- To set a culture which must be used by default for processing incoming web requests, select an appropriate item from the **Culture** list.
- To set a culture which must be used by default when processing searches for a locale-dependent resource, select an appropriate item from the **UI Culture** list.

8. Set a code access security trust level for ASP.NET applications in the **Code Access Security** field.

CAS trust level is a security zone to which applications execution is assigned, defining what server resources the applications will have access to.

Important: When an assembly is assigned a trust level that is too low, it does not function correctly. For more information on the permissions levels see http://msdn.microsoft.com/library/en-us/dnnetsec/html/THCMCh09.asp?frame=true#c09618429_010.

9. Enable the usage of the auxiliary scripts in the **Script Library Settings** field. Specifying the script library settings is necessary if the validation web controls are used on your web site. This option is available only for ASP.NET 1.1.x.

- If you need to use auxiliary scripts (specifically, scripts implementing objects for validating input data), provide the settings for .NET framework script library. To do so, enter the path beginning with the domain root directory preceded by the forward slash into the **Path to Microsoft script library** field, or click the folder icon next to the **Path to Microsoft script library** field and browse for the required location.
- To initiate the auto-installation of files containing the scripts to the specified location, select the **Install** checkbox. If the files already exist there, they will be rewritten.

10. Set client session parameters in the **Session Settings** field:

- To set up the default authentication mode for applications, select an appropriate item from the **Authentication mode** list. **Windows** authentication mode should be selected if any form of IIS authentication is used.
- To set up time that a session can remain idle, type the number of minutes into the **Session timeout** box.

11. Click **OK** to apply all changes.

Web Server Settings

Web server type depends on Panel version: *Apache* (with *nginx*) is used on Panel for Linux, and *IIS* on Panel for Windows. Depending on your Panel version, refer to **Apache Web Server Settings** (on page 408) or **IIS Web Server Settings** (on page 410).

Next in this section:

Apache Web Server Settings.....	408
IIS Web Server Settings	410

Apache Web Server Settings

Panel uses the *Apache web server* (http://en.wikipedia.org/wiki/Apache_HTTP_Server) to deliver the pages of your website to clients (such as browsers through which visitors access your website). By default, to achieve better performance, Apache is supplemented with another web server - *nginx*. For details about how Apache is integrated with *nginx* in Panel, see **Apache with nginx** (on page 30) in the Administrator's Guide.

Default web server settings are specified by the server administrator (hosting provider). For example, these settings can determine how web servers process different types of files, how they use SSL, where they store log files, and so on.

However, you (as a website owner) can set up *custom web server settings* for your website. For example, add a new type of the index file, restrict access to the site, and so on.

Note: You can adjust web server settings for your websites only if your hosting subscription provides the corresponding permission.

Next in this section:

Adjusting Apache Web Server Settings	409
--	-----

Adjusting Apache Web Server Settings

All customizable web server settings are located on the **Websites & Domains > <domain_name> > Web Server Settings** page. Custom settings work only for the selected website. The settings are divided into two groups:

- **Common Apache settings.**

These settings are typically changed by site owners, who may want to add a new type of index files (**Index files**), or a MIME type for files with a certain extension (**MIME types**), to restrict access to the site (**Deny access to the site**), or specify Apache handlers for a certain file type (**Handlers**).

- **nginx settings.**

These settings define how the processing of web requests is divided between the Apache and nginx web servers to achieve better performance for a specific site.

Important: nginx settings are for advanced users only. To learn more about nginx settings, see **Adjusting nginx Settings for Virtual Hosts** (on page 35) in the Administrator's Guide.

- **Smart static files processing.**

Caution: Turn off this option only to troubleshoot nginx related issues.

Turning this option off will limit the role of nginx: It will only pass requests and responses without modification. Except for troubleshooting the nginx related issues, we recommend that you leave this option turned on.

- **Serve static files directly by nginx.**

For sites with a lot of static content (like image or video files) and high load, better performance can be achieved by delegating serving static files to nginx. Apache will not take any part in processing the requests for the files with the specified extensions.

For example, to exclude Apache from delivering jpg and gif files, you should turn on the option **Serve static files directly by nginx** and specify file extensions like this

```
gif jpg
```

or

```
gif|jpg
```

Caution: Because requests for static files never reach Apache, they do not pass through Apache handlers. This means, for example, that rewrite rules or .htaccess directives will not be applied.

- **Process PHP by nginx.**

When the **Process PHP by nginx** option is on, Apache does not take any part in processing the requests for PHP files. All requests for PHP files are processed by nginx using the PHP-FPM handler. The handlers used by Apache are not available on nginx. The PHP-FPM is an advanced version of FastCGI which offers significant benefits for highly loaded web applications. To learn more about PHP-FPM, see <http://php-fpm.org/about/>.

Caution: Because requests for PHP files do not reach Apache they do not pass through its handlers (CGI, FastCGI, or an Apache module), so some web apps may not work as expected.

Note that subdomains have their own web server settings, therefore, when you change web server settings for a site that has subdomains, the subdomains will not receive these changes.

If you do not find the necessary setting, contact your server administrator (hosting provider), who can set up more custom settings for websites.

The Default Value of Server Settings

You can set the value of each parameter either by typing a custom value, or leaving the **Default** value. In the latter case, Panel uses the values from the default web server configuration defined by the server administrator (hosting provider).

Your values override the default ones. The only exception is the **Deny access to the site setting** - IP addresses from the default configuration, as well as the IP addresses specified by you, will all be applied to your website. In case of a conflict (for example, when you allow the IP address that is denied in the default configuration), Apache uses your settings.

IIS Web Server Settings

Panel uses the IIS web server (http://en.wikipedia.org/wiki/Internet_Information_Services) to deliver the pages of your website to clients (such as browsers through which visitors access your website). The behavior of IIS is defined by variety of settings.

Default web server settings are specified by the server administrator (hosting provider). For example, these settings can determine how IIS process different types of files, how it uses SSL, and so on.

However, you (as a website owner) can set up custom web server settings for your website. For example, add a new type of the index file, restrict access to the site, and so on.

Note: You can adjust web server settings for your websites only if your hosting subscription provides the corresponding permission.

Next in this section:

Adjusting IIS Web Server Settings..... 411

Adjusting IIS Web Server Settings

All customizable web server settings are located in **Websites & Domains** > select a website > **Web Server Settings**. Custom settings work only for the selected website. The settings are divided into groups:

Common Settings

These settings are typically changed by site owners, who may want to:

- Allow site visitors to view the listing of files and subdirectories of the site's directory in their browsers (**Directory browsing**). The directory listing will be displayed if there are no matches for default index pages in the site's root directory.
- Add a new type of default index pages (**Default documents**).
- Add a new MIME type for files with a certain extension (**MIME types**).

Directory Security Settings

These settings allow site owners to:

- Restrict access to the site by username and password – only system users will be able to access the site (**Anonymous access**). Denying anonymous access may be useful if your site is not intended for any visitor, for example, it is a web application for internal use. Note that FTP users and additional FTP users created in Panel will have access to such a site if they were granted access to the site's directory.
- Force all clients (such as browsers or FTP clients) to use the secure HTTPS protocol to access their site (**Require SSL**). You need this option, for example, if the site contains and transmits personal information.

Access Restriction Settings

These settings allow site owners to restrict access to the site by IP address of the visitor (**Deny access to the site**) by denying and allowing access from certain IP addresses.

Note: Subdomains have their own web server settings, therefore, when you change web server settings for a site that has subdomains, the subdomains will not receive these changes.

If you do not find the necessary setting, contact your server administrator (hosting provider), who can set up more custom settings for websites.

The Default Value of Server Settings

You can set the value of each parameter either by typing a custom value, or leaving the **Default** value. In the latter case, Panel uses the values from the default web server configuration defined by the server administrator (hosting provider).

Your values override the default ones. The only exception is the **Deny access to the site** setting - IP addresses from the default configuration, as well as the IP addresses specified by you, will all be applied to your website. In case of a conflict (for example, when you allow the IP address that is denied in the default configuration), IIS uses your settings.

Website Content

To create your website and fill it with the content you need (text, images, videos, and so on), use one of the methods provided by the Panel:

- Using website creation and management tools. If you do not have a website yet, consider setting one up by yourself with a tool for creating, editing, and publishing websites. You can do this even if you do not possess the necessary web programming and design skills. The best tools of this sort are the following:
 - *Presence Builder* - a website editor integrated with the Control Panel.
 - *Third-party Content Management Systems (CMS)* - web applications for creating and editing websites.
- Uploading existing websites to your hosting account using one the following methods:
 - *FTP client program*. You can obtain a free FTP client from the Internet, or, if you are using Windows, use Windows Explorer. This enables you to access your directory on the hosting server and manage your files. If you collaborate with other people when managing your website (such as programmers or designers), you can provide them with access to your directory using FTP to let them edit the website by themselves.
 - *File Manager*. A tool for uploading and managing website files and directories through the Panel web interface.

Note: if you have a website created in Microsoft FrontPage editor, refer to the section **Working with Microsoft Frontpage Websites (Windows)** (on page 447) for details on managing this site in Panel.

Below you will find detailed descriptions of the ways to manage your content.

Presence Builder

Presence Builder is a great tool that enables users with no knowledge of HTML markup or graphic design skills to create professional-looking sites. Just pick a suitable page design and content template, add your text to the pages, and publish the site.

You can create and publish websites using Presence Builder if your hosting subscription provides this option. If it does not, or if you have already created and published the allowed number of sites, you still can create a new website with Presence Builder and edit it. However, to publish this website, you will need to upgrade your hosting plan.

To start creating a website using Presence Builder or edit an existing Presence Builder site, go the **Websites & Domains** tab, click you domain name, and click **Launch Presence Builder**. Find more information on creating and editing websites in Presence Builder in the chapter **Building Websites with Parallels Presence Builder** (on page 467).

Third-Party Content Management Systems

To create and maintain a website, you can use third-party *Content Management Systems (CMS)* - web applications that let you easily edit a website's structure and content with a graphical user interface. Examples of such systems are *Drupal* and *Joomla*.

CMS are usually server applications, so to start using one of them you should install it on your hosting account. Hence, if you plan to use a CMS, ensure that your hosting subscription allows such applications to be installed.

➤ **To create a website using a CMS:**

1. Go to the **Applications** tab.
2. Find the CMS you need in the list of available applications, and install it as described in the section **Employing Website Applications (on page 421)**.
3. Create and edit your website in the CMS. For information on how to create websites with your CMS, refer to the relevant documentation.

Uploading Using FTP

If you already have all your website files and directories, consider uploading them to your hosting account using FTP. This is the quickest way for simple uploading of files when you do not need to edit or manage them on the server.


➤ **To upload files using FTP:**

1. Connect to your site's domain name with an FTP client program using your FTP access credentials. Learn how to configure these credentials in the section **Adding FTP Accounts (on page 522)**.
2. Copy the website files and directories to your directory on the server.

File Manager

Another way to publish a website created outside the Panel is File Manager - a tool that provides a set of file management functions through the web interface. File Manager is located on the **Files** tab of the Control Panel.

To upload a website from your computer to Panel server with File Manager, open the **Files** tab of the Control Panel and drag the website folder to the central area of this tab. If your website is compressed to a ZIP file, you can upload this file to the server and then extract it by clicking **Extract Files** in the **More** menu.

If you want to edit pages of your website, you can do it in File Manager. It provides an HTML editor that allows visual editing of HTML pages (without needing to manually type HTML tags). To edit a file in the HTML editor, place the mouse pointer over the file, click the link  to open the file's context menu, and select **Edit in HTML Editor**.

You can also edit files in File Manager's text editor if you like. To open a file in the text editor, open the file's context menu and select the **Edit in Text Editor**.

If you have files or web pages that you want to make inaccessible on the Internet, change these files' access permissions in File Manager. To edit access permissions for a file or a directory, click the corresponding link in the **Permissions** column. To learn how to review and edit the permissions, refer to the sections **Setting File and Directory Access Permissions** (on page 416).

Next in this section:

Setting File and Directory Access Permissions..... 416

Setting File and Directory Access Permissions

➤ ***To review or change the permissions set for files and directories on Linux systems:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, select the required workspace in the **Subscription** menu at the top of the screen.

2. Go to the **Files** tab.

The permissions set for files and directories are shown in the **Permissions** column. They are represented as three sets of symbols, for example, 'rwx rwx r--'. The first set tells what the owner of the file or directory can do with it; the second tells what the user group, the file or directory belongs to, can do with the file or directory; the third set indicates what other users (the rest of the world, that is, Internet users visiting a site) can do with the file or directory. R means the permission to read the file or directory, W means the permission to write to the file or directory, and X means the permission to execute the file or look inside the directory.


3. Locate the file or directory for which you want to modify permissions and click a hyperlink in the **Permissions** column.

4. Modify the permissions as desired and click **OK**.


➤ ***To set access permissions for a file or directory on Windows systems:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.




2. Go to the **Files** tab.

3. Locate the file or directory for which you want to set access permissions, and click the corresponding icon .

4. Do the following:

- To make the file or folder inherit permissions from a parent folder (if it does not), select the checkbox **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here**.
- To make the files and folders, which are contained in this folder, inherit the folder permissions you define, select the checkbox **Replace permission entries on all child objects with entries shown here that apply to child objects**.
- To change or remove permissions from a group or a user, click the required name in the **Group or user names** list. If the group or user is not listed in the **Group or user names** list, select the required user or group name from the menu located above the list and click : the user/group appears in the list. Select it.

To allow or deny permissions to a selected group/user, select the **Allow** or **Deny** checkboxes corresponding to permissions listed under **Permissions for <user/group name>**. If the checkboxes in the **Allow** or **Deny** columns are shown in grey, it means that the corresponding permissions are inherited from a parent folder.

- To deny the permissions, which are inherited from a parent object as allowed, select the required checkboxes under **Deny**. This will override inherited permissions for this file/folder.
 - To allow the permissions, which are inherited from a parent object as denied, clear the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** checkbox: this removes the inherited permissions. Then select the required checkboxes under **Allow** and **Deny**.
 - To remove access permissions from a group or user, select the required name in the **Group or user names** list and click the icon  next to it.
5. If you need advanced fine-tuning of permissions, click the **Advanced** button, and do the following:
- To create a permission entry for a group or user, select the required name from the **Group or user names** list and click .
 - To set or change file/folder permissions for a group or user, select the required name from the **Group or user names** list, select the required **Allow** and **Deny** checkboxes corresponding to permissions listed under **Permissions for <user/group name>**.
 - To remove a permission entry for a group or user, select the required name from the **Group or user names** list and click .
 - To make child objects of a folder inherit its permissions defined under **Permissions for <user/group name>**, select the **Replace permission entries on all child objects with entries shown here that apply to child objects** checkbox, and select checkboxes in the **Apply to** list which correspond to the objects that must inherit the permissions.
6. Click **OK**.

(Advanced) Restricting Access to Content

If you have directories in a site that only authorized users should see, restrict access to these directories with password protection.

➤ ***To protect a directory in your site with a password and to specify authorized users:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the site's domain name.
3. Click **Password-protected Directories**.
4. Click **Add Protected Directory**.
5. In the **Directory name** box, specify the path to the directory that you want to protect with a password.

This can be any directory existing in the site, for example: `/private`. If the directory that you would like to protect has not yet been created, specify the path and the directory name – the Panel will create it for you.

6. If you are using a Linux-based account, you can also protect your CGI scripts stored in the `cgi-bin` directory. To do this, leave '/' in the **Directory name** box and select the **cgi-bin** checkbox.
7. In the **Title of the protected area** box, type a resource description or a welcoming message that your users will see when they visit the protected area.
8. Click **OK**. The directory you specified will be protected.
9. To add authorized users, click **Add New User**.
10. Specify the username and password that will be used for accessing the protected area. The password should be from 5 to 14 symbols in length. Click **OK**.

➤ ***To add an authorized user of a protected directory:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the site's domain name.
3. Click **Password-protected Directories**.
4. Click on the name of the directory you need.
5. Click the **Add New User** icon.

6. Specify the username and password that will be used for accessing the protected area. The password should be from 5 to 14 symbols in length.
7. Click **OK**.

➤ ***To change password for an authorized user of a protected directory:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the site's domain name.
3. Click **Password-protected Directories**.
4. Click on the name of the directory you need. A list of authorized users will open.
5. Click on the user's name.
6. Specify the new password and re-type it for confirmation.
7. Click **OK**.

➤ ***To revoke a permission to access the protected directory from a user:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the site's domain name.
3. Click **Password-protected Directories**.
4. Click on the name of the directory you need. A list of authorized users will open.
5. Select a checkbox corresponding to the user's name.
6. Click **Remove**. Confirm the operation and click **OK**.

➤ ***To remove password protection and make the resource available to the public:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the site's domain name.
3. Click **Password-protected Directories**.
4. Select a checkbox corresponding to the name of the directory, from which you want to remove protection.
5. Click **Remove Protection**. The protection will be removed and the contents of the directory will be accessible to the public without restrictions.

Previewing Websites

After you purchase a domain, its registration can require some time. The reason for the delay is that name servers update their zone information periodically. Thus, until all name servers have received information about your zone, you will not be able to access your site by its domain name. Nevertheless, you can always access your site during domain name propagation using the **Preview** button on the **Websites & Domains** tab.

During domain name propagation other people can access your site too. For this purpose, Panel registers your website as a subdomain of one of the provider's sites. For example, if your website is *my-domain.tld* and a provider has configured the preview service on *provider-domain.tld*, you can access your site on *my-domain.tld.192-0-2-12.provider-domain.tld*. Here *192-0-2-12* is the site's IP address where dots are replaced with dashes.

Notes:

The contents of password-protected directories might be inaccessible in the Preview mode.

If you do not have the site preview button on the **Websites & Domains** page, contact your hosting provider.

Web Applications

You can significantly increase your website functionality by using different web apps. Apps installed on a website can perform a number of tasks. If you are an individual, you can, for example, present yourself with a blog or organize an online storage of your media files. Companies can move their business online using the e-commerce or CRM web apps. All these apps are available for installation from the **Applications** tab of the Control Panel.

The list of available apps is governed by your hosting plan. For example, it might include only free apps or no apps at all. For more information on available apps, contact your hosting provider.

App Types

There are two types of web apps:

- Apps installed directly on your website (for example, the *WordPress* blogging platform or the *Joomla!* content management system).
- Apps installed on external servers and provided by third-parties.

Regardless of the installation type, apps can be either *free* or *commercial*. Commercial apps require you to obtain a license key to start working with them. You can recognize commercial apps in the catalog on the **Application** tab by the button **Buy now** (instead of **Install** for free apps). If you decide to use commercial apps, read the **Managing Commercial App Licenses** section to learn more about acquiring and managing app licenses.

App Installation and Maintenance

The process of installation is fully automated and does not require any specific skills. To learn how to install web apps from the Control Panel, refer to the section **Installing Apps**.

Further app management is also facilitated as you can update or remove apps directly in Panel. Moreover, you can access some functions that apps reveal to the Control Panel (without the need to log in to an app). For example, you can add SugarCRM user account right from your Control Panel. Such app functionality is a *service* provided by the app.

After you install an app, grant other auxiliary user accounts access to it if you want them to be able to use the app. To get started with managing apps, see the section **Managing Apps** (on page 423).

App Databases

If an app requires a database, Panel creates it automatically during installation of the app. To create a database, Panel uses *app database settings*, which you can change in the **Main configuration** section (**Show All Settings** link) when installing an app:

- A database name and a database server where the app will store the database.
- Database user credentials, which Panel will use to access the app database. It may be convenient to employ a single database user with access to all databases. In this case, you can create a universal user account and specify it when installing apps. To learn more, refer to the section **Managing Database User Accounts** (on page 545).

Note that if you exceed the maximum number of databases allowed for your subscription, a new app does not create a new database. Instead, it adds tables to one of the existing databases, and adds *prefixes* to table names. Prefixes make it easier to distinguish tables of different apps from each other. For example, the Wordpress app will add the “*wpress_*” prefix to the names of its tables.

Access to Apps

By default, after you install an app, it is available only for users with the **Owner** role. You can make your apps available to certain auxiliary users by adjusting their permissions. For details on setting up access to apps for auxiliary users, refer to the section **Granting Auxiliary Users Access to Apps** (on page 423).

Apps and Auxiliary User Accounts

Some apps let you create and manage user accounts directly in Panel. For example, the SugarCRM app allows you to add SugarCRM users without logging in to the app. All apps with such “account services” can associate their accounts with users of a Panel subscription (auxiliary users). To perform such an association, you should grant the auxiliary users access to that account service (in the same way as you grant access to apps). For details on account association, refer to the section **Linking Apps and Auxiliary (on page 424)User Accounts**.

Next in this section:

Managing Apps	423
Granting Auxiliary Users Access to Apps	423
Linking Apps and Auxiliary User Accounts.....	424
Updating Apps.....	425
Managing Commercial App Licenses	425

Managing Apps

Generally, all apps allow the configuration of their main parameters directly in the Control Panel. You can access app settings by selecting the app from the list in **Applications > Manage My Applications**. After you select an app, you can configure the following:

- **General settings.**
These are basic settings (for example, the app administrator password) that can be changed with **Change Settings**.
- **Service settings.**
If an app provides a part of its functionality to Panel by means of services, you have the option to configure them. For example, the SugarCRM app allows the creation of user accounts and provides this ability as a service in the Control Panel. After you select this service in **Provided services**, you can view all app user accounts and create new ones. For some apps, you can associate the app accounts with auxiliary user accounts. Learn more about account association in the section **Linking App and Auxiliary (on page 424)User Accounts**.

Granting Auxiliary Users Access to Apps

By default, after you install an app, only users with the **Owner** role can access it. To allow other subscription users to access the app:

- Grant permission to access the app to a certain user group in **Users > User Roles**.
- Be sure to add users of your choice to the group.

Once you allow users to access the app, a link to the app appears on their **Websites & Domains** page under the name of the corresponding website. Note that *you can control app access only for user groups*, so you should either modify the permissions of an existing group or create a new one, and then assign users to it.

By default, the app administrator is a subscription user with the **Owner** role. As well as accessing the apps from the **Websites & Domains** page, this user can also install and manage apps within a subscription. For these purposes, their interface has the additional **Applications** tab. You can provide the same administrative privileges to other subscription users by granting the **Install and manage applications** permission to their role in **Users > User Roles**. This gives users full administrative access to *all* apps within a subscription. As well as the administrator, the users with this permission can install, configure, update, and remove apps through the **Applications** tab in their Control Panel.

Linking Apps and Auxiliary User Accounts

Some apps let you create and manage user accounts without logging in to the app. If an app provides such an *account service*, you can link users of a Panel subscription with accounts in the app. To perform such an association:

1. Organize the users into a certain group (**Users > User Roles**).
2. Grant one of these group permissions:
 - *Public access.*
If granted, all users in the group will have access to the app through the link on the **Websites & Domains** page.
 - *Personal access.*
If granted, *the app will automatically create accounts* for all users in the group. After that, the users' **Websites & Domains** page will contain an additional link that allows logging in to a personal account in the app. Note that if you deny the **Personal access** permission, *the app will automatically remove all accounts* associated with this group.

Updating Apps

Automatic Updates

By default, Panel installs the latest available app versions and updates apps immediately once the newer versions are available. However, updating an app can significantly change its functionality: For example, plug-ins or extensions developed for a particular app version may be incompatible with newer versions. Therefore, you might want to turn off automatic updates for a certain app.

➤ **To turn automatic updates on or off:**

1. Go to **Applications > Manage My Applications** and click the app's name.
2. Click **Change Settings**.
3. Select or deselect the option **Automatically update this app when updates are available**.

Manual Updates

If you prohibit automatic updates for an app, Panel will inform you about the availability of newer versions by adding the link **Update available** under the app name in **Applications > Manage My Applications**. Click this link to review the changes available in the new version and decide whether to update the app or continue with the current version.

Managing Commercial App Licenses

If you decide to buy an application license in the Control Panel and click the corresponding button on the **Applications** tab, you will be forwarded to *Storefront*, the online store where you complete your order. Actually it is not only a store, it also includes its own web interface to help you perform various operations with the licenses you own. For example, from this web interface you can renew a license, cancel it, change your payment methods and so on. This section explains how to carry out these operations.

Storefront Basics

When you order a first license in Storefront, it creates an *account* for you. This account contains your personal and financial information; if you log in to Storefront under this account, you will be able to do various operations with your licenses.

Each time you successfully check out in Storefront, a purchase *order* is generated. It is a document that lists the cart items you ordered. Storefront assigns different statuses to orders. These statuses explain the current state of your purchase - whether it is unpaid, canceled, or successfully delivered.

Storefront and Panel share the service plans business model. In Storefront, each application is presented by a separate *service plan*, and when you order an application license you *subscribe* to one of the service plans. In other words, each license you purchase is shown as a *subscription* in the web interface. For instance, if you would like to view a license price, terms, or an expiration date, you should open the corresponding subscription.

Note: If your Panel license comes in a bundle with licenses for certain commercial apps, you will be able to install such apps without proceeding to Storefront. These apps will be accompanied by the **Install Now** button instead of **Buy Now** as they are considered purchased. The pool of used and unused app license keys is available in **Tools & Settings > License Management > Additional License Keys**.

How to Get a License File or Key

After you order a license and pay for it, Storefront sends you an e-mail with your license file or key. We recommend that you keep the information in a safe place because there is no way to request it again or view it from the web interface. If you did not receive the e-mail with a license file or key, contact us at <https://support.parallels.com/>.

Available Operations

The operations you can carry out in Storefront fall into three groups:

- *Operations with your user account.* These operations include viewing and modifying your personal information and preferences and changing the password to your user account.
- *Operations with payments and payment methods.* This group comprises operations with your credit cards, payments, and orders.
- *Operations with subscriptions.* Use them to acquire new licenses, obtain information about your existing licenses, and check the subscription renewal method for a particular subscription.

Learn more about these operations in the subsections of this section.

Next in this section:

User Account.....	427
Payments and Payment Methods.....	428
Subscriptions.....	429

User Account

You can do the following operations with your user account.

View and Change Your Account Information

The system uses your account information to add your personal and financial details into invoices. If you see that you need to update your details, open the **My Contact Info** submenu on the Navigation menu and select **Account Info**.

View and Change Your Personal Information

Your personal information mostly duplicates the account information. It does not appear in financial documents, but some services use this information as technical contact details. For example, it is possible to order a domain name through Storefront, and if you do so, Storefront will send your personal information (as the technical contact) to a domain name registrar.

To view user personal information, open the **My Contact Info > Personal Info** menu on the left panel. Here you can also edit your personal information and change password to your Storefront account.

Configure e-mail notifications

E-mail notifications are sent on different events to your account contact e-mail address. They fall into a number of categories. For example, subscription renewal and expiration, your credit card(s) expiration, etc. You can select messages format for every group of messages and decide whether to send certain messages or not. To configure messages types to receive, open **My Contact Info > Notification Methods**.

Payments and Payment Methods

This section describes operations with payments and credit cards available to you in Storefront.

Registering a Credit Card

Before a credit card becomes available for making online payments, it is necessary to register it in Storefront. To register a credit card, open **Billing Manager > My Financial Info > Payment Methods** and click the appropriate button.

Configuring Automatic Payments

You can assign one of the registered credit cards to be used for paying orders automatically. In this case, you will not need to pay each order manually. If you assign a payment method to be used for automatic payments, the previous default one is unselected automatically. Thus, only one payment method can be used for automated payments.

To turn on automatic payments from a card, go to **Billing Manager > My Financial Info > Payment Methods**, select the card by clicking on its **ID** or **Type**, and, finally, enable automatic payments on the card properties screen.

Making a Payment

To add new payment, open the **Billing Manager > New Payment** link on the dashboard. The adding new payment wizard starts. The list of pending documents appears on the screen. If there are no pending documents, click **Cancel** to finish the wizard. Otherwise, walk through the wizard by providing the payment settings.

Viewing Open Orders

Your open orders are available in the **Billing Manager > My Financial Info > Open Orders** submenu.

Subscriptions

Storefront offers you a powerful and comprehensive mechanism of subscriptions (licenses) management, allowing you to perform the following operations.

Buying a Subscription

If you want to purchase one more app license or another service offered by Storefront, there is no need for you to go to the Control Panel. The Storefront web interface provides all facilities for making the purchase. To start the subscription ordering wizard, open **Billing Manager > Subscription Management** and click **Buy New Subscription**.

Renewing a Subscription Manually

If you did not configure the auto renewal feature, your subscription will expire unless you do not renew it manually. The auto renewal setup instructions are given later in this section. To renew a subscription manually, open **Billing Manager > Subscription Management > Renew Subscription** and follow the wizard steps.

Renewing Subscriptions Automatically

Configuring a subscription for auto renewal helps renewing your subscriptions in time. To allow the auto renewal, open **Billing Manager > Subscription Management > Renew Subscription**, click a subscription for which you want to turn the option on, and click **Turn On AutoRenew Option**. Clear the option to cancel the auto renewal.

Canceling a Subscription

A subscription cancelation results in termination of the subscription services and money refund. To cancel a subscription, open **Billing Manager > Subscription Management > Renew Subscription**, click a subscription you want to cancel, and start the cancelation wizard by clicking **Cancel Subscription**.

(Advanced) Website Security

Next in this section:

Securing Connections with SSL Certificates	430
Protecting Sites from Hotlinking (Windows)	435

Securing Connections with SSL Certificates

If your website transfers private data, for example, visitors' credit card numbers, we recommend that you use the SSL secure channel for this website. To set up such a channel, you should purchase an *SSL certificate* for your website.

SSL certificates are used not only for establishing secure communication channels on the Internet but also for verifying a website's identity as well. When users visit your secure online store, they are notified that your website is really what it claims to be and that all sensitive data, such as credit card numbers, will be transferred over a secure channel.

SSL certificates are issued by specific organizations - *SSL certificate providers*. However, some hosting providers allow customers to purchase SSL certificates directly from Panel.

Purchasing SSL Certificates

Depending on your hosting provider, you can have the following ways of purchasing SSL certificates:

- *Order an SSL certificate from Panel.* This way is available to you if your provider configures the corresponding Panel settings. The links for purchasing SSL certificates from Panel may let you purchase certificates either from your provider in their online store or from Parallels in the MyPlesk outlet. To learn how to order an SSL certificate through Panel, see the section **Purchasing SSL Certificates through Panel** (on page 431).
- *Order an SSL certificate from the SSL certificate provider you like.* In this case, you should create a *certificate signing request (CSR)* for your website in Panel and submit it to an SSL certificate provider. To learn how to create such request and purchase a certificate with it, refer to the section **Generating Certificate Signing Requests** (on page 432).

Securing Websites

After you obtain a certificate for your website, you should secure the connection to the website with the certificate. The section **Securing Websites** (on page 433) explains how to do this.

Securing Websites with Shared SSL Certificates

On Windows systems, you may be able to secure your websites without purchasing your own SSL certificates. This feature is available to you if your hosting provider offers *shared SSL certificates*. The section **Using Shared SSL Certificates (Windows)** (on page 434) explains how to secure a website with a shared SSL certificate.

Next in this section:

Purchasing SSL Certificates Through Panel.....	431
Generating Certificate Signing Requests.....	432
Securing Websites	433
Using Shared SSL Certificates (Windows).....	434

Purchasing SSL Certificates Through Panel

The links for purchasing SSL certificates in Panel let you purchase either certificates from your provider if they offer their own certificates, or certificates from Parallels in the *MyPlesk outlet*. These links may also be unavailable to you if your provider decides so.

➤ **To purchase an SSL certificate through Panel:**

1. Open the corresponding subscription in the Control Panel
2. Go to the **Websites & Domains** and select the website you want to protect with an SSL certificate.
3. Click **Secure Your Sites**.
4. Click **Add SSL Certificate**.
5. Specify the following certificate parameters:
 - *Certificate name*. This will help you identify this certificate in the repository.
 - *Encryption level*. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.
 - *Your location and organization name*. The values you enter should not exceed the length of 64 symbols.
 - *The domain name for which you want to purchase an SSL certificate*. This should be a fully qualified domain name. Example: *your-domain.com*.
 - *The website administrator's e-mail address*.
6. Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.
7. Click **Buy SSL Certificate**.
8. Complete all steps of an SSL certificate purchase in the online store and you will receive your SSL certificate by e-mail.

Generating Certificate Signing Requests

If your hosting provider does not allow purchasing SSL certificates through Panel, you can create a certificate signing request and submit it to an SSL certificate provider. The provider will generate an SSL certificate for your website basing on this request.

➤ **To generate a certificate signing request:**

1. Open the corresponding subscription on the Control Panel
2. Go to the **Websites & Domains** and select the website you want to protect with an SSL certificate.
3. Click **Secure Your Sites**.
4. Click **Add SSL Certificate**.
5. Specify the following certificate parameters:
 - *Certificate name*. This will help you identify this certificate in the repository.
 - *Encryption level*. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.
 - *Your location and organization name*. The values you enter should not exceed the length of 64 symbols.
 - *The domain name for which you want to purchase an SSL certificate*. This should be a fully qualified domain name. Example: *your-domain.com*.
 - *The website administrator's e-mail address*.
6. Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.
7. Click **Request**. Panel will generate your private key and certificate signing request and add them to your certificates repository (**Websites & Domains > Secure Your Sites**).
8. In the list of certificates, click the name of the certificate you need.
9. Locate the **CSR section** on the page, and copy the text that starts with the line **-----BEGIN CERTIFICATE REQUEST-----** and ends with the line **-----END CERTIFICATE REQUEST-----** to the clipboard.
10. Visit the website of the certification authority from which you want to purchase an SSL certificate, and follow the links on their site to start a certificate ordering procedure. When you are prompted to specify CSR text, paste the data from the clipboard into the online form and click **Continue**. The certification authority will create an SSL certificate in accordance with the information you supplied.

Securing Websites

After you receive an SSL certificate for your website, secure the website with this certificate.

➤ **To secure a website with an SSL certificate:**

1. Log in to the Control Panel and select the subscription that contains the website you want to secure in the **Subscriptions** menu at the top of the screen.
2. Go to the **Websites & Domains** and select the website you want to protect with an SSL certificate.
3. Click **Secure Your Sites**.

Upload the SSL certificate: Click **Browse** in the middle of the screen and navigate to the location of the saved certificate. Select it, and then click **Send File**.

This will upload and install the certificate against the corresponding private key.

1. To install the certificate on a site, return to the **Websites & Domains** tab, and click the domain name of the website that you want to secure.
2. To switch on SSL protection, select the **Enable SSL support** checkbox.
3. From the **SSL certificate** menu, select your SSL certificate and click **OK**.

Using Shared SSL Certificates (Windows)

If your hosting service provider offers shared SSL for securing access to sites, then you can switch on SSL encryption without purchasing your own SSL certificate.

➤ ***To secure connections to a site by using an SSL certificate shared by your provider:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** and select the website you want to protect with an SSL certificate.
3. Click **Shared SSL**.
4. Select the domain name of the site that you want to secure.
5. Select the **Switch on shared SSL** checkbox.
6. Specify the virtual directory name in the corresponding input field. The virtual directory with the supplied name will be created under the domain whose SSL certificate is shared (called master SSL domain). This directory will be used for accessing your site through SSL.

For example, let us suppose that you have a domain named mydomain.com, the master SSL domain is defined as master_ssl_domain.com, and the virtual directory name you supplied is my_virtual_dir. In this case, to access your site through SSL, you need to use the following address: https://master_ssl_domain.com/my_virtual_dir.

Note: You cannot use your domain name (for example, mydomain.com) to access your site via SSL if you are using shared SSL.

7. Select the directory where protected content is located under your website. The documents within the specified directory will be accessible only through SSL.
8. To make your domain accessible via SSL only, select the checkbox **Make this website accessible only through secure connections**.
9. Click **OK**.

Protecting Sites from Hotlinking (Windows)

Hotlinking (also called file leeching, remote linking, direct linking, bandwidth stealing or bandwidth banditism) is a term used for describing a situation when a web page of one domain owner is directly linking to images (or other multimedia files) on the web pages of another domain owner, usually using an tag. If your domains are hotlinked, you may face the problem of excessive bandwidth usage.

➤ *To protect a website from hotlinking:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Hotlink Protection**.
4. Click **Switch On** to enable the protection from hotlinking.
5. Specify the extensions of files that you want to protect from hotlinking (for example, jpg, bmp, and so on) in the **Protected files extensions** field. When listing several file extensions, separate them with white spaces.
6. If you want to allow direct linking to your files from certain sites, type the website addresses into the **Addresses of friendly websites** field, and click **Add**.
7. Click **OK**.

(Advanced) Extended Website Management

Panel provides a number of operations on websites and domains for advanced users: Working with third-party applications and services, fine tuning of some system services, and much more. This section contains the detailed instructions on all these operations.

Next in this section:

Working with a Staging Site.....	436
Setting Up Mobile Sites	438
Setting Up Custom Error Pages	439
Using Google Services	441
Hosting Personal Web Pages Under Your Domains	443
Limiting Bandwidth and Number of Connections to Websites	446
Working with Microsoft FrontPage Websites (Windows).....	447
Using Virtual Directories (Windows)	452
Setting Up IIS Application Pool (Windows)	465
Web Publishing with Web Deploy (Windows)	466

Working with a Staging Site

If you have a production website and are planning major site changes, consider setting up a staging site — a separate location on the server where you can conveniently update and test a copy of the site before putting it into production.

We recommend that you work with a staging site in the following way:

1. Decide where you want to host the development copy and prepare the development environment. You can choose to host it in the same webspace, in a separate webspace on the same server, or upload it to an FTP account on another server.
If you choose the same webspace, then you first need to set up a new website by adding a domain or a subdomain.
2. (Optional step.) If you set up your development environment under your account in the Panel and your production site has APS applications installed via the Panel (at the **Applications** tab), install the desired site applications in your development environment in the same subdirectory as you have on your production site. This step is optional; however, it will help you avoid changing manually database connection settings in the application scripts.
3. Make a copy of the website and place it in the staging environment.
4. Make copies of the databases used by the site and deploy them in the staging environment.
5. Change database connection settings in the scripts to point at the databases in the staging environment.
6. (Optional step.) Complete APS applications setup. Go to the **Applications** tab for your development site, locate the application in the list of installed applications, open its **Settings** screen and re-save the parameters. With this operation, the APS scripts should stop pointing at the production database and reconnect the application to the database copy. This step is needed if your production site has APS apps installed via the Panel and you performed Step 2 of the current instruction.
7. Make the required changes to the site copy in the staging environment, and test them to make sure everything works as intended.
8. Publish the updated site. This is done by pointing the document root of the production site to the staging site location.

➤ *To set up a site for staging purposes:*

1. Go to the **Websites & Domains** tab.
2. Click either **Add New Domain** or **Add New Subdomain**.
We recommend that you use a subdomain for staging purposes.
3. Proceed as described in **Adding Domains** (on page 379) or **Adding Subdomains** (on page 381).

If you do not want your staging site to be accessible to the Internet users, do not register the newly added domain or subdomain name with a domain name registrar, or use an `.htaccess` file (on Linux hosting) to restrict access to it.

➤ **To make a copy of website files:**

1. Go to the **Websites & Domains** tab and click the name of the website you want to copy.
2. Click **Website Copying**.
3. To copy website files to the document root of an existing site:
 - a. Select the option **Website in the Panel**.
 - b. Select the destination site from the **Site name** menu.
 - c. Specify what to do with the files that might already be present in the destination directory.
4. To copy website files to an FTP account on this or another server:
 - a. Select the option **FTP storage**.
 - b. Specify the server's host name and credentials for connecting to the FTP account.
 - c. In the **FTP connection method** field, leave the **Active mode** option selected. If the Panel fails to connect to the external FTP account, select the **Passive mode** option here.
5. Click **OK**.

If the site uses scripts that work with a database, copy the database to the staging environment:

- If the database is hosted on the same server managed by Panel 10, use the procedure below to copy it.
- If the database is hosted on a server which is not managed by Panel 10, use the `mysqldump` utility to export the database, move the resulting data dump file to the staging environment and deploy it there. Modify the site's scripts in the staging environment so that they connect to the copied database.

➤ **To make a copy of a database from the Panel-managed server:**

1. Go to the **Websites & Domains** tab > **Databases**.
2. Click **Copy** in the databases list for the database you want to copy.
3. Specify the following:
 - **Destination database server.** You can select the same Panel-managed database server, or a database server located elsewhere. For an external database server, specify the host name or IP address, and access credentials: the username and password of a database management system user authorized to create new databases and database tables.
 - **Destination database.** You can choose to create a new database or copy the data to an existing database.
 - **Create a full copy.** Leave this option selected to copy the database structure and all data.

4. Click OK.

The copy of the database will be deployed on the destination server.

5. Modify the site's scripts in the staging environment so that they connect to the copied database.

When the site copy in the staging environment is updated and ready to go live, publish it as described in the following steps.

➤ To publish the updated site to the production environment:**1. Go to the Websites & Domains tab.****2. In the list of domain names, locate the address of your production site and click it.****3. In the Document root box, specify the document root directory of the staging site.****4. Click OK.**

This will make the updated site copy in the staging site location accessible to visitors of your production site address.

Setting Up Mobile Sites


Your service plan may include the option to create website copies optimized for viewing on mobile devices. The copies are hosted with external UNITY Mobile online service.

Important: In Panel 10.4, if a customer ordered the Unity Express offering from the Applications tab, the system could confuse the offering with Unity One. If you faced this problem, we recommend that you remove the site created with Unity One and create the new one in order to get Unity Express.

➤ To create a copy of your website optimized for viewing on mobile devices, or set up a new mobile website:**1. Go to Websites & Domains tab and click the site's domain name.****2. Click Mobile Websites.****3. Click the corresponding Create Mobile Site link.****4. Specify an address for the mobile site.**

If your site is accessible, for example, by domain name `example.com`, you can type a prefix like `mobile`, and then the optimized copy of your website will be accessible by the address `mobile.example.com`.

5. Click OK.**6. Click Edit Site Content.** A UNITY Mobile site opens in a new browser window or tab, and you are logged on under your account.

7. In the **Import from the web** section showing your main website's domain name, click the button .
8. Complete the website import wizard by following instructions presented on the screen.

After the mobile site is created, you can add a link to it to your main site.

You can now perform the following operations on the mobile site using links in Control Panel:

- Open site editor.
- Remove mobile site.

Setting Up Custom Error Pages

When visitors coming to a site request pages that the web server cannot find, the web server generates and displays a standard HTML page with an error message. You may want to create your own error pages and use them for your sites or individual virtual directories. The following error messages are the ones customized most often:

- 400 Bad File Request. Usually means the syntax used in the URL is incorrect (for example, uppercase letter should be lowercase letter; wrong punctuation marks).
- 401 Unauthorized. Server is looking for some encryption key from the client and is not getting it. Also, wrong password may have been entered.
- 403 Forbidden/Access denied. Similar to 401; a special permission is needed to access the site – a password or username, if it is a registration issue.
- 404 Not Found. Server cannot find the requested file. File has either been moved or deleted, or the wrong URL or document name was entered. This is the most common error.
- 500 Internal Server Error. Could not retrieve the HTML document because of server configuration problems.
- 503 Service Temporarily Unavailable. The site is temporarily unavailable due to maintenance.

Next in this section:

Setting Up Custom Error Pages on Windows Servers	440
Setting Up Custom Error Pages on Linux Servers	441

Setting Up Custom Error Pages on Windows Servers

➤ **To configure the web server to show custom error pages for a site or a directory within a site:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Switch on support for custom error documents.
 - a. Go to the **Websites & Domains** tab and click the **Hosting Settings** button beside domain name you need.
 - b. Select the **Custom error documents** checkbox.
 - c. Click **OK**.
3. Go to the **Websites & Domains** tab.
4. Click the domain name you need.
5. Click **Virtual Directories** to see the list of error documents for the root web directory. Error documents located here are used for all web pages of the selected site. If you want to customize error pages for a specific virtual directory, navigate to that directory.
6. Click **Error Documents** tab and click the required error document in the list.
 - To use the default document provided by IIS for this error page, select **Default** in the **Type** menu.
 - To use a custom HTML document already located in the `error_docs` directory in the virtual host directory of the domain, select **File** in the **Type** menu and specify the file name in the **Location** field.
 - To use a custom HTML document located in a directory other than `error_docs` on a domain, select **URL** in the **Type** menu and enter the path to your document in the **Location** field. The path should be relative to the virtual host root (that is, `<vhosts>\<domain>\httpdocs`).

For example, you have created a file `forbidden_403_1.html` and saved it in the `my_errors` directory located in the `httpdocs`. To use this file as an error document, you need to type the following path into the **Location** field:

```
/my_errors/forbidden_403_1.html.
```

Note: You can use a connection over FTP or File Manager in the Panel to upload your custom error document to the server. By default, all error documents are stored in the `/vhosts/your-domain.com/error_docs/` directory (located in `C:\InetPub` by default).

7. Once the web server is restarted, it will start using your error documents.

Setting Up Custom Error Pages on Linux Servers

➤ ***To configure the web server to show custom error pages for a site:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Switch on support for custom error documents.
 - a. Go to the **Websites & Domains** tab and click the **Hosting Settings** button beside domain name you need.
 - b. Select the **Custom error documents** checkbox.
 - c. Click **OK**.
3. Connect to your FTP account, and go to the `error_docs` directory.
4. Edit or replace the respective files. Be sure to preserve the correct file names:
 - 400 Bad File Request - `bad_request.html`
 - 401 Unauthorized - `unauthorized.html`
 - 403 Forbidden/Access denied - `forbidden.html`
 - 404 Not Found - `not_found.html`
 - 405 Method Not Allowed - `method_not_allowed.html`
 - 406 Not Acceptable - `not_acceptable.html`
 - 407 Proxy Authentication Required - `proxy_authentication_required.html`
 - 412 Precondition Failed - `precondition_failed.html`
 - 414 Request-URI Too Long - `request-uri_too_long.html`
 - 415 Unsupported Media Type - `unsupported_media_type.html`
 - 500 Internal Server Error - `internal_server_error.html`
 - 501 Not Implemented - `not_implemented.html`
 - 502 Bad Gateway - `bad_gateway.html`
 - 503 Service Temporarily Unavailable - `maintenance.html`

The web server will start using your error documents in a few hours, after it is restarted.

Using Google Services

Using links in the Panel, you can generate code for inserting a custom Google search engine into your site, submit your website to Google through Webmaster Tools area, enroll in the AdSense program, embed YouTube videos, Google Translate service, or other Google products into your site.

Google Custom Search is a search engine provided by Google. It adds search functions to your site and allows you to apply your website's look and feel to the search results page. It can be used for free on websites of individuals and non-profit organizations. Websites related to for-profit businesses can either use a Custom Search Engine that will show advertisements from Google, or purchase a subscription to Google Site Search service, which starts from \$100 per year. To learn more about Google Site Search and current prices, visit <http://www.google.com/sitesearch>.

Google Webmaster Tools allow webmasters to submit a website to Google and view search statistics. To learn more about Webmaster Tools, visit <http://www.google.com/support/webmasters/?hl=en>.

Google AdSense allows webmasters to earn money for displaying targeted Google ads on their websites. To learn more about AdSense, visit <https://www.google.com/adsense/login/en/>.

Google Web Elements allows webmasters to easily add their favorite Google products to websites. Embed content, such as news, maps, YouTube videos, and social conversations from Google Friend Connect to Web pages with simple cut-n-paste. To learn more about Google Web Elements, visit <http://www.google.com/webelements/>.

Before you start using Google services, you need to confirm acceptance of Google Terms of Services, and then confirm ownership for your sites.

➤ ***To confirm acceptance of Google terms of service and then confirm ownership of your sites:***

1. Go to the **Websites & Domains** tab, and click the **Google Services for Websites** link.
2. Click the appropriate links in the Panel to open and read the Terms of Service documents.
3. To confirm that you accept the Terms of Service, select the checkbox and click **Confirm**.

Now you can do the following:

- Submit your site to Google and improve site visibility in search results by clicking **Google Webmaster Tools**.
- Add search functions to a site by clicking **Add New Custom Search Engine**.
- Enroll in the AdSense program by clicking **Google AdSense**.
- Embed Google products into your site by clicking **Google Web Elements**.

➤ ***To submit a site to Google:***

1. Go to the **Websites & Domains** tab and click the site's domain name.
2. Click the **Google Services for Websites** link.

3. Click **Google Webmaster Tools**.

The Google Webmaster Tools area opens in a new browser window or tab.

4. Create a *Sitemap* and submit it to Google by following instructions at <http://www.google.com/support/webmasters/bin/answer.py?hl=en&answer=156184>.

➤ ***To add a custom search engine to a site:***

1. Go to the **Websites & Domains** tab and click the site's domain name.
2. Click the **Google Services for Websites** link.
3. Click **Custom Site Search**.
4. Click **Add New Custom Search Engine**.
5. Type a search engine name and select the website you need.
6. Select the checkbox to confirm your acceptance of Terms of Service, and click **OK**.

The record corresponding to the new search engine is added to the Panel.

7. Click the corresponding **Get Code** link, copy the generated code to the clipboard and paste it into the source code of your website pages.

The other links in the list of Custom Search Engines will help you perform the following operations:

- **Make Money.** Connect your Custom Search Engine to a Google AdSense account. You make money when users click on an ad they see in your search results. If you have more than one Custom Search engine, all of your search engines will automatically be associated with the same AdSense account.
- **Manage.** Manage your Custom Search Engines.
- **Look and Feel.** Adjust the appearance of search box and search results page.
- **Upgrade.** Upgrade a Custom Search Engine to ads-free Google Site Search.
- **Statistics.** Review site search reports.
- **Delete.** Delete a Custom Search Engine.

➤ ***To participate in the Google AdSense program:***

1. Go to the **Websites & Domains** tab and click the site's domain name.
2. Click the **Google Services for Websites** link.
3. Click **Google AdSense**.
4. Click **Google AdSense** account.
5. Fill in all the required fields to create a new AdSense account, or select an existing account, and click **OK**.

A confirmation e-mail with further instructions will be sent to your e-mail address.

Hosting Personal Web Pages Under Your Domains

You can host on your web server personal web pages for users who do not need their own domain names. These pages usually have web addresses like `http://your-domain.com/~username`.

➤ ***To accommodate a personal web page under your domain and set up an FTP account for publishing:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the domain name under which you want to create a personal web page.
3. Click **Web Users**.
4. Click **Settings**.
5. If you want to allow execution of scripts embedded in personal web pages, select the **Allow web users to use scripts** checkbox.
6. Click **OK**.

The settings you have defined at the step 4 are common for all personal web pages you might host on your account. Therefore, you will not need to perform the steps from 3 to 5 next time you set up a new web user account.

7. Click **Add New Web User**.
8. Specify a username and a password that will be used for accessing the workspace through FTP and publishing the web pages.
You can use only lower-case alphanumeric, hyphen and underscore symbols in the username. The username should begin with an alphabet character. It cannot contain white spaces. The password cannot contain quotation marks, white space, username, and should be between 5 and 14 characters in length.
9. If you want to limit the amount of disk space that can be occupied by the web page content, type the desired value in megabytes into the **Hard disk quota** box.

When the specified limit is exceeded, the web page owner will not be able to add files to his or her workspace.

10. Specify the programming languages that should be supported for the web page.
For example, if the web page is written in PHP, select the **PHP support** checkbox.
11. If you use a Windows-based hosting account and this personal web page's applications need to use a file-based database (like Jet) located in the root of `httpdocs` directory, select the **Additional write/modify permissions** option. Note that selecting this option might seriously compromise the website security.

12. Click **OK**.

Now you can tell your user the FTP account credentials, so that he or she can publish their web page.

➤ ***To change FTP password for a web page owner:***

1. Go to the **Websites & Domains** tab and click the name of the domain that contains the personal page.
2. Click **Web Users**.
3. Click the user name you need.
4. Type the new password into the **New password** and **Confirm password** boxes.
5. Click **OK**.

➤ ***To allocate more disk space to the web page owner:***

1. Go to the **Websites & Domains** tab and click the name of the domain that contains the personal page.
2. Click **Web Users**.
3. Click the user name you need.
4. Type the amount of disk space in megabytes into the **Hard disk quota** box.
5. Click **OK**.

➤ ***To remove a web page owner's account together with their web page:***

1. Go to the **Websites & Domains** tab and click the name of the domain that contains the personal page.
2. Click **Web Users**.
3. Select a checkbox corresponding to the user account you want to remove and click **Remove**.
4. Confirm removal and click **OK**.

Limiting Bandwidth and Number of Connections to Websites

To avoid excessive usage of bandwidth, and protect your site from Denial Of Service attacks, you can limit bandwidth usage for a site and number of simultaneous connections.

➤ ***To limit bandwidth usage and number of connections to a site:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the site's domain name.
3. Click **Bandwidth Limiting**.
4. Select the **Switch on bandwidth limiting** checkbox.
5. In the **Maximum bandwidth usage (KB/S)** box, specify the maximum speed, measured in kilobytes per second, that a website can share among all its connections.
6. Select the **Switch on connections limiting** checkbox.
7. In the **Connections limited to** box, specify the maximum number of simultaneous connections to the site.
8. Click **OK**.

Working with Microsoft FrontPage Websites (Windows)

Microsoft FrontPage deals with two kinds of websites: disk-based and server-based. In short, a disk-based site is a FrontPage website you create on your local hard disk and then later publish to the server. A server-based site is one you create and work with directly on the server, without the extra step of publishing. This section provides you with instructions on publishing only disk-based websites.

You can publish disk-based websites either through FTP or HTTP. If your hosting server is running FrontPage Server Extensions, you would publish your site over HTTP. For example: `http://your-domain.com/MyWebSite`. If your hosting server supports FTP, you would publish to an FTP location. For example: `ftp://ftp.your-domain.com/myFolder`.

After publishing, you can manage your site through FrontPage Server Extensions.

➤ *To access FrontPage Server Extensions management interface:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Click the **Websites & Domains** tab and click the name of the website you want to manage in Frontpage.
3. Click **FrontPage**.
4. Do either of the following:
 - To manage a site over HTTP connection, click **Frontpage Webadmin**.
 - To manage a site over a secure SSL connection, if SSL support is enabled for the site, click **Frontpage SSL Webadmin**.
5. Type your FrontPage administrator's username and password, and click **OK**.

For instructions on using FrontPage server extensions, see online help (**Frontpage Webadmin > Help**) or visit Microsoft website.

The following FrontPage settings are changeable through the Panel:

- The use of Microsoft FrontPage IIS Index Server for building the full-text index of your website.
- SMTP mail server and sender's e-mail address. These options are applicable if you use FrontPage forms that submit information from your site by e-mail. By default, SMTP server specified in the domain's DNS zone is used for sending mail. If no SMTP server is specified in the zone, then FrontPage uses the mail service running on the server where the domain (site) is hosted.

➤ **To change any of these settings:**

1. Click the **Websites & Domains** tab and click the name of the website you want to manage in Frontpage.
2. Go to **FrontPage > Settings**.
3. Make the required changes and click **OK**.

Next in this section:

Publishing FrontPage Websites	449
Adding FrontPage Accounts	451

Publishing FrontPage Websites

➤ *To publish files through FTP:*

1. Open your FrontPage program.
2. Open a FrontPage website: open **File** menu and select the **Open Site** item.
3. Go to **Remote Web site** view: click the **Web Site** tab, and then the **Remote Web Site** button at the bottom of the window.
4. Set up your Remote Web Site Properties:
 - Click the **Remote Web Site Properties** button in the upper-right corner of the window.
 - Select **FTP** as the remote Web server.
 - In the **Remote Web site location** box, type your host name (for example, ftp://ftp.your-domain.com)
 - In the **FTP directory** box, type your FTP directory if your hosting company provided one. Leave it blank if they did not specify one.
 - Select the **Use Passive FTP** check box if your computer or network is protected by a firewall.
5. Click **OK** to connect to the remote site.

The Remote Web site view will show files that you have in your local and remote sites.
6. Click the **Publish Web site** button in the lower-right corner of the window.

➤ *To publish files through HTTP on a server that supports FrontPage Server Extensions:*

1. Open your FrontPage program.
2. Open a FrontPage website: open **File** menu and select the **Open Site** item.
3. Go to **Remote Web site** view: click the **Web Site** tab, and then the **Remote Web Site** button at the bottom of the window.
4. Click the **Remote Web Site Properties** button in the upper-right corner of the window.
5. On the **Remote Web Site** tab, under **Remote Web server type**, click **FrontPage or SharePoint Services**.
6. In the **Remote Web site location** box, type the Internet address, including the protocol, of the remote website that you want to publish folders and files to, for example, http://www.your-domain.com, or click **Browse** to locate the site.

7. Do any of the following:

- To use Secure Sockets Layer (SSL) for establishing a secure communications channel to prevent the interception of critical information, click **Encryption connection required (SSL)**. To use SSL connections on your web server, the server must be configured with a security certificate from a recognized certificate authority. If the server does not support SSL, clear this check box. Otherwise, you will not be able to publish folders and files to the remote website.
- To remove specific types of code from web pages as they are being published, on the **Optimize HTML** tab, select the options you want.
- To change the default options for publishing, on the **Publishing** tab, select the options you want.

8. Click **OK** to connect to the remote site.

The **Remote Web site** view will show files that you have in your local and remote sites.

9. Click the **Publish Web site** button in the lower-right corner of the window.

Adding FrontPage Accounts

If you are using Microsoft FrontPage for collaborating on website content with other users, then you need to create additional Microsoft FrontPage accounts.

➤ *To create an additional Microsoft FrontPage account:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the domain name of the website for which you create the account.
3. Click **FrontPage**.
4. Click **Add New FrontPage Account**.
5. Specify the following:
 - Username and password for the account.
 - Limit on disk space. If you wish to limit the amount of disk space that can be used by this account, clear the **Unlimited** check box and type the desired value in megabytes into the **Hard disk quota** box.

When the specified limit is exceeded, the user will not be able to upload more files to the workspace.
6. Click **OK**.

➤ *To change settings for an additional Microsoft FrontPage account:*

1. Go to the **Websites & Domains** tab and click the domain name of the website that contains the account.
2. Click **FrontPage**.
3. Click the required account name in the list.
4. Adjust the settings as necessary and click **OK** to save changes.

➤ *To remove an additional Microsoft FrontPage account:*

1. Go to the **Websites & Domains** tab and click the domain name of the website that contains the account.
2. Click **FrontPage**.
3. Select the checkbox corresponding to the account you want to remove.
4. Click **Remove**.
5. Confirm the removal and click **OK**.

Using Virtual Directories (Windows)

A virtual directory is a link to an existing physical directory that is present on the server's hard disk. Virtual directories can have a number of specific settings like custom ASP.NET configuration, access permissions, and protection with a password.

Because any virtual directory can have its own settings, including customized ASP.NET configuration, virtual directories are very useful in setting up your web applications, especially those written in ASP.NET. For example, if you have three web applications that use ASP.NET version 1.1, and you need to install one web application that uses ASP.NET version 2.0, you can create a virtual directory for the ASP.NET 2.0 application, configure ASP.NET settings for this directory so as to enable support for version 2.0, and then successfully install the required application.

Virtual directories can also be used as aliases. For example, you have a web application installed on your domain "example.com" in the physical directory `"/my_data/web_apps/forum"`. To access this web application, users need to type `"example.com/my_data/web_apps/forum"`, which is hard to remember and too long to type. You can create virtual directory called `forum` in the root of your virtual host, and link this virtual directory to `"/my_data/web_apps/forum"`, so the users who want to access the web application will need to type `"example.com/forum"`, which is much shorter and easier to remember.

Next in this section:

Creating Virtual Directories.....	453
Configuring ASP.NET for Virtual Directories.....	455
Configuring PHP for Virtual Directories.....	457
Setting Up Access to Virtual Directories	458
Changing Virtual Directory Settings	461
Adding and Removing MIME Types	463

Creating Virtual Directories

➤ **To create a virtual directory within a website:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**. You are in your web site root now.
4. Navigate to the directory in which you want to create a new virtual directory.
5. Click **Create Virtual Directory**.

Note: To create a physical directory instead of virtual directory, click **Create Directory**, specify the name of the directory and click **OK**.

6. Specify the required parameters:
 - **Name** - specify the virtual directory name.
 - **Path** - specify the virtual directory path:
 - Select the **Create physical directory with the same name as virtual directory** checkbox to automatically create a physical directory with the same name as the virtual directory you are creating.
 - Clear the **Create physical directory with the same name as virtual directory** checkbox and specify the path in the field to select a physical directory that already exists.
 - **Script source access** - select this checkbox to allow users to access source code if either Read or Write permissions are set. Source code includes scripts in ASP applications.
 - **Read permission** - select this checkbox to allow users to read files or directories and their associated properties.
 - **Write permission** - select this checkbox to allow users to upload files and their associated properties to the virtual directory or to change content in a write-enabled file. Write access is allowed only if browser supports the PUT feature of the HTTP 1.1 protocol.
 - **Directory browsing** - select this checkbox to allow users to see a hypertext listing of the files and subdirectories in the virtual directory.
 - **Log visits** - select this checkbox if you want to store the information about visits of the virtual directory.
 - **Create application** - select this checkbox to make the directory an IIS application. The directory becomes logically independent from the rest of the website.
 - **Execute permissions** - select the appropriate program execution level allowed for the virtual directory.
 - **None** - allow access only to static files such as HTML or image files.
 - **Scripts only** - allow running scripts only, not executables.

- **Scripts and Executables** - remove all restrictions so that all file types can be executed.
- **ASP Settings** - set specific settings for ASP-based web applications.
 - If you are using ASP-based applications that cannot operate correctly under data transfer restrictions currently set by IIS, clear the **Defined by parent directory** checkbox corresponding to the field you want to change and type in the required number.
 - If you want to enable debugging of ASP applications on the server side, clear the corresponding **Defined by parent directory** checkbox and select the **Enable ASP server-side script debugging** checkbox.
 - If you want to enable debugging of ASP applications on the client side, clear the corresponding **Defined by parent directory** checkbox and select the **Enable ASP client-side script debugging** checkbox.

Note that if you are trying to change ASP Settings for the root virtual directory, the default checkbox names will be **Defined by IIS** instead of **Defined by parent directory**.

7. Click **OK**.

➤ ***To remove a virtual directory from a website:***




1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Select the checkbox corresponding to the directory you want to remove.
5. Click **Remove**.
6. Confirm the removal and click **OK**.

Configuring ASP.NET for Virtual Directories


➤ *To configure ASP.NET settings for a virtual directory within a website:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Browse to the required directory and click a link with its name.
5. Click **ASP.NET Settings**.
6. Set up the strings that determine database connection data for ASP.NET applications that use databases. This option is available only for ASP.NET 2.0.x.

When you open the ASP.NET configuration page for the first time, sample connection parameters with common constructions are displayed. You can delete them and specify your own strings.

- To add a string, enter the required data into the **Name** and **Connection Parameters** input fields and click  next to them.
 - To remove a string, click  next to it.
7. Set up custom error messages that will be returned by ASP.NET applications:
 - To set the custom error messages mode, select an appropriate option from the **Custom error mode** menu:
 - **On** - custom error messages are enabled.
 - **Off** - custom error messages are disabled and detailed errors are to be shown.
 - **RemoteOnly** - custom error messages are displayed only to remote clients, and ASP.NET errors are shown to the local host.
 - To add a new custom error message (which will be applied unless the **Off** mode was selected), enter the values in the **Status Code** and **Redirect URL** fields, and click .
 - **Status Code** defines the HTTP status code resulting in redirection to the error page.
 - **Redirect URL** defines the web address of the error page presenting information about the error to the client.

Due to possible conflicts, you cannot add a new custom error message with an error code that already exists, but you can redefine the URL for the existing code.

 - To remove a custom error message from the list, click  next to it.
 8. Configure compilation settings in the **Compilation and Debugging** field:
 - To determine the programming language to be used as default in dynamic compilation files, choose an entry from the **Default web page language** menu.
 - To enable compiling of retail binaries, leave the **Switch on debugging** checkbox empty.

- To enable compiling of debug binaries, select the **Switch on debugging** checkbox. In this case, the source code fragments containing error will be shown in a diagnostic message.

Note: When running applications in debug mode, a memory and performance overhead occurs. We recommended that you use debugging when testing an application, and disable it before deploying the application into production scenario.

9. Configure encoding settings for ASP.NET applications in the **Globalization Settings section:**

- To set an adopted encoding of all incoming requests, enter an encoding value into the **Request encoding** field (default is utf-8).
- To set an adopted encoding of all responses, enter an encoding value into the **Response encoding** field (default is utf-8).
- To set an encoding which must be used by default for parsing of `.aspx`, `.asmx`, and `.asax` files, enter an encoding value into the **File encoding** field (default is Windows-1252).
- To set a culture which must be used by default for processing incoming web requests, select an appropriate item from the **Culture** list.
- To set a culture which must be used by default when processing searches for a locale-dependent resource, select an appropriate item from the **UI Culture** list.

10. Set a code access security trust level for ASP.NET applications in the **Code Access Security field.**

CAS trust level is a security zone to which applications execution is assigned, defining what server resources the applications will have access to.

Important: When an assembly is assigned a trust level that is too low, it does not function correctly. For more information on the permission levels, see http://msdn.microsoft.com/library/en-us/dnnetsec/html/THCMCh09.asp?frame=true#c09618429_010.

11. If you are using ASP.NET 1.1.x, then you can enable the usage of the auxiliary scripts in the **Script Library Settings field. Specifying the script library settings is necessary if the validation web controls are used on your web site.**

- If you need to use auxiliary scripts (specifically, scripts implementing objects for validating input data), provide the settings for .NET framework script library. To do so, enter the path beginning with the domain root directory preceded by the forward slash into the **Path to Microsoft script library** field, or click the folder icon next to the **Path to Microsoft script library** field and browse for the required location.
- To initiate installation of files containing the scripts to the specified location, select the **Install** checkbox. If the files already exist there, they will be rewritten.

12. Set client session parameters in the **Session Settings** field:

- To set up the default authentication mode for applications, select an appropriate item from the **Authentication mode** list. **Windows** authentication mode should be selected if any form of IIS authentication is used.
- To set up the allowed session idle time, enter appropriate number minutes into the **Session timeout** field.

13. Click **OK** to apply all changes.

Configuring PHP for Virtual Directories



To be able to use web applications that require PHP4 or PHP5, you can select the required PHP version for individual virtual directories.


➤ ***To select PHP version for a virtual directory within a website:***



1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Browse to the required directory and click a link with its name.
5. In the **Tools** group, click **PHP Settings**.
6. Select the required version of PHP and click **OK**.

Setting Up Access to Virtual Directories

➤ **To set access permissions for a virtual directory within a website:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. To set access permissions for the current virtual directory, in the **Tools** group, click **Directory Access Permissions**. If you want to set permissions for a subdirectory located within the current directory, click the corresponding icon .
5. Do the following:
 - To make the file/folder inherit permissions from a parent folder (if it does not), select the checkbox **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here**.
 - To make the files and folders, which are contained in this folder, inherit the folder permissions you define, select the checkbox **Replace permission entries on all child objects with entries shown here that apply to child objects**.
 - To change or remove permissions from a group or a user, click the required name in the **Group or user names** list. If the group or user is not listed in the **Group or user names** list, select the required user or group name from the menu located above the list and click : the user/group appears in the list. Select it.

To allow or deny permissions to a selected group/user, select the **Allow** or **Deny** checkboxes corresponding to permissions listed under **Permissions for <user/group name>**. If the checkboxes in **Allow** or **Deny** columns are shown in grey, it means that the corresponding permissions are inherited from a parent folder.
 - To deny the permissions, which are inherited from a parent object as allowed, select the required checkboxes under **Deny**. This will override inherited permissions for this file/folder.
 - To allow the permissions, which are inherited from a parent object as denied, clear the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** checkbox: this removes the inherited permissions. Then select the required checkboxes under **Allow** and **Deny**.
 - To remove access permissions from a group or user, select the required name in the **Group or user names** list and click the icon  next to it.

6. If you need advanced fine-tuning of permissions, click the **Advanced** button, and do the following:
 - To create a permission entry for a group or user, select the required name from the **Group or user names** list and click .
 - To set or change file/folder permissions for a group or user, select the required name from the **Group or user names** list, select the required **Allow** and **Deny** checkboxes corresponding to permissions listed under **Permissions for <user/group name>**.
 - To remove a permission entry for a group or user, select the required name from the **Group or user names** list and click .
 - To make child objects of a folder inherit its permissions defined under **Permissions for <user/group name>**, select the **Replace permission entries on all child objects with entries shown here that apply to child objects** checkbox, and select checkboxes in the **Apply to** list which correspond to the objects that must inherit the permissions.
7. Click **OK**.

➤ ***To restrict access to files and directories located within a virtual directory:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Navigate to the directory you want to protect and click the **Protection** tab.
5. Click **Protect**.
6. To specify users who will be able to access the directory, click **Add User**, specify username and password, and click **OK**.
7. If you want to specify a title for the protected area that will be shown to users when they attempt to access the directory, click **Settings**, specify a title, and click **OK**.

➤ ***To revoke a permission to access a directory from a user:***


1. Go to the **Websites & Domains** tab and click the website's domain name.
2. Go to the **Virtual Directories > Protection** tab.
3. Select the checkbox corresponding to the user's name and click **Remove**.

➤ ***To remove protection from a directory and allow the general public to see the directory contents without restrictions:***

1. Go to the **Websites & Domains** tab and click the website's domain name.
2. Go to the **Virtual Directories > Protection** tab.
3. Click **Remove Protection**.
4. Click **OK** to confirm removal.

Changing Virtual Directory Settings

➤ *To change settings of a virtual directory within a website:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Browse to the directory whose preferences you want to change, and click the corresponding icon , or click **Directory Properties** when inside the required directory.
5. Change the settings as required:
 - **Name** - specify virtual directory name.
 - **Path** - specify the path to the physical directory to which the virtual directory is linked.
 - **Script source access** - select this checkbox to allow users to access source code if either Read or Write permissions are set. Source code includes scripts in ASP applications.
 - **Read permission** - select this checkbox to allow users to read files or directories and their associated properties.
 - **Write permission** - select this checkbox to allow users to upload files and their associated properties to the virtual directory or to change content in a write-enabled file. Write access is allowed only if browser supports the PUT feature of the HTTP 1.1 protocol.
 - **Directory browsing** - select this checkbox to allow users to see a hypertext listing of the files and subdirectories in the virtual directory.
 - **Log visits** - select this checkbox if you want to store the information about visits to the virtual directory.
 - **Create application** - select this checkbox to make the web directory an IIS application. The directory becomes logically independent from the rest of the website.
 - **Execute permissions** - select the appropriate program execution level allowed for the virtual directory.
 - **None** - allow access only to static files such as HTML or image files.
 - **Scripts only** - allow running scripts only, not executables.
 - **Scripts and Executables** - remove all restrictions so that all file types can be executed.
 - **Allow to use parent paths** - select this checkbox to allow using double period in the path name when referring to a folder above the current directory. This enables users to move up the folder tree without knowing the folder name or the whereabouts in the hierarchy. If the option is selected, parent path directories should not have the **Execute permission** checkbox selected in their properties, so that applications do not have the ability of unauthorized running of programs in the parent paths.

- **Allow application execution in MTA (multi-threaded apartment) mode** - select this checkbox to allow the application execution in multi-threaded apartment (MTA) mode. Otherwise, the application will run in a single-threaded apartment (STA) mode. Using STA, each application pool is executed in a dedicated process. With MTA, several concurrent application pools are executed in one thread which can increase performance in some cases.
- **Use default documents** - select this checkbox to allow the use of default documents for the current directory. The default document is sent when users access the directory on the web without a specific file name (for example, using `http://www.example.com` as opposed to `http://www.example.com/index.html`). If this checkbox is cleared and the **Directory browsing** checkbox is selected, the web server returns a folder listing. If this checkbox is cleared and the **Directory browsing** checkbox is cleared as well, the web server returns an "Access Forbidden" error message.
- **Default documents search order** - specifies the order in which IIS searches for the default document, sending user the first available file it finds. If no match is found, IIS behaves as in the cases when the default content page is disabled.
- **Allow anonymous access** - select this checkbox if you want to make the directory public so that the Internet users could access it without authentication.
- **Require SSL** - select this checkbox to enable access to the folder only via SSL-encrypted connections.
- **ASP Settings** - set specific settings for ASP-based web applications.
 - If you are using ASP-based applications that cannot operate correctly under data transfer restrictions set by IIS, clear the **Defined by parent directory** checkbox corresponding to the field you want to change and type in the required number.
 - If you want to enable debugging of ASP applications on the server side, clear the corresponding **Defined by parent directory** checkbox and select the **Enable ASP server-side script debugging** checkbox.
 - If you want to enable debugging of ASP applications on the client side, clear the corresponding **Defined by parent directory** checkbox and select the **Enable ASP client-side script debugging** checkbox.

Note that if you are trying to change ASP Settings for the root directory, the default checkbox names will be **Defined by IIS** instead of **Defined by parent directory**.

6. Click **OK** to save changes.

Adding and Removing MIME Types

Multipurpose Internet Mail Exchange (MIME) types instruct a web browser or mail application how to handle files received from a server. For example, when a web browser requests an item on a server, it also requests the MIME type of the object. Some MIME types, like graphics, can be displayed inside the browser. Others, such as word processing documents, require an external application to be displayed.

When a web server delivers a web page to a client web browser, it also sends the MIME type of the data it is sending. If there is an attached or embedded file in a specific format, IIS also tells the client application the MIME type of the embedded or attached file. The client application then knows how to process or display the data being received from IIS.

IIS can only operate files of registered MIME types. These types could be defined both on the global IIS level and on the website or virtual directory level. Globally-defined MIME types are inherited by all websites and virtual directories while ones defined on the website main or virtual directory level are used only for the area where they are defined. Otherwise, if the web server receives request for a file with unregistered MIME type, it returns the 404.3 (Not Found) error.

➤ *To add a new MIME type for a virtual directory within a website:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Navigate to the required virtual directory and click the corresponding link with its name.
5. Click the **MIME Types** tab.
6. Click **Add MIME Type**.
7. Specify the following:
 - Type the file name extension in the **Extension** field. File name extension should begin with a dot (.), or a wildcard (*) to serve all files regardless of file name extension.
 - Specify the file content type in the **Content** field.
 - You can either select the appropriate value from the list or define a new content type. To do this, select **Custom** and enter the content type in the input box provided.
8. Click **OK** to finish the creation.

➤ ***To edit a MIME type for a virtual directory within a website:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Navigate to the required virtual directory and click the corresponding link with its name.
5. Select the **MIME Types** tab.
6. Select the required MIME type in the list.
 - Type the file name extension in the **Extension** field. File name extension should begin with a dot (.), or a wildcard (*) to serve all files regardless of file name extension.
 - Specify the file content type in the **Content** field.
 - You can either select the appropriate value from the list or define a new content type. To do this, select **Custom** and enter the content type in the input box provided.
7. Click **OK** to save changes.

➤ ***To remove a MIME type for a virtual directory within a website:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab and click the website's domain name.
3. Click **Virtual Directories**.
4. Navigate to the required virtual directory and click the corresponding link with its name.
5. Select the **MIME Types** tab.
6. Select the checkbox corresponding to the MIME type you want to remove.
7. Click **Remove**.
8. Confirm removal and click **OK**.

Setting Up IIS Application Pool (Windows)

IIS Application Pool contains all web applications installed on your sites. If your service provider allocated a dedicated IIS application pool for your sites, then you can have a level of isolation between web applications used by your sites and web applications used by other hosting users who host their websites on the same server. Because each application pool runs independently, errors in one application pool will not affect the applications running in other application pools.

Once you switch on the application pool, all web applications on your websites will be using it.

➤ *To switch on dedicated IIS application pool for your websites:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Websites & Domains** tab > **Dedicated IIS Application Pool for Your Websites**.
3. Click **Switch On**.
4. To limit the amount of CPU resources that this application pool can use, select the **Switch on CPU monitoring** checkbox and type a number in percents into the **Maximum CPU use (%)** box.
5. Click **OK**.

➤ *To stop all applications running in the application pool:*

1. Go to the **Websites & Domains** tab > **Dedicated IIS Application Pool for Your Websites**.
2. Click **Stop**.

➤ *To start all applications in the application pool:*

1. Go to the **Websites & Domains** tab > **Dedicated IIS Application Pool for Your Websites**.
2. Click **Start**.

If you run applications that are known to have memory leaks or become unstable after working for a long time, then you might need to restart them from time to time.

➤ *To restart all applications running in the application pool:*

1. Go to the **Websites & Domains** tab > **Dedicated IIS Application Pool for Your Websites**.
2. Click **Recycle**.

➤ *To switch off the dedicated IIS application pool for your websites:*

1. Go to the **Websites & Domains** tab > **Dedicated IIS Application Pool for Your Websites**.
2. Click **Switch Off**.

Web Publishing with Web Deploy (Windows)

Web Deploy (Web Deployment Tool) is a Microsoft tool that significantly simplifies the migration, management, and deployment of your websites and web applications. More precisely, you can write a code in your local environment, for example, in *Visual Studio*® (IDE) or *WebMatrix*® (development tool), and then periodically publish the updates to your production server by means of Web Deploy.

Differences Between Visual Studio® and WebMatrix®

If you are looking for an environment that allows you to seamlessly publish code updates to your account, it is likely you will choose between Visual Studio® and WebMatrix®.

- Visual Studio® is a classic integrated development environment (IDE) for writing .NET applications and sites of any scale. It has a variety of plugins that extend its basic functionality. However, to run and debug your applications in Visual Studio®, you should perform extra configuration (such as preparing a database and adjusting environment settings). Thus, this tool is more suitable for advanced users.
- With WebMatrix® you have a built-in set of application templates and even working applications (WordPress, Joomla) right out of the box. If you wish to instantly add an app to your customer account or run it, you just need to select the app from the list and WebMatrix® will transparently configure it for you. Moreover, you can promptly find and subscribe to a hosting plan for your project without leaving WebMatrix®. Summing up, this tool is suitable even for novice users, and encourages fast development by providing ready-to-run applications and templates. The details on how to install and use WebMatrix® are available at <http://www.microsoft.com/web/webmatrix/>.

It is up to you to decide which is better for your project.

How to Configure Web Publishing in Visual Studio® and WebMatrix®

To set up web publishing in your environment, you should open the publishing settings and specify the IP address of your customer account and the username and password you use to log in to the Control Panel.

In WebMatrix®, the publishing settings are found in **Home > Publish**. You can provide these settings either manually or as an XML file that Panel automatically generates. To download the file for a certain website, click on a corresponding **Download** link in **Websites & Domains > <domain_name> > Web Deploy Publishing Settings**. The settings are only available if Web Deploy is installed on the Panel server and is running. If you do not see these settings, contact your hosting provider.

For step-by-step instructions on how to set up web publishing in WebMatrix®, see <http://www.microsoft.com/web/post/how-to-publish-a-web-application-using-webmatrix>.

To learn more about publication settings in Visual Studio®, see <http://msdn.microsoft.com/en-us/library/7z83t16a.aspx>.

Note: You can decide whether to transfer updates securely to your customer account by selecting the corresponding option in the publication settings. If your hosting provider does not have a valid SSL certificate, you will receive an error message on attempting publication. To resolve the problem, contact your hosting provider for assistance or avoid using the secure connection.

Securing WebMatrix® Publishing Settings

An XML file which keeps WebMatrix® publishing settings may include the password to a customer's account. Administrators have the option to configure Panel so that it excludes these passwords from the XML files. If the administrators wish to improve the security of the system and prevent stealing the passwords, they can specify to exclude the password from the XML file. The customers then will have to enter the password directly in WebMatrix®. The option is available on the **Tools & Settings > Server Settings** page.

Creating Sites with Presence Builder

Parallels Presence Builder (also referred to as *editor*) is a visual editor that lets small business owners and individuals create their websites quickly and easily. With Presence Builder, you do not have to write code or configure servers to start a blog, open an online store, or set up any other form of website. You just add the content blocks that comprise your site (text, image gallery, online store) by dragging them to pages, fill these blocks with your content, and publish the result. That's it!

Start Creating a Website

When you start working on your website, you do not have to write text, search for the images, and adjust the site look. Just choose a topic that best suits your website, and Presence Builder will generate a site template that already contains a set of pages, pictures, and text relevant to the selected topic. Each time Presence Builder generates a website, it uses a random set of element designs, so you can be sure that your website design is never repeated.

Once you have selected the topic, you will be prompted to enter some additional information that Presence Builder will add to the website's pages, for example, your phone number, which will appear on the *Contact Us* page.

For more details on how to start creating your website, see the section **Creating a Website** (on page 472).

Import Websites Created in SiteBuilder 4.5

If you already have a website created with SiteBuilder 4.5 and hosted elsewhere, you can import your website to your new customer account. Learn how to move your SiteBuilder 4.5 website to Presence Builder in the section **Importing Sites from SiteBuilder 4.5** (on page 473).

Fill the Site with Content

As soon as Presence Builder creates your website, you can fill it with your content. Your main editing tool is the Presence Builder's main menu. You can do the following by using the menu:

- *Change the structure of your site:* Add or remove pages.
- *Edit the website design:* Change colors and layout.
- *Fill the site with your content:* Remove unused predefined content and add your own elements:
 - Text
 - Images and image galleries
 - Videos
 - Scripts
 - Blogs
 - Search boxes
 - Other elements
- *Let your visitors share the information in your website in social media* such as Facebook or Twitter: Add the corresponding buttons to the pages of your site.

To learn more about actions available to you in the editor, refer to the section **Getting Familiar With the Presence Builder Editor** (on page 470).

Find instructions on managing website look and content in the section **Editing a Website** (on page 474).

Make the Site Available on the Internet

After you finish editing the website, make it available on the Internet. To let people see your site at your domain name, *publish* the website by clicking the corresponding button in the main menu. When you click this link, Presence Builder generates the static pages and scripts that comprise your website and places them in the appropriate locations on the server so that people see them when they enter your domain name in their browsers. Learn more about publishing websites in the section **Publishing a Website to the Internet** (on page 515).

You can also attract more visitors to your sites by placing a site copy on *Facebook* - a popular social network. Refer to the section **Publishing a Website Copy to Facebook** (on page 516) for detailed instructions on how to do this.

Next in this section:

Getting Familiar With Presence Builder	470
Creating a Website	472
Importing Sites from SiteBuilder 4.5	473
Editing Websites.....	474
Saving and Loading Copies of a Website	513
Publishing a Website to the Internet	515

Publishing a Website Copy to Facebook 516
Viewing Site Visits Statistics, Comments, and New Orders on the Dashboard .. 518
Deleting Websites 520

Getting Familiar With Presence Builder

The interface of the Presence Builder editor has two main parts: your website and the main menu.

A website consists of a number of elements, or modules. Each module can be edited separately. Here we will familiarize you with the basic principles of website module editing. These are similar for all modules.

When adding a module to a page, you can choose whether it should be shown only on the current page (page-specific module) or on all pages of the site (site-wide module). The only exceptions are the **Search**, **Advertisement**, **Site Logo**, **Navigation**, and **Breadcrumbs** modules: when you add them, they are placed on all pages of the website.

To place a module only on the current page, select the module under the **Modules** tab, and drag it to any of the areas marked with the text **ONLY ON THIS PAGE**. Such areas are located within the main content block and near the top of each sidebar.

To place a module on all pages of the website, select the module under the **Modules** tab, and drag it to any of the areas marked with the text **ON ALL PAGES**. Such areas are located above and below the main content block, in sidebars, header, and footer.

To locate or edit a website module, hover the mouse pointer over the part of the website you want to change. A dotted frame will appear around the module. A control panel prompting you to move, edit, or remove the module will appear next to the dotted frame.

The dotted frame around page-specific modules is green, but around site-wide modules it is blue.

The editor's main menu offers website editing options grouped under five tabs:

- **Modules.** Here you can choose necessary modules and drag them to any place on the page to fill your website with content.
- **Design.** Here you can select the layout and general color scheme for your website, change colors of different elements, and select fonts and border style.
- **Pages.** Here you can add and delete pages, rename them, edit page meta information such as descriptions and keywords for use by search engines, or mark a page as hidden so that your visitors cannot access it from the site menu.
- **Documents.** Here you can upload documents, images, and other files in various formats to your hosting account. You can then easily insert links to these documents into your website pages. Or, you can just keep the files on the hosting account for your own needs.
- **Settings.** Here you can edit your website name, description and keywords for search engines, upload a site icon (favicon), optimize the ranking of your website in search engine results, connect your site to Google Analytics, and add a copy of your site to a Facebook page.

From the main menu, you can also do the following:

- Access the **Dashboard** to perform the following operations:
 - View statistics on website visits. The statistics are provided by Google Analytics.
 - View new comments left by site visitors on your website pages. The commenting functionality is provided by Disqus.
 - View new orders from customers visiting your online stores. The online store functionality is provided by Ecwid.
- Save and load copies of your website by using the **Save** and **Revert** options.
- Access **Presence Builder Getting Started** video tutorial, view **User's Guide**, or send us your feedback. To do this, select the corresponding option from the **Help** menu.
- Publish your website by using the **Publish** button.
- Discard any changes made to a site and start creating the site anew by selecting **More > Start Over**. This does not delete your already published site copy.
- Delete a current website draft from the editor by selecting **More > Remove Site**. This does not delete your already published site copy.

You can drag the main menu to any place on the page for your convenience, or minimize it.

You can also access all options of the main menu in the context menu at any place on the page. To open the context menu, click the right mouse button.

Creating a Website

To minimize your efforts when creating a website, Presence Builder offers you a set of predefined website topics. When you start creating a website, choose a topic that is most appropriate for you, and Presence Builder will generate a website with the content relevant to this topic. For example, it will include a price list template for a retail store or an image gallery for an artist's site. If you cannot find a suitable topic, you can contact your service provider to ask them to create the corresponding template and add it to the list of available topics.

When you start creating a website, Presence Builder also prompts you to provide information about yourself or your company. Presence Builder will automatically add this information to certain pages as appropriate, for example, to the *About Us* and *Contact Us* pages.

Note: Presence Builder will not store or use the information you provide anywhere except for your website pages. You can change or remove this information later.

➤ ***To start creating a website in Presence Builder:***

1. Go to the **Websites & Domains** tab and click the desired domain name.
2. Click **Launch Presence Builder**.
3. Select a website topic.
4. Type the website name and select website language.
5. Provide the information to pre-fill your website.
6. Click **Create Site**.

Importing Sites from SiteBuilder 4.5

If you have a site created with SiteBuilder 4.5, you can import it to Presence Builder.

Note: The import of sites from earlier versions of SiteBuilder or other content management systems is not supported.

If your site was created with an earlier version of SiteBuilder (4.4 or earlier), and you would like to transfer your site, you can do the following:

- Contact your hosting provider and ask them to upgrade your account to the latest version of Presence Builder.
- Transfer your site manually by copying and pasting the content.

During site import, most parts of the site structure and content can be transferred successfully. However, we cannot guarantee that all content will be transferred.

In most cases, the following elements are imported successfully:

- Site map.
- Static pages, including links and images in text modules. Note that text blocks exceeding 30 kilobytes may be cut; therefore, some parts of the text may be missing.
- Banner (if it is not a custom image).
- Slogan, site title.
- Logo (if it is not a custom image).
- Footer text.
- Meta info (keywords, description).

The other modules can be imported only as text widgets with static content, links and images. Buttons will not work. The image gallery structure can be imported without images.

➤ **To import a site from SiteBuilder 4.5:**

1. Open the Presence Builder editor, and on the topic selection screen, click **Import Site from SiteBuilder 4.5**.
2. Type the Internet address (domain name) of the site that you want to import. For example: `http://example.com`.
3. Select the checkbox to confirm that you are aware of possible import issues, and click **Import Site**.
4. After the site is imported, review and edit it as required (on page 474). You can compare the imported site version with your original site and add the missing information manually.
5. When finished with editing, publish the site to your customer account (on page 515).

If you are publishing your new site to the same webspace on which your site created with SiteBuilder 4.5 was hosted, the old site will be overwritten.

Editing Websites

In Presence Builder, you can change almost any element of your website. Most of the elements are changed in place - you open a page where the element is used, edit it and see the result right away. Site-wide elements, such as **Search** block and **Advertisement** block are changed in one place but the changes are applied to each page of your website.

Note: If you are using Internet Explorer, we strongly recommend that you avoid using browser zoom to change the size of text displayed in your browser window. Please note that websites in Presence Builder will perform and look best at normal zoom (100%).

Next in this section:

Structure: Pages and Navigation	474
Design: Design Templates, Layout, Styles, Color Scheme, and Header.....	477
Content: Text, Tables, Images, Video, Forms, and Scripts	485
Settings and Tools for Webmasters.....	508

Structure: Pages and Navigation

This section describes how to add pages to a site, set their location in the site structure, and add navigation links.

Next in this section:

Adding and Removing Pages	475
Adding and Removing Navigation Links	476

Adding and Removing Pages

Your site can have two levels of nested pages. The total number of pages you can create depends on your hosting plan. The editor will let you know when you have reached the allotted number of pages: an icon with the dollar sign (\$) will be shown over the **Add page** button.

➤ ***To add a new page to your website:***

1. Go to the **Pages** tab.
2. Click **Add page**. The new page appears highlighted in green.
3. Position the new page by dragging it to the right place or by clicking the arrows.
4. Specify the page title.
5. Give a concise description of the page content that will be displayed on search engine results pages and the keywords by which the page will be found by search engines.

Note: **Page name** and **Page link name** are required fields. **Description** and **Keywords** are optional fields. If you specify keywords for a page, they should be separated by commas without white spaces.

6. If you want to make the page invisible to your website visitors, select the **Hidden page** checkbox.
7. If you want to restrict access to the page with password authentication, select the **Protected page** checkbox and specify a username and a password.
8. Click **OK** to save changes.

➤ ***To change the location or properties of a page:***

1. Go to the **Pages** tab.
2. Select the page you want to edit.
3. Change the page position by dragging it to the right place or by clicking the arrows.
4. Edit the page title.
5. Edit or remove the concise description of the page content that will be displayed on search engine results pages and the keywords by which the page will be found by search engines.

Note: **Page name** and **Page link name** are required fields. **Description** and **Keywords** are optional fields. If you specify keywords for a page, they should be separated by commas without white spaces.

6. If you want to make the page invisible to your website visitors, select the **Hidden page** checkbox.

7. If you want to restrict access to the page with password authentication, select the **Protected page** checkbox and specify a username and a password.
8. Click **OK** to save changes.

➤ ***To delete a page from your website:***

1. Go to the **Pages** tab.
2. Select the page you want to delete.
3. Click **Delete page**.
4. Click **OK** to save changes.

Adding and Removing Navigation Links

By default, a horizontal navigation bar with links to site pages is inserted below or above the header of your site. It is automatically updated every time you add, change, move, or remove pages from the site.

If you use sidebars on the site, then the horizontal bar under the header includes only links to the first level pages, and the sidebars show the links of the second and third levels.

You can move navigation blocks by dragging them to other areas of the site.

For each navigation block, you can specify what levels of pages should be included in the menu, change menu alignment (for example, show it in the middle of the page instead of the default alignment to the left), and change the color, style, and size of the font used for the links. To change any of these settings, place the mouse pointer over a navigation block and click **Edit**.

If you occasionally remove a navigation block, you can re-insert it. To do this, go to the **Modules** tab, select **Navigation**, and drag the block to the area on the page where you want to add it. The navigation block will be inserted into all pages of the website.

For the convenience of your site visitors, you might also want to add breadcrumb navigation blocks. Breadcrumb navigation is a chain of links that represents the user's path from the site's main page to a current page. To add a breadcrumb navigation block, go to the **Modules** tab, select **Breadcrumbs**, and drag the module to the area on the page where you want to add it. The navigation block will be inserted into all pages of the website.

Design: Design Templates, Layout, Styles, Color Scheme, and Header

This section describes how to change the layout, color scheme, and header elements of the site.

Next in this section:

Selecting a Website Design Template	478	
Changing Your Website Layout	480	
Selecting Website Colors, Background Images, Fonts, and Styles for Borders and Corners		482
Changing the Website Header Elements	484	

Selecting a Website Design Template

When a new website is generated, the editor applies a random design template to the site. A design template is a combination of website elements (banner, footer, sidebars), page layout settings, and colors.

The editor provides a selection of 24 design templates, 16 of which are randomly generated, and 8, created by graphic designers especially for Presence Builder.

You can review the list of design templates and select the design you like the most, or you can individually adjust the layout and colors of website elements, as described further in this document.

You can also prepare your own design templates and save them to ZIP archives, upload them to the editor, and apply to websites.

Selecting and Applying a Design Template

Note: When you apply a design template, all site-wide elements and modules are overwritten along with the content they might contain.

➤ *To select a design template and apply it to a site:*

Go to the **Design** tab > **Templates**, select the template you want, and click **OK**.

Randomly generated designs are listed in the **Generated** section, and the templates prepared by designers, 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:***

1. Adjust the layout and design, as described in **Changing Your Website Layout** (on page **480**) and **Selecting Website Colors, Fonts, and Styles for Borders and Corners** (on page **482**).
2. Add the necessary site-wide modules and a banner, as described in the chapter **Content: Text, Tables, Images, Video, Forms, and Scripts** (on page **485**), and in the section **Changing the Website Header Elements** (on page **484**).
3. Save the design template: Go to the **Design** tab, and click **Export Design**.

Importing and Applying a Custom Design Template

Note: When you import and apply a design template, all site-wide elements and modules contained on the site are overwritten along with the content they might contain.

➤ ***To upload and apply a design template:***

1. Go to the **Design** tab, and click **Import Design**.
2. Select the ZIP archive containing the design template.

Changing Your Website Layout

The layout of your site can consist of the following elements:

- **Header.** This is the topmost area where a banner image and a company logo are usually placed. You can do the following to the header:
 - Move the banner image and logo from the header area to any place on the page.
 - Reduce the header height to 25 pixels by removing all elements from it.
 - Change the header width from the default size to 100 percent, so that it is expanded to fit the page width.
- **Content area.** This is the main part of a webpage where most of the content is placed. You can do the following to the content area:
 - Adjust the height of the content area.
 - Divide the content area into several columns. You can do this by dragging new modules to the left or right edge of the content area and inserting them.
 - Change location of the columns in the content area by moving the content to the left or to the right.
- **Sidebars.** These are vertical columns that can be used for placing all kinds of modules, site-wide and page-specific. You can do the following to sidebars:
 - Add one sidebar and place it to the left or to the right of the content area.
 - Add two sidebars. They will be placed to the left and to the right of the content area.
 - Adjust the height and width of the sidebars.
 - Move the sidebars to the top of the page and place them to the left or to the right of the header area.
 - Switch places of the sidebars.
- **Footer.** This is the lowest area where the company name, contact information, or a copyright notice are usually placed. You can do the following to the footer:
 - Reduce the footer height to 25 pixels by removing all elements from it.
 - Change the footer width from the default size to 100 percent, so that it is expanded to fit the page width.
- **Advertisement block below the footer.** Depending on your hosting plan, an additional text block containing some advertisement from your hosting provider might appear below the website footer. If that advertisement block appears on your site, you might want to upgrade to another hosting plan to remove it.

➤ ***To change the layout of your site:***

1. Go to the **Design** tab > **Layout** tab.
2. Select the number of sidebars: Under **Sidebars**, select **No**, **One**, or **Two**.
3. Select the locations of sidebars:
 - To move a sidebar to another side of your website, or to switch places of sidebars (if you have two sidebars on your site), click **Switch sidebars**.
 - To move the sidebars to the top of the page, click them in the layout model.
4. Set the size of page elements:
 - To set the total width of the website pages, under **Website width**, select either of the following:
 - **Fixed layout**: your website will be of a specific size regardless of the size of the browser window viewing the page. In this case, specify your website width in pixels.
 - **Liquid layout**: based on percentages of the current browser window's size. In this case, specify your website width as a percentage of the browser window's size.
 - To change the width of the header, footer, and the main content area to fit the page width, click the corresponding elements in the layout model.
 - Under **Minimal column height in pixels**, specify the height of the main content area and each sidebar, if you have chosen to use them.

This value shows the height of your website elements without content. When you add content to the main content area and to the sidebars, they will stretch in height to fit the content.
 - To ensure that the sidebars and the content area are vertically aligned, select the checkbox **Stretch the sidebars and the content area down to the footer**.
 - If you use one or two sidebars, under **Sidebar width in pixels**, specify the width of each sidebar. The size of the main content area will be determined automatically.
 - Under **Margin sizes in pixels**, specify the size of vertical and horizontal margins. A margin is the space between the edges of neighboring elements.
5. Click **OK** to save changes.

Selecting Website Colors, Background Images, Fonts, and Styles for Borders and Corners

The general color scheme, or styleset, of your website comprises four colors. Each color is used for several website elements at once. You can adjust colors of individual elements on the **Design** tab > **Colors** tab.

➤ **To select the general color scheme for your website:**

1. Go to the **Design** tab > **Scheme** tab.
2. Select the color scheme, or styleset, of your website in the menu.
You will see the four colors used in the color scheme of your website.
3. To adjust one of the colors of your website color scheme, click the respective color field and change the hexadecimal color code value or select a color with the color picker.

Note: These changes will override any previous changes of individual elements' colors made on the **Colors** tab.

4. Click **OK** to save changes.

➤ **To set colors or background images for individual website elements:**

1. Go to the **Design** tab > **Colors** tab.
2. Select the website element in the **Page area** menu.
3. Click the arrow in the **Color or image** menu.
4. Do any of the following:
 - To fill with a solid color, leave the **Solid color** option selected, and select a color with the color picker.
 - To fill with a gradient, select the **Gradient** option, and then select a pattern from the library.
 - To fill with a background image, select the **Image** option, select a pattern from the library or click **Upload** to upload your own image. Specify where it should be placed and whether it should be tiled.
5. For an element with text, adjust font colors by clicking the respective color field and editing the hexadecimal color code value or by selecting a color with the color picker.

Note: Modifying the styleset on the **Scheme** tab will override the changes made on the **Color** tab.

6. Click **OK** to save changes.

➤ **To select fonts for headings and body text of your website:**

1. Go to the **Design** tab > **Fonts** tab.
2. For each font type, select the font face and size in the menus.
3. For headings, select the font decoration. You can use bold (the **B** icon) and italics (the *I* icon).

Note: The settings made here define only general rules for your website fonts. You can always adjust fonts of individual elements in place.

4. Click **OK** to save changes.

➤ **To select the shape of corners (square or rounded) for website elements:**

1. Go to the **Design** tab > **Corners** tab.
2. In the **Page area** menu, select the element whose corners you want to change.
3. Do any of the following:
 - To make rounded corners, select the corresponding checkboxes.
 - To make square corners, clear the corresponding checkboxes.
4. Click **OK** to save changes.

➤ **To select borders for website elements:**

1. Go to the **Design** tab > **Borders** tab.
2. Select the border type for elements inside your website from the **Internal containers border** menu.
3. Select the elements that will have the border.

Note: You can select only one internal border type for all elements on your website, but you can select whether this border will be used for certain elements.

4. Select the external border for your website from the **External site border** menu.
5. Click **OK** to save changes.

Changing the Website Header Elements

The site header consists of the following elements:

- **Banner.** You can do the following to the banner:
 - Upload your own banner image or a Flash file in SWF format.
 - Select and apply a banner from the Presence Builder library.
 - Remove the banner and use a background filled with a color or images.
 - Remove the banner and all other elements from the header area to reduce its height to 25 pixels.
 - Move the banner to the content area and insert it into a specific page or into all pages of the website.

Note: You can use only one banner per site. If you choose to insert it into a specific page, you will not be able to add it to other pages of the website. For this reason, we recommend that you place it into the site-wide areas.

- **Logo image.** You can do the following to the logo:
 - Upload your own logo image or a Flash file in SWF format.
 - Move the logo from the header area to other parts of webpages, such as sidebars and content area.
 - Insert any number of logo images into the site-wide areas.
 - Resize the logo by specifying the desired dimensions in pixels, or by dragging the sides and corners of the image with a mouse pointer.
 - Remove the logo.
- **Site name.** This usually contains a company name or a brief site description like, for example, "John Doe's Recipes".
- **Site slogan.** This usually includes a description of your site or a company slogan.

➤ ***To change the banner image or other elements of the header (logo, site name, or slogan):***

1. Click the banner image.
2. Select the option **Use an image**, and then click the image in the **Image list** menu.
3. Do any of the following:
 - To use an image from the library, select it. To find relevant images, type a keyword into the input box.
 - To use your own image or a Flash file in the SWF format, click **Upload**, and select the file that you want to use. Images should be in the GIF, JPEG, and PNG formats, preferably not wider than 900 pixels.
4. If you want to scale a banner to fit the header area, select the **Fit image size** checkbox.
5. Under **Show banner elements**, select the checkboxes corresponding to the elements that you want to show in the header.

6. If you want to remove a logo image or upload your own logo, click the logo image.
7. If you want to change the site name or slogan, click the corresponding fields on the header and change them as you want.

To make it easier to see the site name or slogan, select the **Outline** checkbox. This adds a black or white outline around text, one pixel in width. If the font color in site title or slogan is black, then the outline is white, and vice versa.

Note that you can freely move the blocks with website name, description, and logo within the header area.

If you occasionally remove the banner, you can re-insert it.

➤ **To remove the banner:**

Click the banner, select the option **Do not use an image**, and specify the height of the header block in pixels. Click **OK**.

➤ **To insert a banner:**

Go to the **Modules** tab, select **Banner**, and drag the module to any of the site-wide areas on the page where you want to add it.

➤ **To insert a logo:**

Go to the **Modules** tab, select **Site Logo**, and drag the module to any of the site-wide areas on the page where you want to add it. You can upload a new logo image or a Flash file in the SWF format, and align it to the left, center, or right.

You can also resize the logo image by specifying the desired dimensions in pixels, or by dragging the sides and corners of the image with a mouse pointer.

Note: When you resize the image with a mouse pointer, the option to **keep the original aspect ratio** is switched off automatically.

Content: Text, Tables, Images, Video, Forms, and Scripts

This section describes how to fill your site with content and enhance it with useful functions provided by the editor's modules.

When adding a module to a page, you can choose whether it should be shown only on the current page (page-specific module) or on all pages of the site (site-wide module). The only exceptions are the **Search**, **Advertisement**, **Site Logo**, **Navigation**, and **Breadcrumbs** modules: when you add them, they are placed on all pages of the website.

- To place a module only on the current page, select the module under the **Modules** tab, and drag it to any of the areas marked with the text **ONLY ON THIS PAGE**. Such areas are located within the main content block and near the top of each sidebar.

To divide the content area into columns and insert a module into one of them, drag the module to the left or right edge of the content area and then insert it. Note that sidebar areas cannot be divided into columns.

- To place a module on all pages of the website, select the module under the **Modules** tab, and drag it to any of the areas marked with the text **ON ALL PAGES**. Such areas are located above and below the main content block, in sidebars, header, and footer.

The number of modules that you can add to a website depends on your hosting plan. The editor will let you know when you have used the allotted number of modules: icons with the dollar sign (\$) will be shown over the module icons in the editor's toolbar.

Next in this section:

Text, Tables, Hyperlinks, Flash Files, and Images.....	487
Image Gallery.....	492
Image Slider.....	494
Embedded Video.....	496
Contact Form.....	496
Blog.....	497
Commenting.....	500
Documents and Other Downloadable Files.....	502
Buttons for Sharing on Social Networks.....	503
Site Search.....	503
Online Store.....	504
Map.....	505
Custom Scripts.....	507
Advertisements.....	507

Text, Tables, Hyperlinks, Flash Files, and Images

Before you start working on website content, we suggest that you select the appropriate website language in **Settings** tab > **Languages** > **Website language** menu.

The website language is a site-wide setting that defines the language in which you will be adding content to your website. It affects the following:

- The language in which certain website elements (in particular those provided by third-party services), such as Google Search and navigation buttons in image galleries, will be shown. Note that not all third-party services and modules provided by the editor support all available languages.
- The direction in which you will type text in the editor (from left to right or from right to left). If you select a right-to-left language, your website content and design will be RTL-enabled.

Note: Changing a website language does not reload the currently selected website topic in a different language. The topic language will remain unchanged, however, the text orientation will change.

➤ *To add text, lists, tables, or images to a page:*

1. Go to the **Modules** tab, select **Text & Images**, and drag the module to the page:

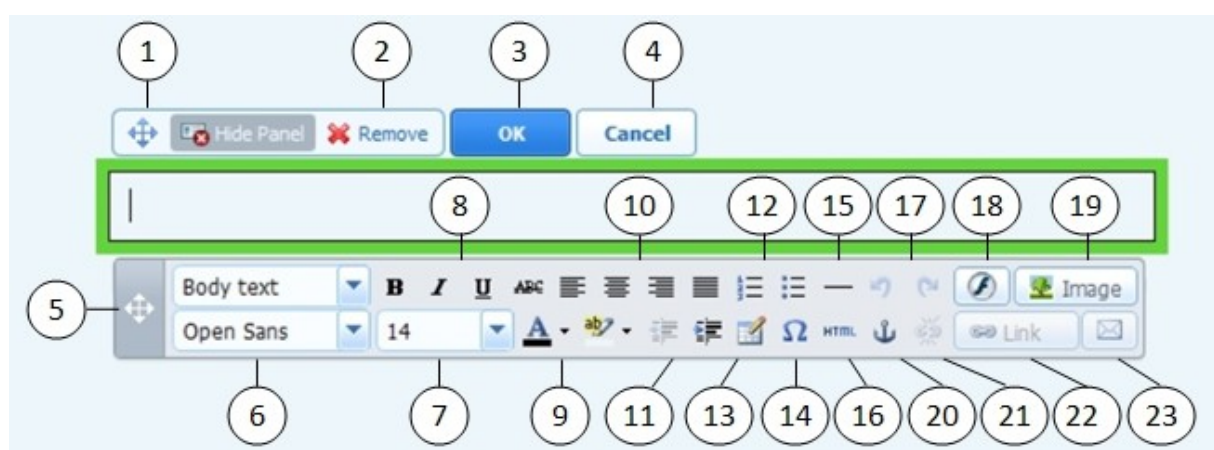
- To add a block with text and images to the current page, drag the module to any of the areas marked with the text **ONLY ON THIS PAGE**. Such areas are located within the main content block and near the top of each sidebar.

To divide the content area into columns and insert a block into one of them, drag the module to the left or right edge of the content area and then insert it. Note that sidebar areas cannot be divided into columns.

- To add a block with text and images to all pages of the site, drag the module to any of the areas marked with the text **ON ALL PAGES**. Such areas are located above and below the main content block, in sidebars, header, and footer.

2. Type the text on the screen and use the icons on the module's toolbar to format the text, add tables, hyperlinks, and images.

The toolbar of the **Text & Images** module provides access to the following tools and functions.



1. Move the text and image block within the webpage.
2. Remove the block with its contents.
3. Save changes.
4. Cancel the changes made.
5. Move the toolbar.
6. Select the paragraph style and font face. Note that the Terminal font is not supported by Google Chrome.
7. Select the font size.
8. Select the font style: bold, italics, underlined, and strikethrough.
9. Select the text and background colors.
10. Select text alignment: left, center, right, or justified (aligned to both the left and right margins with added extra spaces between words).
11. Increase and decrease the indent level of the paragraph.
12. Start a numbered or bulleted list.
13. Insert a table and specify the number of rows and columns.

After you insert a table, a number of additional icons become accessible from the toolbar. Use them to change the properties of the table rows and cells, to insert and remove rows and columns, or to split and merge table cells.
14. Insert symbols that are not on your keyboard, such as copyright and trade mark signs, and other Unicode symbols.
15. Insert a horizontal line.
16. Edit the HTML source code of the page.
17. Undo and redo changes.
18. Insert a Flash object in the SWF format.
19. Insert an image, adjust its size, specify a description, and text wrapping.

You can choose to show the description below the image, show it over the image only when users hover the mouse pointer over it, or to not show it. The description also serves as alternative text: In browsers that do not support or are configured to not show images, the description will be shown instead.

If you want to insert many pictures into a single page, consider using the **Image Gallery** module instead of the **Text & Images** module. With **Image Gallery**, you can upload pictures from your local computer or use pictures published to the Picasa Web Albums photo sharing service. To learn more about the **Image Gallery** module, see the section **Image Gallery** (on page 492).

If you want to add a slide show with multiple images, use the **Image Slider** module. To learn more about the **Image Slider** module, see the section **Image Slider** (on page 494).
20. Insert HTML anchors into particular sections of webpages so that you can link to them from the same or other pages of your site.
21. Remove hyperlinks from selected text.

22. Add hyperlinks to pages of your website or external resources.

23. Add a link to an e-mail address.

To learn more about adding hyperlinks, see the section **Hyperlinks, Links to E-mail Addresses, and Anchors** (on page 490).


Next in this section:

Hyperlinks, Links to E-mail Addresses, and Anchors 490

Hyperlinks, Links to E-mail Addresses, and Anchors

Creating Links to Other Pages


➤ **To insert a hyperlink into text:**

1. Select the text that you want to make a link.
2. On the toolbar of the **Text & Images** module, click the icon  .
3. Do any of the following:
 - To add a link to another webpage on your site, select the option **A page of this site**. In the **Select page** menu, select the target webpage or a webpage section where you have placed an anchor.
 - To add a link to a webpage or a file located on another site, select the option **A webpage or file on the Internet**, and type the address. For example, `http://example.com`.
 - To add a link to a document or another downloadable file that you have previously uploaded through the Document Manager (as described in Documents and Other Downloadable Files (on page 502)), select the option **A document on this site**, and select the target file.
4. In the **Open link in** menu, select where you want to open the target page. You can choose to open it in the same or in a new browser window or tab.
5. In the **Title** box, type the description that should appear when users place the mouse pointer over the link.
6. Click **OK**.


Creating Links to Different Sections of a Webpage

If you have a lengthy webpage consisting of several sections, consider inserting a table of contents with links to these sections in the top of the page, to help your site visitors navigate through the page content. You can do this with the help of so-called anchors.

➤ **To add links to different sections within a webpage:**


1. Insert an anchor in the beginning of each section.
 - a. In the text block, highlight with the mouse pointer a section heading or, if there is no heading, a first letter at the beginning of a paragraph.
 - b. On the **Text & Images** module's toolbar, click the icon .
 - c. Specify a name for the anchor and click **OK**.

Anchor names should begin with a Latin alphabet letter. They can contain Latin alphabet letters, underscore, and numbers. For example: `section_1`.


- d. Repeat these steps to add as many anchors as needed.
2. Insert a table of contents or a list of sections in the top of the page.
3. Add hyperlinks to the table of contents or the list of sections.
 - a. Highlight with the mouse pointer a section name.
 - b. On the **Text & Images** module's toolbar, click the icon .
 - c. Leave the option **Link to a page of this site** selected.
 - d. In the **Select page** menu, select the required anchor name.
 - e. Click **OK**.
 - f. Repeat these steps to add hyperlinks to all the sections you need.

Creating Links to E-mail Addresses

➤ *To insert a link to an e-mail address into text:*

1. Select the text that you want to make a link.
2. On the toolbar of the **Text & Images** module, click the icon .
3. Specify the e-mail address and click **OK**.

If you want to specify multiple e-mail recipients or predefine the message subject, use the following alternative method:

1. Select the text that you want to make a link.
2. On the toolbar of the **Text & Images** module, click the icon .
3. Select the option **A webpage or file on the Internet**, and type [mailto:<address>](mailto:postmaster@example.com). For example, `mailto:postmaster@example.com`.

You can also:

- Specify multiple recipients in the To field, separating addresses with a comma (,) or a semicolon (;). For example:
`mailto:postmaster@example.com,mail@example.com`.

Note: It is better to separate addresses with a semicolon because users of Microsoft Office Outlook might experience issues with sending e-mail to recipient addresses separated with commas. Microsoft Office Outlook 2003 and later versions do not recognize a comma as an e-mail address separator, unless they are specifically configured to do so. For details, see the article at <http://support.microsoft.com/kb/820868>.

- Predefine the message subject line. For example:
`mailto:postmaster@example.com?subject=My%20Subject`.

- Add recipients to CC and BCC lists. For example:
`mailto:postmaster@example.com?subject=My%20Subject&cc=address1@example.com&bcc=address2@example.com.`
- Predefine text to put in the message body. For example:
`mailto:postmaster@example.com?subject=My%20Subject&body=This%20is%20sent%20from%20your%20site!`

Note: You should replace white spaces with %20.

4. Click **OK**.

Image Gallery

➤ *To add an image gallery to your site and upload pictures:*

1. Go to the **Modules** tab, select **Image Gallery**, and drag the module to the page.
2. In module settings, on the **Image Storage** tab, select where you want to keep pictures:
 - If you do not have a Picasa Web Albums account that you would like to use, leave the **Presence Builder** option selected. All images you use on your site will be kept on your customer account.
 - If you have an account in Picasa Web Albums and want to use pictures that you store there on your site, do the following:
 - a. Select the **Picasa** option, click the link on the **Image Storage** tab to sign in to Google, and grant access to your albums from Presence Builder.
 - b. Select the album whose pictures you want to use or click **Create Album** to create a new album.
 - c. If you want Presence Builder to remove images from Picasa Web Albums when you remove them from the gallery, select the checkbox **Delete images when I remove them from gallery**.

When you upload images to an image gallery through the Presence Builder editor, they are automatically copied to your Picasa Web Albums account. When you remove images from the gallery, they are removed from Picasa Web Albums only if you have selected the option **Delete images when I remove them from gallery**.

3. (Optional steps.) If you want to select the size of image thumbnails to be shown in the image gallery, change the gallery alignment (place it to the left, in the center, or to the right), or adjust the number of images to be displayed per page, click the **Gallery Properties** tab and make the desired changes.

The following thumbnail sizes are available:

- Small (95 x 75 pixels).
- Normal (140 x 130 pixels). This is the default setting.

- Large (170 x 170 pixels).
4. To add images to the gallery, on the **Image Storage** tab, click the text **Click here to upload your images**, select the images that you want to upload, and click **OK**.
You can select and upload multiple images at once. Only images in GIF, JPEG, and PNG formats are supported.
We recommend that you use resized images that do not exceed 1024 x 768 pixels.
 5. To change image title and description, click the corresponding thumbnail, click the title or description, and edit the text.
If you delete the default text entirely, it will not be shown on your published site; however, it will still be shown when you edit the site in the Presence Builder editor.
 6. To rearrange images in the gallery, drag them to the desired location.

➤ ***To remove an image from the gallery:***

Place the mouse pointer over the image thumbnail and click the icon [x].

➤ ***To remove an image gallery with all pictures:***

Place the mouse pointer over the image gallery block and click **Remove**.

Image Slider

The Image Slider module enables you to add a slide show with multiple images and various transition effects. The following image formats are supported: GIF, JPEG, and PNG.

Images are not resized automatically; for this reason, we recommend that you upload images of the same dimensions. Otherwise, the slide show will not look good.

When adding images, you can add descriptions to them and link the images to specific pages of your website.

The following transition effects are supported:

- Random
- Slice down and to the right
- Slice down and to the left
- Slice up and to the right
- Slice up and to the left
- Slice up and down
- Slice up and down and to the left
- Fold
- Fade
- Box random
- Box rain
- Reverse box rain
- Growing box rain
- Reverse growing box rain

The effect names might tell you little about how the effects look, so it is better to see them in action. To do this, add the Image Slider module, upload at least two images, go to the module settings (**Settings** tab), and select an effect from the **Transition effect** menu.

➤ ***To add Image Slider to your site and upload pictures:***

1. Go to the **Modules** tab, select **Image Slider**, and drag the module to the page.
2. Click **Add Images**, select the images that you want to upload, and click **OK**.

You can select and upload multiple images at once. We recommend that you use resized images that do not exceed 1024 x 768 pixels.


Once you have uploaded images, you can arrange them in the desired order, and remove them. To do any of these actions, place the mouse pointer over an image thumbnail, and

use the corresponding icons:   .

3. To add an image description, select a thumbnail, and type the text into the **Description** box.
4. To add a link to a webpage, select a thumbnail, select the option **Link to a webpage**, and select the page from the menu below.

5. Click the **Settings** tab and select the desired transition effect from the **Transition effect** menu.
6. Specify how long each image must be shown.
7. Specify whether the round navigation icons for switching between slides must be shown.
The option **Inside** will show the icons over the images, in the upper right corner of Image Slider, and **Below** will show the icons below the images.
8. Specify whether the navigation arrows for switching between slides must be shown.
9. Click **OK**.

➤ ***To remove an image from the slide show:***

Click on the slide show block, place the mouse pointer over the image thumbnail, and click the icon .

➤ ***To remove a slide show with all pictures:***

Place the mouse pointer over the slide show block and click **Remove**.

Embedded Video

You can embed into website pages video clips located on popular video sharing sites, such as YouTube (youtube.com), Vimeo (vimeo.com), MySpace (myspace.com), and Dailymotion (dailymotion.com).

➤ *To insert a video into a webpage:*

1. Go to the **Modules** tab, select **Embedded Video**, and drag the module to the page.
2. Insert a link to the video or select the option **Embed code** if you have obtained a code from a file sharing site, and then paste the code.
3. Click **OK**.

➤ *To remove a video:*

Place the mouse pointer over the video and click **Remove**.

Contact Form

If you want your site visitors to be able to send you messages from your site, you can add a contact form.

➤ *To add a contact form:*

1. Go to the **Modules** tab, select **Contact Form**, and drag the module to the page.
2. On the **Settings** tab, specify the following:
 - Recipient's e-mail address. You can specify several e-mail addresses separating them with commas (,) or semicolons (;).
 - Message subject.
 - Text to be shown on the button that sends the message.
 - Protection from automated spam postings. Leave the checkbox **Enable the protection from automated spam postings** selected if you want to avoid receiving spam sent by scripts or spam bots through the contact form.

The protection is based on a highly efficient mechanism, called reCAPTCHA. In the contact form, it is shown as an input box accompanied by a combination of distorted words or symbols that can be recognized only by humans. Before a message can be sent through the contact form, a user is prompted to recognize the symbols and type them in.

3. If you want to add, move, or remove input fields from the form, or change their labels, click the **Fields** tab, and make the required changes.

4. If you want to change the default message "Your message was sent. Thank you." which is shown when a message is sent, click the **Reply** tab and type the new text.
5. Click **OK**.

➤ **To remove a contact form:**

Place the mouse pointer over the form and click **Remove**.

Blog

If you want to maintain an online diary on your site, or regularly publish articles on a subject and automatically present them in a chronological order, then you need a blog.

A blog module can be added only to the first-level pages that do not have subpages. Within blog posts, you can use text, images, embedded videos and scripts. Each blog post can have its distinctive page description and meta information to be used by search engines. Note that blog posts are not listed on the Pages tab (on page 475).

To let your visitors comment on your blog posts, you need to register with Disqus, a free third-party service that provides commenting functions for your sites and keeps all comments.

➤ **To add a blog to your webpage:**

1. Go to the **Modules** tab, select **Blog**, and drag the module to the page.
2. In the module properties, specify the following:
 - Number of blog posts to show on the page.
 - Specify whether the site visitors will be able to leave their comments.
3. Click **OK**.
4. To enable commenting, click the link **Click here to add a new blog post**.
5. Click within the gray information box at the bottom of the blank blog post.
6. To register with Disqus, click the **Register** button. A registration form will open in a new browser window or tab.
7. Specify the following:
 - Your site's URL, desired name and shortname (unique ID). You will need to specify this site ID (shortname) later in the Blog module settings to enable commenting.
 - Comment moderator's username, password, and e-mail address. A confirmation message will be sent to this e-mail address, so be sure that it is valid.
8. Click **Continue**.
9. Specify your language and other settings, and click **Continue**.
10. On the last step of the registration form, no further action is required. Just log out of the Disqus site.

11. Check your e-mail inbox for the confirmation message from Disqus. In this message, click the link to verify your address.
12. Return to the browser window where you have the Presence Builder editor with the Blog module properties opened.
13. In the box titled **Apply here the website ID (shortname) received during registration**, type or paste the site ID that you specified during registration with Disqus in step 7.
14. Click **Apply**.
15. Click **OK**.

Now your blog can accept comments from visitors, and you can make the first post.

➤ ***To add a blog post:***

1. Go to the website page containing a blog module.
2. Click the link **Click here to add a new blog post** (might also appear as **New Post Title**).
3. Type the post title and content.

If you want to change the date of posting, click within the field **Posted dd.mm.yy** and then select a date from the calendar.

If your post is lengthy and contains numerous text blocks, images, and embedded videos, you might want to show only a portion (beginning of the post) to site visitors in your blog's main page. To do this, while editing a blog post, move the divider element (containing the line ----- **Drag this above modules that should not appear in the list of posts** -----) to the desired area.

4. Click **OK**.
5. If you want to view, edit, or remove a concise description of the page that will be displayed on search engines results pages and the keywords by which the page will be found by search engines, click in a blank area to the right of the post title, and then click the **SEO Settings** tab.

Note: **Post link name** is a required field. **Meta description** and **Meta keywords** are optional fields. If you specify keywords for a page, they should be separated by commas without white spaces.

6. To return to the blog's main page, click the **Back** link below the post you have just created.

➤ ***To remove a blog post:***

1. Go to the website page containing a blog module.
2. Place the mouse pointer over the post title and click **Remove**.
3. Click **Yes** to confirm removal.

➤ ***To edit a blog post:***

1. Go to the website page containing a blog module.
2. Click the post title.
3. Make the required changes and click **OK**.

➤ ***To remove a blog with all posted content:***

1. Go to the website page containing a blog module.
2. Place the mouse pointer over the link **Click here to add a new blog post** and click **Remove**.
3. Click **Yes** to confirm removal.

Commenting

If you want to let your site visitors leave comments on webpages, you need to insert the Commenting module into those webpages.

The commenting functionality is powered by Disqus, a third-party service that stores and processes all comments. Before your visitors can leave comments, you need to register an account with Disqus and then specify a site ID in the Commenting module settings.

You can insert several Commenting modules into a single website. Because all Commenting modules on the site will use the same site ID, you will only need to specify the site ID once in the module settings, when inserting the first Commenting module.

➤ *To add commenting functions to a webpage:*

1. Go to the **Modules** tab, select **Commenting**, and drag the module to the page.
2. If you have not registered an account with Disqus yet, click the **Register** button. A registration form will open in a new browser window or tab.
3. Specify the following:
 - Your site's URL, desired name and shortname (unique ID). You will need to specify this site ID (shortname) later in the Commenting module settings to enable commenting.
 - Comment moderator's username, password, and e-mail address. A confirmation message will be sent to this e-mail address, so be sure that it is valid.
4. Click **Continue**.
5. Specify your language and other settings, and click **Continue**.
6. On the last step of the registration form, no further action is required. Just log out of the Disqus site.
7. Check your e-mail inbox for the confirmation message from Disqus. In this message, click the link to verify your address.
8. Return to the browser window where you have the Presence Builder editor with the Commenting module properties opened.
9. In the box titled **Apply here the website ID (shortname) received during registration**, type or paste the site ID that you specified during registration with Disqus in step 3.
10. Click **Apply**.
11. Click **OK**.

Now you can publish your website to the customer account and start receiving comments from your visitors.

In addition to adding and viewing comments, you can do the following:

- Edit comments.
- Delete comments.
- Mark comments as spam.
- Ban users (by e-mail or IP address) from posting comments on your site.
- Change the settings, such as appearance of comments, and remove the [trackback URL](#). You can do this by logging in to your account at www.disqus.com, and going to the **Settings** tab.

➤ ***To moderate comments:***

1. Log in to Disqus as the site administrator. You can do this in either of the following ways:
 - Visit the Disqus site at www.disqus.com and log in there.
 - In the Presence Builder editor, go to the page where you have the Commenting module and click inside the **Add New Comment** field. Click the **Post as** button, click the **Disqus** link in the left navigation pane, type your username and password, and click **Login**.
2. After you are logged in to Disqus, you can moderate comments in either of the following ways:
 - On the Disqus site, use the items in the **Dashboard** and **Admin** areas.
 - In the Presence Builder editor or on the published site, go to the page where you have the Commenting module, place the mouse pointer over the comment you want to moderate, and use the **Moderate** link that will appear next to the comment.

Alternately, you can moderate comments by using links in the notification messages that Disqus sends you when someone leaves a comment on your site.

➤ ***To remove commenting functions from a webpage:***

1. In the Presence Builder editor, go to the website page containing the Commenting module.
2. Place the mouse pointer over the **Add New Comment** field and click **Remove**.
3. Click **Yes** to confirm removal.

Documents and Other Downloadable Files


The editor now provides a convenient control panel for working with files in your customer account. You can upload your documents, images, and other files in various formats to the editor (on the **Documents** tab), and then insert links to them in your website pages. Alternatively, you can just keep them in your customer account for your own needs.

➤ ***To upload a file to the customer account:***

1. Go to the **Documents** tab.
2. Click **Upload**.
3. Select the file and click **Open**.

Now, to let your site visitors download this file, you can insert a link to it in a webpage.

➤ ***To insert a link to file:***

1. Select the text that you want to make into a link.
2. On the **Text & Images** module's toolbar, click the icon  .
3. Select the option **A document on this site**.
4. Select your file and click **OK**.

➤ ***To remove a file from the customer account:***

1. Go to the **Documents** tab.
2. Select the file and click **Remove**.
3. Confirm removal and click **OK**.

Buttons for Sharing on Social Networks

If you want to let your visitors easily share your content on social networks or online bookmarking services, you can insert a toolbar with buttons for sharing on Facebook, Twitter, Myspace, and other popular services.

➤ *To add the Share on Social Media toolbar to a webpage:*

1. Go to the **Modules** tab, select **Social Sharing**, and drag the module to the page.
2. Select the appearance of the toolbar.
3. If you want to modify the list of social networks and sharing services shown on the toolbar, place the mouse pointer over the icon **[+]** and click the **Settings** link.

The changes you make to the list of services will be visible after you publish the site.

4. Click **OK**.

Note: When someone shares your content on Twitter by using the Tweet button, the counter of tweets is not increased immediately. It can take several hours for the counter to update.

➤ *To remove the Social Media toolbar:*

Place the mouse pointer over the toolbar and click **Remove**.

Site Search

If you want to let your visitors search for information on your website, you can add a search bar to the site. After inserting the search bar into a webpage, it is automatically added to all pages of the site.

By default, the search bar is configured to use the Google search engine. If you want to use another search engine, you can obtain the search script code and insert it into the **Search** module.

➤ *To add a search bar to the site:*

1. Go to the **Modules** tab, select **Search**, and drag the module to the page.
2. Do any of the following:
 - If you want to use the search service provided by Google, leave the **Google** option selected.
 - If you want to use another search engine, select **Other** and paste the code that you have obtained from that service.

Make sure that the code you insert is correct, as Presence Builder does not validate it.
3. Click **OK**.

The search bar will appear on your site after publishing.

➤ **To remove a search bar:**

Place the mouse pointer over the search bar and click **Remove**.

Online Store

If you want to sell products or services through your site, you can use the **Online Store** and **Shopping Cart** modules to add a fully functional online store to the site. You can add only one store per site.

The store functionality is provided by Ecwid - a third-party SaaS solutions provider that securely stores and processes all your data, including product catalogs, images, orders, and customers' payments.

➤ **To add an online store to your site:**

1. Go to the **Modules** tab, select **Online Store**, and drag the module to the page.
2. Create an account with Ecwid if you do not have one yet, or specify the ID of an existing store if you have previously created a store at Ecwid through Presence Builder and want to show it on your site.

If you do not have an account with Ecwid yet, do the following:

- a. In module settings, on the **General** tab, select the option **Register with Ecwid**.
- b. Type your name, e-mail address, and password. You will use the e-mail address and password to sign in to Ecwid and manage your store.
- c. Click **Send**. A confirmation message from Ecwid will be sent to your e-mail address. You will need to confirm that you own this e-mail address within three days, otherwise the online store will be deactivated.

If you already have an account with Ecwid, select the option **Enter an ID of an existing shop**, specify the store ID and e-mail address that you specified during account registration, and click **Apply**.

Note: If the online store was created directly at the Ecwid website without using Presence Builder, you can do the following: Create a new Ecwid account through Presence Builder, log in to the previously existing Ecwid account, export all the goods to a CSV file. After that, log in to the new account and import the file.

3. (Optional step.) If you want to let your customers add items to the cart by dragging them to a shopping bag icon, go to the **Modules** tab, select the **Shopping Cart** module, and drag it to the page.

Note that the shopping bag icon will be inserted into all pages of your site. If you do not want that, do not use the **Shopping Cart** module. Your customers will still be able to add items to the cart and proceed to checkout by using the **Shopping Bag** link that appears at the top of the product catalog area.

4. (Optional step.) If you want to change the appearance of the product catalog, in module settings, go to the **View** tab.
5. To set up your store, fill the product catalog with items, and remove the default fruit and vegetable items added by Ecwid, click the **Manage** link on the module's toolbar.

The Ecwid control panel will open in a new browser window or tab.

6. After you have finished setting up the store in the Ecwid control panel, return to the Presence Builder editor and click the **Reload** link on the **Online Store** module's toolbar.

You must use the **Reload** link to synchronize the content of your online store with online store at Ecwid.

7. Click **OK** to finish setting up the store.

➤ **To manage a store:**

Place the mouse pointer over the product catalog and click **Manage**. The Ecwid control panel will open in a new browser window or tab.

Note: After publishing your site, you can also view information about new orders on the Dashboard (on page 518).

➤ **To remove a store:**

Place the mouse pointer over the product catalog and click **Remove**.

Map

With the Map module, you can easily add a map with your location to a website. Maps are provided by the Google Maps service, which is available free of charge.

The following functions are supported:

- Searching for an object on a map by address or by latitude and longitude coordinates.
- Selecting the mode of map display by switching between **Map**, **Satellite**, **Satellite with labels**, and **Terrain** views.
- Adjustment of the map scale: zoom in or out on **House**, **Street**, or **Town**.

When you add a map, the module uses the information about your location that you specified after selecting a website topic. You can specify a new location at any time.

➤ **To add a map to your site:**

1. Go to the **Modules** tab, select **Map**, and drag the module to the page.
2. Specify the desired location and click **Search**. You can type an address or coordinates. For example: `37.754481, -122.383772`.

3. Select the desired map view from the **Map mode** menu, and the zoom level from the **Zoom level** menu. To show your organization's location on the map, you might want to choose the **Map** option and the **Street** zoom level.
4. Select the desired map size from the **Map size** menu.
5. Click **OK**.

➤ ***To remove a map:***

Place the mouse pointer over the map and click **Remove**.

Custom Scripts

You can insert custom scripts written in PHP, JavaScript, or VBScript in any page of your website.

➤ ***To insert a script in a webpage:***

1. Go to the **Modules** tab, select **Script**, and drag the module to the page.
2. Paste the code into the input field.

For PHP, use the opening tag `<?php`. Make sure the code you insert into this field is correct, as Presence Builder does not validate it.

3. Click **OK**.

Your code will be active only on the published website.

➤ ***To remove a script:***

Place the mouse pointer over the script block and click **Remove**.

Advertisements

If you are participating in a banner exchange or other online advertising programs, you might want to add an advertisement block to your site. After inserting the block in a webpage, it will be automatically added to all pages of your site.

➤ ***To add an advertisement block:***

1. Go to the **Modules** tab, select **Advertisement**, and drag the module to the page.
2. Paste the code provided by your advertising vendor into the input field.

Make sure that the code you insert into this field is correct, as Presence Builder does not validate it. With some advertising vendors, you will need to validate your account first.

3. Click **OK**.

Advertisements will appear on your website after publishing.

➤ ***To remove an advertising block:***

Place the mouse pointer over the block and click **Remove**.

Settings and Tools for Webmasters

This section describes how to do the following:

- Change website name, description, and keywords.
- Upload a site icon (favicon) for your website.
- Make your website more visible in search results, and embed various search engine services.
- Prevent certain pages or areas of your website from being indexed by search engines and shown in search results.
- Notify site visitors about the use of non-essential cookies on your site. This might be of interest only to webmasters residing in the European Union.

Changing Website Name, Description, and Keywords

Website name is a line of text that is shown in the title bar of a user's browser when they visit your website. By default, it is "My website", but you can change it to anything you want.

Website description is shown by search engines when your website is listed in search results. Website keywords are analyzed by search engines and are used for displaying your website when people search for these keywords.

You can specify the site description and keywords that the editor will use for all pages of your website (in **Settings** tab > **Basic**), and specify custom values for specific pages (in **Pages** tab > page name > **Edit page description and keywords**).

➤ ***To edit your website name, description, and keywords:***

1. Go to the **Settings** tab > **Basic** tab.
2. Specify the website name that your visitors will see as the title of their browser window when they visit your website.
3. To show both your website name and the current page name in the browser title window and to increase your website recognition in search engine results, select the **Add website name to page titles** checkbox.
4. Add short description (up to 255 symbols) of your website.
5. Provide a list of keywords that describe your website (10-15 keywords are recommended).

The description and keywords will be used by default for new and existing pages.

6. Click **OK** to save changes.

Uploading a Site Icon (Favicon)

A favicon is a small icon displayed in the browser's address bar when you visit a website, and also appears next to the website name in the list of favorite bookmarks. You can create a favicon using a variety of online tools and then upload your favicon through the Presence Builder editor. All your website visitors will see this favicon.

➤ *To upload a favicon for your website:*

1. Go to the **Settings** tab > **Basic** tab.
2. Click **Browse** and select the location of the favicon to upload. The favicon will be uploaded.
3. Click **OK** to save changes.

➤ *To remove a favicon from your website:*

1. Go to the **Settings** tab > **Basic** tab.
2. Click **Remove** in the **Favicon** section. The favicon will be removed.
3. Click **OK** to save changes.

Verifying Website Ownership

Most search engines require you to verify website ownership when you register your website or sign up for webmaster assistance services. Verification is typically done by uploading or creating a file with a specific file name.

➤ *To verify website ownership:*

1. Go to the **Settings** tab > **Advanced** tab.
2. Provide the verification file:
 - If you know the name of the verification file requested by a search engine, provide the verification file name in the **Create verification file** field and click **OK**. Presence Builder will create it in the correct place.
 - If you have already downloaded your verification file from a search engine, upload the verification file to the **Upload verification file** field and click **OK**.
3. After the verification file is created or uploaded and your website is published, confirm your ownership on the search engine website.
4. Click **OK** to save changes.

➤ **To edit the HTML <head> section of your website (for example, to add ownership verification meta code):**

1. Go to the **Settings** tab of the Presence Builder's main menu, then go to the **Advanced** subtab.
2. Click **Edit Metadata**.
3. Insert the code into the provided field and click **Add**.

Note: Only valid HTML tags permitted for <head> section by HTML standards are supported. Metadata changes will be available only after you publish your website.

4. Click **OK** to save changes.

Embedding Google Analytics Code

Google Analytics is a tool that allows you to obtain information about your visitors. After you register with Google Analytics and acquire the required code, you can embed Google Analytics on your website.

➤ **To embed Google Analytics:**

1. Register with the Google Analytics service and acquire the code.
2. Go to the **Settings** tab > **Advanced** tab.
3. Click **Embed Google Analytics**.
4. Insert the code you have received from Google Analytics into the provided field and click **Add**.

Note: Google Analytics will start working only after you publish your website.

5. Click **OK** to save changes.

Downloading the Sitemap

Some search engines will ask you to provide your sitemap for analysis and optimization purposes. You can download your sitemap from the Presence Builder editor.

➤ **To download your website sitemap:**

1. Go to the **Settings** tab > **Advanced** tab.
2. Click **Download Sitemap**.
3. Click **OK** to start downloading the `sitemap.xml` file.

Preventing Search Engines from Indexing Certain Pages of Your Site

To prevent search engines from indexing certain pages of your website, you can add the appropriate directives into the `robots.txt` file. This file is stored on the customer account to which your site is published.

➤ **To prevent search engines from indexing certain areas of your website:**

1. Go to the **Settings** tab > **Advanced** tab.
2. Click the link **Edit robots.txt**.
3. Type your directives into the input field. Place each directive on a new line.

For example, to prevent all search engine robots and crawlers from indexing the contents of the directory `/private` and the file `/my_secret.html` on your customer account, add the following lines:

```
User-agent: *
Disallow: /private/
Disallow: /my_secret.html
```

For more information about the `robots.txt` file and directives you can use, refer to <http://www.robotstxt.org/robotstxt.html>.

Notifying Site Visitors About the Cookie Policy

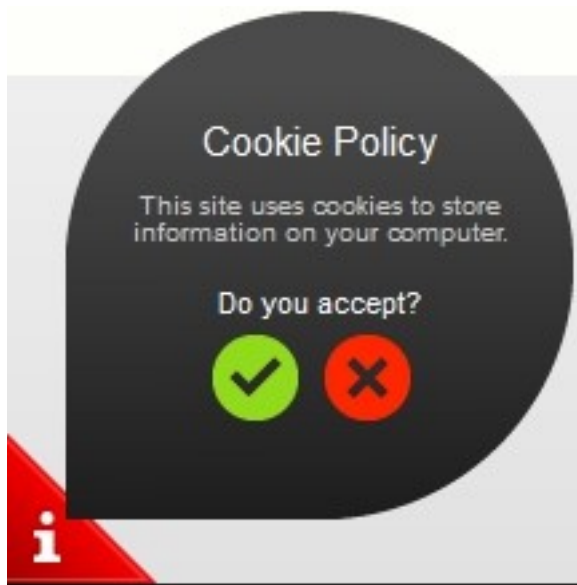
If you are located in the European Union, your site must inform its visitors about the use of non-essential cookies and obtain informed consent.


Cookies are small files that web servers save on visitors' computers. Cookies may be used for a number of purposes, from remembering personal preferences to tracking users' behavior for presenting targeted advertisements. Non-essential cookies are those that are not required for websites to function properly. Examples of non-essential cookies include those from analytics, advertising, and affiliate networks such as Google Analytics and Google AdSense.

Most likely, your site uses non-essential cookies if it uses the following functions:

- Google Analytics
- Publishing to Facebook
- Embedded video
- Image gallery module (with Picasa selected as storage)
- Online store module
- Map module
- Commenting module
- Social sharing module
- Script module
- Site search

If you choose to show a notice on the site, its visitors will be prompted to confirm that they accept your policy.



If they accept it, the notice is no longer shown (the icon  is shown instead in the page corner), and they can continue browsing your site. If they do not accept it, they are taken to google.com.

➤ ***To show a cookie notice on the site:***

1. Go to the **Settings** tab > **Advanced** tab.
2. Click the link **Notify Site Visitors About the Cookie Policy**.
3. Select the checkbox **Show the cookie notice on the site** and click **OK**.

Saving and Loading Copies of a Website


While working on the content and design of a website, you can save several copies of each site to the server and restore sites from the saved copies (also referred to as *snapshots*).

Saving site copies can be useful in the following cases:

- You want to prepare several versions of the same website, so that you can later load them for review, choose the best designed or the most appropriate version, and publish it to the Internet.
- You want to make significant changes or experiment on the site design or content, but be sure that you can safely undo the changes should anything go wrong.

Note: Pictures from the **Image Gallery** modules are not saved in snapshots. Images are stored on your customer account or Picasa Web Albums (if you use that option).


➤ *To save the current design and content of a site:*

1. In the Presence Builder editor's main menu, click the icon  next to the **Save** option.

Note: If you click **Save**, a quick-save site copy will be saved under the name **auto-saved snapshot**. You will be able to restore a site from this copy later, by clicking **Revert** in the main menu.

2. In the list that opens, select a free saving slot, type a name for the backup copy, and click **Save**.



➤ *To restore a site from a saved copy:*

1. In the Presence Builder editor's main menu, click the icon  next to the **Revert** option.



Note: If you click **Revert**, a site will be restored from the quick-save copy that was made the last time you clicked **Save**.

2. In the list that opens, select a site copy and click **Load**.
3. Click **Yes** to confirm you want to restore.



➤ *To download a site copy:*

1. In the Presence Builder editor's main menu, click the icon  next to the **Save** option.
2. Locate the copy that you want to download and click the  (Download) icon.
3. Select the directory on your computer where you want to save the file and click **OK**.

➤ **To upload a site copy:**

1. In the Presence Builder editor's main menu, click the icon  next to the **Revert** option.
2. Click the  (Upload) icon next to the slot to which you want to upload the copy.
3. Browse to the site snapshot file in the SSB format and select it.
4. If you want to restore a site from the uploaded snapshot, select it and click **Load**.

➤ **To remove a site copy:**

1. In the Presence Builder editor's main menu, click the icon  next to the **Save** option.
2. Locate the site copy that you want to remove and click the corresponding  (Remove) icon.

Publishing a Website to the Internet

When your website design and content are ready to be published to the Internet, click **Publish** in the top right corner of the main menu. Presence Builder will publish your website automatically to the location specified by your hosting provider.

Publishing a Website Copy to Facebook

After publishing a site on the Internet, you can drive more visitors to it by publishing a site copy to the popular social network site - Facebook (www.facebook.com).

A site copy on Facebook will show most of the content from your site; however, the following changes will be applied to its design, layout, and functionality:

- Headers, sidebars, and footers will not be shown.
- The navigation menu will be shown only at the top of the site pages.
- Page width will be limited to 520 pixels. For pages wider than 520 pixels, a horizontal scrollbar will be shown.
- The font face, size, and color will be changed to comply with the Facebook design, unless these font properties were specifically selected by the site owner in the Presence Builder editor.
- Image galleries, online store, and links for sharing on social media sites will not be shown.
- Any links pointing to other pages on Facebook will not work.

➤ ***If you want to add a site copy to Facebook, do the following:***

1. In the main menu, click the **Settings** tab > **Social Media** tab.
2. Leave the checkbox **Show a copy of my site on Facebook** selected.
3. Click the link **Add your site copy to Facebook**. The Facebook home page opens in a new browser window or tab.
4. To log in to your Facebook account, type your e-mail address and password, and click **Log In**.
5. If you do not have a Facebook page where you want to show a site copy, create one. To do this, click **Create It Now**, and follow the onscreen guidelines. After your page is created, return to the **Parallels Presence Builder at Facebook** page, which is shown in another browser window or tab.
6. Click **Add Parallels Presence Builder Application**. This application provides synchronization between the website on your hosting account and its copy on Facebook.
7. To confirm that you want to add the application to your page, click **Add Parallels Presence Builder**.

Now your site copy is added. To see it, click the **Website** link in the Facebook navigation pane on your left.

Whenever you make changes to your site and republish it through the Presence Builder editor, your site copy on Facebook will be updated accordingly.

➤ ***To remove a site copy from Facebook, do the following:***


1. In the Presence Builder editor's main menu, click the **Settings** tab > **Social Media** tab.
2. Clear the checkbox **Show a copy of my site on Facebook**.
3. Click **Yes** to confirm.
4. Go to your Facebook page and remove the Presence Builder application from there.

Viewing Site Visits Statistics, Comments, and New Orders on the Dashboard

After publishing a site, you can access the Dashboard from the Presence Builder's main menu to perform the following tasks:

- View statistics on website visits. The statistics are provided by Google Analytics and are available after you specify the code for Google Analytics in website settings, as described in the section *Settings and Tools for Webmasters* (on page 508).
- View new comments left by site visitors on your website pages. The comments are visible on the Dashboard after you set up the commenting functionality, as described in the sections *Blog* (on page 497) and *Commenting* (on page 500).
- View new orders from customers visiting your online stores. The new orders are visible on the Dashboard after you set up an online store, as described in the section *Online Store* (on page 504).

➤ *To view website visits statistics:*

1. On the main menu, click **Dashboard**.
2. If you access the dashboard for the first time, confirm association of your site with your Google Account:
 - a. Click **Log In to Google Analytics**.
 - b. Log in to your Google Account.
 - c. Confirm that you want to allow access to your account.
3. Under the **Website Visits Statistics** chart, click the link **See more charts**, or click the  icon.


The **Overview** section shows the following statistics for the past 30 days:

- A detailed chart for the metric currently selected under **Profile report**.
- The total number of visits during the past 30 days.
- The number of new visits.
- Average time spent on a site by users.
- The total number of page views.
- The number of page views per each visit.
- The percentage of new visits.


The **Traffic sources overview** section shows the addresses of websites from which your visitors were coming during the past 30 days. The **(direct)** item shows the percentage of visitors who accessed your site by typing its address directly in their browsers.

The **Visitors' locations** section shows the geographic locations of the visitors for the past 30 days.

➤ ***To view comments from your site visitors:***

1. On the main menu, click **Dashboard**.
2. Under **Comments**, click the link **See them**, or click the  icon.
3. To go to the webpage where the comment was left, click **Link to the comment**.
4. To go to the Disqus site for moderating the comments, click **Manage Comments**.

➤ ***To view orders submitted by the customers visiting your online stores:***

1. On the main menu, click **Dashboard**.
2. Under **Orders**, click the link **See them**, or click the  icon, and then click the **Orders** tab.
3. To go to the Ecwid site for processing the orders, click **Manage Orders**.

Deleting Websites

When you delete a site from the Presence Builder editor, only the current site draft opened in the editor and saved site copies (snapshots) are removed.

By default, the site copy published to your hosting account is not removed. However, this policy might be changed by your hosting provider.

➤ ***To delete a current site copy from the editor:***

In the Presence Builder editor's main menu, select **More > Remove Site**.

FTP Access to Your Websites

One of the most convenient ways to update your website content is to upload it through FTP. FTP (File Transfer Protocol) is a standard network protocol that allows transferring files between two hosts (for example, your computer and a Panel server). Panel acts as an FTP server, while users should use some FTP client to access the directories on the server. Panel provides all main FTP features:

- *Authorized access to the server.* Learn more in the section **Changing FTP Access Credentials** (on page 521).
- *Multiple user accounts* for collaborative work. Learn more in the section **Adding FTP Accounts** (on page 522).
- *Anonymous FTP access:* The access without authorization that may be used, for example, to share software updates. Learn more in the section **Setting Up Anonymous FTP Access** (on page 524).

Note: Your service provider's settings may require that you connect to the server by FTP using the secure protocol *FTPS* (or *FTP-SSL*). Thus, when connecting to the Panel server over FTP, make sure that your client supports FTPS and the connection to the Panel server uses this protocol.

In this chapter:

Changing FTP Access Credentials.....	521
Adding FTP Accounts.....	522
Setting Up Anonymous FTP Access.....	524

Changing FTP Access Credentials

➤ **To change FTP account username or password:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the webspace where the website is hosted.
2. Click the **Websites & Domains** tab.
3. Click **Web Hosting Access**.
4. Type a new username or password.
5. Click **OK**.

Adding FTP Accounts

If you are working on your website together with someone else or host subdomains for other users, you might want to create separate FTP accounts for them.

➤ ***To create an additional FTP account:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Click the **Websites & Domains** tab.
3. Click **FTP Access**.
4. On the **Additional FTP Accounts** tab, click **Create Additional FTP Account**.
5. Specify the following:
 - **FTP account name.** Type an arbitrary name.
 - **Home directory.** Select the directory to which the user will be taken when he or she connects to the FTP account.
 - **FTP password.**
 - **Hard disk quota** (on Windows hosting). To limit the amount of disk space on the server that the FTP user can occupy, clear the **Unlimited** checkbox next to the **Hard disk quota** box, and type the amount of disk space in megabytes.
 - **Read permission** (on Windows hosting). To allow the FTP user to view the contents of the home directory and download files from it, select the **Read permission** checkbox.
 - **Write permission** (on Windows hosting). To allow the FTP user to create, view, rename and delete directories in the home directory, select the **Write permission** checkbox.

On Window hosting, if you do not grant any permissions, a connection to the FTP account will be made, but the contents of the home directory will not be shown to the user.

6. Click **OK**.

➤ ***To change the properties of an additional FTP account:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Click the **Websites & Domains** tab.
3. Click **FTP Access**.

4. On the **Additional FTP Accounts** tab, click the required FTP account name in the list.
5. Make the required changes and click **OK**.

➤ ***To remove an additional FTP account:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Click the **Websites & Domains** tab.
3. Click **FTP Access**.
4. On the **Additional FTP Accounts** tab, select the checkbox corresponding to the FTP account you want to remove and click **Remove**.
5. Confirm removal and click **OK**.

Setting Up Anonymous FTP Access

If your site is hosted on a dedicated IP address (not shared by other users or sites), you can set up a directory within the site, where other users will be able to anonymously download or upload files through FTP. Once anonymous FTP is switched on, the users will be able to log in to the directory at an address like ftp://ftp.your-domain.com with the "anonymous" username and any password.

➤ **To allow anonymous FTP access:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Click the **Websites & Domains** tab.
3. Click **FTP Access**.
4. Click the **Anonymous FTP** tab.
5. Do the following:
 - a. To activate anonymous FTP service, click **Switch On**.
 - b. To set up a welcoming message to be displayed when users log in to FTP site, select the **Display login message** checkbox and type the message text in the input field as desired.

Note that not all FTP clients display welcoming messages.
 - c. To allow visitors to upload files to the `/incoming` directory, select the **Allow uploading to incoming directory** checkbox.
 - d. To allow users to create subdirectories in the `/incoming` directory, select the **Allow creation of directories in the incoming directory** checkbox.
 - e. To allow downloading files from the `/incoming` directory, select the **Allow downloading from the incoming directory** checkbox.
 - f. To limit the amount of disk space that can be occupied by uploaded files, clear the **Unlimited** checkbox corresponding to the **Limit disk space in the incoming directory** option, and specify the amount in kilobytes.

This is the hard quota: The users will not be able to add more files to the directory when the limit is reached.

- g. To limit the number of simultaneous connections to the anonymous FTP server, clear the **Unlimited** checkbox corresponding to the **Limit number of simultaneous connections** option and specify the number of allowed connections.
 - h. To limit the bandwidth for anonymous FTP connections, clear the **Unlimited** checkbox corresponding to the **Limit download bandwidth for this virtual FTP domain** option and enter the maximum bandwidth in kilobytes per second.
6. Click **OK**.
- **To change settings for anonymous FTP service or switch it off:**
1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
 2. Click the **Websites & Domains** tab.
 3. Click **FTP Access**.
 4. Click the **Anonymous FTP** tab.
 5. Perform the operation you need:
 - Adjust the settings as required and click **OK**.
 - To switch off the anonymous FTP service, click **Switch Off**.

Mail Accounts

You can create and remove mail accounts right from the Control Panel, set up mail forwarding, protection from spam and viruses, and so on.

Panel allows you to configure mail services on two levels:

- *Configuring mail account settings.* These settings affect mail account only. For example, where to forward received messages or what to do with potential spam. Learn more about possible operations on mail accounts in the section **Configuring Mail Account** (on page 528).
- *Configuring global mail settings.* These are subscription-wide settings that affect all mailboxes within a subscription. For example, which webmail system Panel should use, or what to do with mail sent to nonexistent users. These settings may be unavailable in your hosting plan. To get the details on how to change global mail settings, refer to the section **(Advanced) Configuring Global Mail Settings** (on page 535).

If you want to use some of your e-mail addresses to distribute news and promotions, or set up group discussions, consider setting up mailing lists. These are e-mail addresses to which a number of users are subscribed. Learn more in the section **Using Mailing Lists** (on page 536).

Next in this section:

Adding Mail Accounts	527
Configuring Mail Account.....	528
(Advanced) Configuring Global Mail Settings	535
Using Mailing Lists	536

Adding Mail Accounts

➤ *To create an e-mail address:*

1. Run the **Create E-mail Address** wizard from the **Mail** tab of the Control Panel.
2. Specify the following mailbox settings:
 - **E-mail address.** Type the left part of the e-mail address before the @ sign, and, if you have several domain names on your account, select the domain name under which the e-mail address will be created.
 - **Access to the Control Panel.** Select this option if you want Panel to create an auxiliary user for the mail account owner. By default, this user has the role Application user. However, you can change this role and other user's properties later. For details, see the section **(Advanced) Managing Auxiliary User Accounts** (on page 370).
 - **Password.** Set the password for accessing the mailbox. If you leave the option **Access to the Control Panel** selected, the same password will be used for logging the user in to to the Control Panel.
 - **Mailbox.** Turning off this option makes sense only if you want to use this address as a mail forwarder, which will forward all incoming mail to another address.
 - **Mailbox size.** If you leave the option Mailbox selected, specify the mailbox size or use the default size defined by the provider's policy or your service plan.

Configuring Mail Account

If the provider's policy allows setting up mail accounts and services, then you can set up and use multiple email services located on the following tabs of the mail account page:

- **General.** General mail account properties, such as its address, password and size.
- **Forwarding.** Email forwarding service that will send copies of all incoming messages to another email address.
- **Email Aliases.** Additional email addresses that are associated with a user's primary (or main) email address. Email aliases can be used as temporary disposable addresses that can be published on the Internet. When spam starts coming to an address that was set up as an email alias, you can remove that alias and create another one.
- **Auto-Reply.** Automatic response service that sends a predefined email message in reply to any incoming message. This is useful for sending "out of office" or "on vacation" notices when you are away.
- **Spam Filter.** Checking all incoming messages by antispam filter. In addition, you can specify what to do with messages identified as spam: Remove them, move to a special folder, or just add some text to the message subject.
- **Antivirus.** Checking all incoming and outgoing mail for viruses.
- **Additional Services.** If you use web apps that provide email-related services, for example, antispam or webmail, you can define if each of these services is able to access this mail account.

Next in this section, we will provide instructions on how to configure these services for mail accounts.

Next in this section:

Setting Up Mail Forwarding	529
Creating Mail Aliases	529
Setting Up Auto-Reply	530
Protecting from Spam	530
Protecting from Viruses	533
Additional Services	534

Setting Up Mail Forwarding

➤ *To set up e-mail forwarding for an e-mail address:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **e-mail address** > **Forwarding** tab.
3. Select the **Switch on mail forwarding** checkbox.
4. Specify one or several e-mail addresses to which e-mail must be forwarded. When specifying e-mail addresses, separate them with white spaces, commas, semicolons, or type each of them on a new line.
5. Click **OK**.
6. If you do not want to keep copies of forwarded messages in the mailbox, go to the **Mail** tab > **e-mail address**, clear the **Mailbox** checkbox, and click **OK**.

➤ *To switch off mail forwarding:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **e-mail address** > **Forwarding** tab.
3. Clear the **Switch on mail forwarding** checkbox, and click **OK**.

Creating Mail Aliases

➤ *To add or remove additional e-mail addresses (e-mail aliases) for a mail account:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **e-mail address** > **E-mail Aliases** tab.
3. Do any of the following:
 - To add an address, type it into the **E-mail alias** box, and click **OK**.
 - To remove an address, click the **Remove** link to the right of the address you want to remove.

Setting Up Auto-Reply

➤ *To set up automatic reply settings for an e-mail address:*

1. Go to the **Mail** tab > **e-mail address** > **Auto-Reply** tab.
2. Select the **Switch on auto-reply** checkbox, and specify the following settings:
 - **Auto-reply message subject.**
 - **Message format.** We recommend that you leave the option Plain text selected because some of your recipients might be unable to see the text formatted with HTML.
 - **Encoding.** We recommend that you leave the UTF-8 encoding selected to ensure that the letters in your message are displayed properly.
 - **Message text.**
 - **Forward to.** If you want to forward incoming messages to another email address, type an email address in this box.
 - **Send an automatic response to a unique e-mail address no more than...** The default value is "1 time a day", meaning that if your mailbox receives several messages from the same email address in one day, Panel will send automatic response only to the first message. If the value is "2", then Panel will send automatic response to the first and the second messages, and so on.
 - **Attached files.** If you want to attach a file to your message, click **Browse** and select a file.
3. Click **OK**.

To switch off automatic reply, deselect the **Switch on auto-reply** option and click **OK**.

Protecting from Spam

➤ *To switch on spam filtering for a mailbox:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Mail** tab > **e-mail address** > **Spam Filter** tab.
3. Select the checkbox **Switch on spam filtering for this e-mail address**.
4. Specify what to do with messages classified as spam.
 - If you want to filter mail with the software on your local computer, select the option **Mark spam messages by adding the following text to message subject**, and then specify how spam filter should mark the messages recognized as spam. "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers are added to the message source by default, and if you want, the spam filter will also add a specific text string to the beginning of the subject line and to the message body.

- If you are sure that your spam filter is accurate, you may want to set the filter to automatically delete all incoming messages recognized as spam. To do this, select the option **Delete all spam messages**.
- If you are accessing your mailbox over IMAP protocol and want the spam filter to move all messages considered spam to the IMAP folder called Spam, select the option **Move spam to the Spam folder**.

Because all messages are automatically removed from the Spam folder after 30 days, you will need to review the contents of the Spam folder on a regular basis to make sure you do not miss any important messages, and move all non-spam messages back to the Inbox folder.

When the option **Move spam to the Spam folder** is selected, you can train the spam filter and improve its accuracy by moving spam messages from Inbox to Spam, and non-spam messages from Spam to Inbox.

5. If you want to adjust spam filter sensitivity, click **Show Advanced Settings**, and type a number of points that a message must score to be considered spam. SpamAssassin performs a number of different tests on contents and subject line of each message. As a result, each message scores a number of points. The higher the number, the more likely a message is spam. For example, a message containing the text string "BUY VIAGRA AT LOW PRICE!!!" in subject line and message body scores 8.3 points. By default, the filter sensitivity is set so that all messages that score 7 or more points are classified as spam.
 - If you receive lots of spam messages with the current setting, to make filter more sensitive, try setting a lesser value in the **Spam filter sensitivity** box; for example, 6.
 - If you are missing your e-mails because your spam filter thinks they are junk, try reducing filter sensitivity by setting a higher value in the **Spam filter sensitivity** box.

Note: To further improve spam filter accuracy, you may want to train your spam filter on e-mail messages you receive, as described further in this section.

6. If you want to be sure that you will not miss e-mail from specific senders, type e-mail addresses or domain names into the **White list** field.

Place each address in one row, or separate addresses with a coma, a colon, or a white space. You can use an asterisk (*) as a substitute for a number of letters, and question mark (?) as a substitute for a single letter. For example: address@mycompany.com, user?@mycompany.com, *@mycompany.com. Specifying *@mycompany.com will add to the white list all e-mail addresses that are under the mycompany.com mail domain.
7. If you do not want to receive e-mail from specific domains or individual senders, type e-mail addresses or domain names into the **Black list** field.

Place each address in one row, or separate addresses with a coma, a colon, or a white space. You can use an asterisk (*) as a substitute for a number of letters, and question mark (?) as a substitute for a single letter. For example: address@spammers.net, user?@spammers.net, *@spammers.net. Specifying *@spammers.net will block the entire mail domain spammers.net.
8. If you use a Windows-based customer account, then you can also specify trusted languages and character sets. E-mail messages written in the specified languages and with the defined character sets will pass the spam filter and will not be marked as spam.

9. On Windows-based customer accounts, you can also specify IP addresses of computers or networks from which e-mail must always be accepted. When specifying network addresses, type an address and add a network mask after a slash. For example, 192.168.10.10/24.

10. Click OK.

You can improve accuracy of spam detection if SpamAssassin spam filter on the server is switched on for your account and you are accessing your mailbox over IMAP protocol.

➤ ***To improve accuracy of spam detection:***

1. Access your mailbox with webmail or a mail client program on your computer.
2. Review the messages in your **Inbox** folder. Move all spam messages to the **Spam** folder. This will make the SpamAssassin spam filter recognize spam more efficiently.

Protecting from Viruses

To defend your system from viruses, do not open suspicious e-mail attachments, enable antivirus protection on the server side, if this service is provided by your hosting company, and be sure to have a firewall and antivirus software installed on your personal computer. Also keep your operating system up-to-date and timely install security hot fixes and patches.

➤ *To switch on antivirus protection for a mailbox:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **e-mail address** > **Antivirus** tab.
3. Select the checkbox **Switch on antivirus protection for this e-mail address**.
4. Choose the desired mail scanning mode. You can switch on scanning for incoming mail, outgoing mail, or both.
5. Click **OK**.

When an infected message comes, you will be notified by e-mail. If Kaspersky Antivirus is used by your provider, then you might be able to configure it at the **Mail** tab > **e-mail address** > **Antivirus** tab.

➤ *To switch off antivirus protection for a mailbox:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **e-mail address** > **Antivirus** tab.
3. Clear the checkbox **Switch on antivirus protection for this e-mail address**.
4. Click **OK**.

Additional Services

Some email-related web apps (like webmail or antispam) are able to provide a part of their functionality right in your Control Panel. For example, you can associate a mail account with an account in the *Open-Xchange* webmail. In this case, the mail user will see the link to webmail right in their Control Panel.

To integrate an app in such a way, you should allow these app to access a certain mail account. You can do this on the mail account settings page during the account creation or editing.

➤ ***To allow certain apps to access an email account:***

1. Go to the **Mail** tab > select an email address > **Additional Services** tab.
2. In the list of installed apps that provide email-related services, select the **Granted** option for the apps that should access this email account.
3. Click **OK**.

➤ ***To deny certain apps to access an email account:***

1. Go to the **Mail** tab > select an email address > **Additional Services** tab.
2. In the list of installed apps that provide email-related services, select the **Denied** option for the apps that should not access this email account.
3. Click **OK**.

(Advanced) Configuring Global Mail Settings

You can configure the following mail service settings that apply to all domains created under a subscription:

- Mail service status. You can switch the mail service on or off. If the mail service is switched off, then e-mail messages cannot be sent or received.
- Mail bounce settings. When somebody sends an e-mail message to an e-mail address that does not exist under your domain, the mail server, by default, accepts mail, processes it, and when it finds out that there is no such a recipient under the domain, it returns the mail back to sender with an error message. You can choose to:
 - Continue returning all such mail back to senders (**Bounce with message** option),
 - Forward all such mail to the specified e-mail address (**Forward to address** option),
 - Forward all such mail to another mail server with the specified IP address using the option **Redirect to external mail server with IP address** (available only for Windows hosting),
 - Reject such mail without accepting it and without notifying senders (**Reject** option).
- Webmail. If your service plan provides the option to choose which webmail program to use for your account, then you can select it in the global mail settings.

➤ *To configure the mail service settings:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab, and then click **Change Settings**.
3. Select the required options, and click **OK**.

Using Mailing Lists

Mailing list is a group e-mail address to which a number of users are subscribed. Mailing lists are used for sending e-mail messages to multiple recipients at once. E-mail messages sent to mailing list subscribers can include anything from plain text to colorful newsletters and promotions with embedded images and links, and attached multimedia and presentation materials.

How it all works: you create a mailing list e-mail address in the Panel, and subscribe users to it. Then you send your message to the mailing list address, and all subscribers receive it.

➤ *To set up a mailing list and subscribe users to it:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **Mailing Lists** tab.
3. Click **Create Mailing List**.
4. Type the mailing list address and, if you have several websites, select the website under which the mailing list will be created.
5. To subscribe users to the mailing list, type their e-mail addresses, one address per line.
6. To notify the mailing list administrator about mailing list creation, select the checkbox **Notify administrator on the mailing list creation**.
7. Click **OK**.

➤ *To subscribe or unsubscribe users:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **Mailing Lists** tab.
3. Click the mailing list address.
4. Do any of the following:
 - To subscribe users to the mailing list, type their e-mail addresses into the **Subscribers** field, one address per line.
 - To unsubscribe users, remove their addresses from the **Subscribers** field.
5. Click **OK**.

➤ **To remove a mailing list:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Mail** tab > **Mailing Lists** tab.
3. Select a checkbox corresponding to the mailing list you want to remove and click **Remove**.
4. To confirm removal, click **Yes**.

➤ **To switch off the mailing lists service and all mailing lists created under the currently selected subscription:**

1. Go to the **Mail** tab > **Mailing Lists** tab.
2. Click **Switch Off the Service**.

➤ **To switch on the mailing lists service for the currently selected subscription:**

1. Go to the **Mail** tab > **Mailing Lists** tab.
2. Click **Switch On the Service**.

Scheduling Tasks

If you need to run scripts on your hosting account at specific time, use the task scheduler in the Panel to make the system automatically run the scripts for you.

Next in this section:

Scheduling Tasks (Linux)	538
Scheduling Tasks (Windows)	540

Scheduling Tasks (Linux)

If you need to run scripts on your hosting account at specific time, use the task scheduler in the Panel to make the system automatically run the scripts for you.

During installation of the Panel, the following tasks are automatically created:

- `autoreport.php` – delivers daily, weekly and monthly reports on domains (three separate tasks)
- `backupmng` – initiates scheduled backing up of domains once every 30 minutes
- `statistics` – generates statistics on resource usage by domains
- `mysqldump.sh` - creates a backup copy of three MySQL databases: psadump, MySQL, and Horde databases

As all these tasks are related to statistics, databases, and reports, it is strongly recommended that you neither change nor remove them.

➤ *To schedule a task:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
3. Click **Schedule New Task**.
4. Leave the **Switched on** checkbox selected.
5. Specify when to run your command:
 - **Minute** - enter the value from 0 to 59
 - **Hour** - enter the value from 0 to 23
 - **Day of the month** - enter the value from 1 to 31
 - **Month** - enter the value from 1 to 12, or select the month from a drop-down box
 - **Day of the week** - enter the value from 0 to 6 (0 for Sunday), or select the day of the week from a menu.

You can schedule the time using the UNIX crontab entry format. In this format, you can:

- Enter several values separated by commas. Two numbers separated by a hyphen mean an inclusive range. For example, to run a task on the 4th, 5th, 6th, and 20th of a month, type 4-6,20.
- Insert an asterisk to specify all values allowed for this field. For example, to run a task daily, type * in the **Day of the month** text box.

To schedule the task to run every Nth period, enter the combination */N, where N is a value for this field (minute, hour, day, month). For example, */15 in the **Minute** field schedules the task to start every 15 minutes.

You can type the contracted names of months and days of the week, which are the first three letters: Aug, Jul, Mon, Sat, and so on. However, the contracted names cannot be separated with commas or used together with numbers.

6. Specify which command to run. Type it into the **Command** input box.

For example, if you want to run the backup creation task at the specified time and have the backup file sent to your e-mail, you need to specify the following command in the **Command** input box:

```
/usr/local/psa/admin/sbin/backupmng
```

7. Click **OK**.

➤ ***To receive notifications when the tasks are started:***

1. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
2. Click **Settings** and specify the notification policy.

➤ ***To temporarily suspend execution of a scheduled task:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
3. Locate the task that you want to suspend and click the corresponding link in the **Command** column.
4. Clear the **Switched on** checkbox and click **OK**.

➤ ***To resume execution of a scheduled task:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
3. Locate the task whose execution you want to resume and click the corresponding link in the **Command** column.
4. Select the **Switched on** checkbox and click **OK**.

➤ ***To cancel a task:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
3. Select a checkbox to the left of the task that you want to cancel and click **Remove**.
4. Confirm removal and click **OK**.

Scheduling Tasks (Windows)

If you need to run scripts on your hosting account at specific time, use the task scheduler in the Panel to make the system automatically run the scripts for you.

During installation of the Panel, the following tasks are automatically created:

- Update antivirus database – updates Parallels Premium Antivirus database.
- Statistics calculation - generates statistics on resource usage, such as traffic and disk space.

As all these tasks are related to site statistics, databases and reports, it is strongly recommended that you neither change nor remove them.

➤ *To schedule a task:*

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
3. Click **Schedule New Task**.
4. Leave the **Switched on** checkbox selected if you want your scheduled task to be active immediately after the creation.
5. Type a name for your task in the **Description** field.
6. In **Scheduler notification**, specify whether the scheduler should notify you when it runs this task. The following options are available:
 - **Switched off** - do not notify you.
 - **Send to the default e-mail** - send the notification to your default e-mail address.
 - **Send to the e-mail I specify** - send the notification to the e-mail specified in the corresponding field. After selecting this option, you need to type the required e-mail address in the field on the right.
7. Specify which command or executable file to run. Type it into the **Path to executable file** input box. If you need to run the command with certain options, type them in the **Arguments** field.
 - For example, if you want to run the statistics calculation task to count disc space and see more detailed information for the example.com and example.net domains, you need to specify the following path in the **Path to executable file** input box:

```
C:\Program Files\Parallels\Parallels  
Panel\admin\bin\statistics.exe
```

and the following options in the **Arguments** field:

```
--disk-usage --process-domains=example.com, example.net -  
verbose
```

- If you want to run your own PHP script using the task scheduler, you need to specify the following path in the **Path to executable file** input box:

```
C:\Program Files (x86)\Parallels\Parallels  
Panel\Additional\PleskPHP5\php.exe
```

and specify the script location in the **Arguments** field:

```
C:\Inetpub\vhosts\mydomain.tld\httpdocs\myscript.php
```

8. Select the appropriate priority in the **Task priority** field. Task priority can be set to **Low**, **Normal** or **High**.
9. Specify when to run your command by selecting the appropriate checkboxes in the **Hours**, **Days of month**, **Months** or **Days of week** fields.
10. Click **OK** to schedule the task or click **Run Now** to schedule the task and immediately run it.

➤ ***To temporarily suspend execution of a scheduled task:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
3. Choose a task that you want to suspend and click the corresponding link in the **Description** column.
4. Clear the **Switched on** checkbox.
5. Click **OK**.

➤ ***To resume execution of scheduled task:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.
3. Choose a task whose execution you want to resume and click the corresponding link in the **Description** column.
4. Select the **Switched on** checkbox.
5. Click **OK**.

➤ ***To cancel a task:***

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required workspace.
2. Go to the **Websites & Domains** tab > **Scheduled Tasks**.

3. Select a checkbox to the left of the task that you want to cancel and click **Remove**.
4. Confirm removal and click **OK**.

Website Databases

If your website incorporates custom data processing applications or is designed to generate web pages dynamically, you will probably need a database for storing and retrieving data.

In Panel, you can manually create a new database (on page 543) for your site, make a database copy (on page 544) and manage database user accounts (on page 545). These operations are available in **Websites & Domains** tab > **Databases**. In addition, you can use the third-party database management tools supplied with Panel to edit tables in databases, export and import data (on page 544), and run SQL queries. These tools are available under the **Webadmin** link in **Websites & Domains** tab > **Databases** and may vary depending on the database type. For example, Panel employs phpMyAdmin to manage MySQL databases.

Note that when you install an app from the Application Catalog, all required databases and database user accounts are created automatically. Alternatively, you can assign a manually created user account to a database created by a web app. For more information, see the section **Using Website Applications > App Databases**.

Accessing Databases with ODBC

If you wish to deploy an application which works with a database through an Open Database Connectivity (ODBC) driver, you will need to create an appropriate ODBC data source in the operating system. In Panel for Windows you can add new ODBC data sources for a number of supported ODBC drivers. For more information, see **Accessing Databases with ODBC (Windows)** (on page 546).

For the details on operations with databases and database users, refer to the relevant sections of this chapter.

Next in this section:

Creating Databases.....	543
Accessing Databases.....	543
Copying Databases.....	544
Exporting and Importing Databases.....	544
Managing Database User Accounts.....	545
Accessing Databases with ODBC (Windows).....	546

Creating Databases

Panel allows you to create and remove databases on the **Websites & Domains tab > Databases** page.

You can create a database by specifying its name. If your subscription grants you the corresponding permission, you can choose a database type and the database server on which the database should be created.

A database must have at least one user account associated with it. Otherwise, it will be impossible to access the database. You can create a database user while creating a database by selecting the **Create a new database user** checkbox. Alternatively, you can clear the checkbox and select a user later, for example, if you want to use one of the existing user accounts. For more information, see **Database User Accounts** (on page 545).

Note that you can only remove the databases and database users that are not used by APS apps. If the required checkbox appears grayed out, it means that this database is used by an app and you can remove it only by removing the respective app.

Accessing Databases

After you have created a database and assigned a database user to it, you can access it from Panel using the **Webadmin** link on the **Websites & Domains tab > Databases** page. In this case, Panel automatically uses the corresponding database user credentials.

If you want to access your database using other tools (like SQL Server Management Studio) or want to give other applications access to it, you will need to provide these tools and applications with the following:

- To connect to *MySQL* and *PostgreSQL*, you will need to provide the host name (or IP address) and the database user login and password.
- To connect to *Microsoft SQL Server*, you will also need to specify the Microsoft SQL Server instance. For *Microsoft SQL Server 2008*, Panel uses the `MSSQLSERVER2008` named instance. Therefore, the host can be specified as `mydomain.com\MSSQLSERVER2008` or `123.123.123.123\MSSQLSERVER2008`. For *Microsoft SQL Server 2005*, Panel uses the default instance (`MSSQL 2005`), and you do not need to specify the instance name.

Copying Databases

Panel allows you to copy databases from one database server registered in Panel to another, as well as to any remote server, provided that the source and the destination servers are of the same type, for example, MySQL.

You can copy a database by running **Websites & Domains > Databases > Copy** for this database and specifying the destination server, the subscription and the database name. For a remote server, you should select **Other** in the **Database destination server** list and provide the following additional information:

- *Host name or IP address* of the remote database server.
- *Username and password* of the remote database server's administrator. For example, the MySQL administrator's credentials.

Note: When you choose an existing database as a destination, those tables in the destination database whose names also appear in the source database will be fully replaced.

Types of Copy

When you copy a database, you can choose whether to create a full database copy including data in the tables (the **Create a full copy** option), or to copy only the database structure. In the latter case, Panel will create tables without data in the destination database.

Exporting and Importing Databases

With Panel, to export a database means to save a source database in a file which can be used for storage or distribution. To import a database means to restore data from the file to a destination database. You can import a database to the same or another database server. The only restriction is that the destination database should be of the same type, for example, MySQL.

One reason for exporting databases is to back them up. While Panel for Windows offers a separate functionality for backing up databases (on page 552), on Panel for Linux, exporting is the only option for creating separate database backup files.

The export and import functionality is provided by the database management tool available through the **Webadmin** link in **Websites & Domains > Databases**.

Note: It is recommended that you import data into a new database.

For the instructions on how to perform import and export with database management tools, refer to the tools' built-in help sections.

Managing Database User Accounts

When you work with a database in Panel, the latter accesses the database on behalf of a user account associated with the database. Therefore, every database should have at least one associated user account; otherwise, you will be unable to access it.

Any database user can be set as *default* for a certain database. Panel will always access the database using this default user even if there are other users associated with it. If a database has several associated user accounts, none of which are default, the first account from the list will be used.

Types of Database Users

There are two types of database user accounts in Panel:

- *User accounts which have access to only one particular database.*
If you collaborate with other people on managing a website and wish to give them access to the database, you should create separate user accounts for them. Each of these accounts is used to access only one database. In this case, you first create a database and then user accounts.
- *Universal user accounts which have access to all databases.*
Universal users have access not only to *all* existing databases, but to all newly created databases as well.
If you plan to install a number of web apps on your site, it may be convenient to create one universal user account, so that all the apps can access their databases using this account. In this case, you first create a user account and then specify it when installing apps.

Note: A universal user acts only within one database server. If you use several database servers, create a separate universal user account for each server.

Operations with Database Users

You can create, update or remove a database user by going to **Websites & Domains > Databases**, and selecting the **Users** tab of the required subscription.

When creating a database user, you will be prompted to provide the user credentials for accessing the database and the name of the database which the specified user will access. A *universal* database user can be created by selecting **Any** for a **Database name**.

Notes:

1. You can remove a default database user only by removing the database associated with this user. Alternatively, you can edit the user and clear the **Make the user default for this database** option, and then remove the user.
 2. If a database user was created by an APS app, you can remove this user only by removing the respective app.
-

Accessing Databases with ODBC (Windows)

If your application needs to access external databases through ODBC, you can create the necessary ODBC connection in Panel. After you have created the ODBC connection, you can customize the application to use that ODBC connection to access information in the database.

Note that the database does not necessarily need to be external; ODBC can be used to access local databases as well.

Operations with ODBC Connections

You can create, change or remove ODBC connections on the **Websites & Domains > <domain_name> > ODBC Data Sources** page.

When you create an ODBC connection, you should provide the connection name and description as well as the required driver. Depending on the selected driver, you will be prompted to specify some additional parameters, such as the path to the database, user credentials, and other connection options.

Backing Up and Recovering Websites

Panel provides the backing up and restoration facilities that you can use to prevent the loss of your data.

During the backup operation, Panel saves your account settings and websites' content into a number of files. You can create a number of backups and restore any of them at any time later.

This chapter describes how to perform the following operations in Panel:

- Backing up all data related to your account and sites. Learn more in the section **Backing Up Account and Websites** (on page 550).
- Backing up databases (Windows). Learn more in the section **Backing Up Databases (Windows)** (on page 552).
- Scheduling backups. Learn more in the section **Scheduling Backups** (on page 553).
- Restoring data from backup archives. Learn more in the section **Restoring Data** (on page 556).

Next in this section:

Backing Up Data	548
Managing Backup Files	554
Restoring Data	556

Backing Up Data

Depending on your needs, Panel can perform two types of backup:

- *Customer account configuration.* Such backups have small size and are convenient for restoring account settings in case of configuration problems.
- *Customer account configuration and websites content.* This type of backup requires more disk space and system resources because the Panel also saves the content of all websites. Such full backups are the best way to prevent data loss.

You can perform backup manually at any time, or schedule it for a specific time. For example, make the full backup once a day at night time when the number of site visits is minimal. To get the details on scheduling backups, refer to the section **Scheduling Backups** (on page 553).

Storing Backups

There are two ways of storing backups in Panel:

- *On the Panel-managed hosting server.* All backup files are stored on your Panel server along with other account content. Note that in this case backup files occupy the disk space provided by your subscription.
- *On a remote FTP server.* All backup files are stored on a remote FTP repository. In this case, backup files do not occupy the disk space provided by your subscription. The instructions on how to configure Panel to save backups to an FTP account are provided below in this section.

Creating Password-protected Backups

Since Panel 11.0, you are able to secure sensitive data in your backups by protecting them with a password. Protection makes it impossible for an attacker to reveal backup data if the security of your external backup storage is compromised.

You can specify a backup password in the following circumstances:

- In your FTP repository settings (**Websites & Domains > Backup Manager > Personal FTP Repository Settings**).
- When downloading a backup file from the Panel internal repository to some external location.

When uploading these backups back to Panel and restoring them, you will be prompted to provide the password you used for protection.

Important:

If you forget the password you used for backup protection, it cannot be recovered. Therefore, it is strongly recommended to keep a list of your passwords and corresponding backup file names in a safe place.

Configuring Panel for Working with an FTP Repository

If you are going to use an FTP server for storing backup files, you should specify its settings in **Account** tab > **Back Up My Account and Websites** > **Personal FTP Repository Settings**:

- FTP server's IP address or host name.
- Directory on the server where you want to store backup files.
- User name and password for access to the FTP account.
- Password that Panel will use for protecting backup files.

Next in this section:

Backing Up Account and Websites	550
Backing Up and Restoring Databases (Windows).....	552
Scheduling Backups	553

Backing Up Account and Websites

➤ **To back up all data related to your account and all your subscriptions:**

1. Go to the **Account** tab > **Back Up My Account and Websites** > **Back Up**.
2. Specify the following:
 - Backup file name prefix and description. You cannot specify an arbitrary file name, however, you can set the Panel to add a prefix to backup file names. Note that the Panel automatically adds the date and time of backup file creation (in Universal Time) to backup file names.
 - Splitting of the backup file. To create a multivolume backup, select the corresponding checkbox and specify volume size in megabytes.
 - Location where to store the backup file. Select the repository where you would like to store the backup file.
 - E-mail notification on backup completion. If you want to be notified of the backup completion, type your e-mail address.
 - What data to back up. You can back up only the account settings or account settings and all data (including databases).
 - **Suspend domains until backup task is completed.** Select this option to prohibit users from making changes to content or settings of websites while they are being backed up.

Note: If you select this option, then, after restoring the data from this backup file, you will need to manually switch on every domain alias for every site that needs to have domain aliases. This can be done at **Websites & Domains** tab > *domain alias name* > **Switch On**.

3. Click **Back Up**.

When backing up is finished, the backup file will be saved to the repository you selected.

➤ **To back up all websites related to a subscription:**

1. If you are subscribed to several hosting packages and have access to several webspaces associated with your account, in the **Subscription** menu at the top of the screen, select the required webspace.
2. Go to the **Account** tab > **Back Up Websites** > **Back Up**.
3. Specify the following:
 - Backup file name prefix and description. You cannot specify an arbitrary file name, however, you can set the Panel to add a prefix to backup file names. Note that the Panel automatically adds the date and time of backup file creation (in Universal Time) to backup file names.
 - Splitting of the backup file. To create a multivolume backup, select the corresponding checkbox and specify volume size in megabytes.
 - Location where to store the backup file. Select the repository where you would like to store the backup file.

- E-mail notification on backup completion. If you want to be notified of the backup completion, type your e-mail address.
- What data to back up. You can choose to back up:
 - Only settings of websites.
 - All settings and data with or without mail accounts and messages in mailboxes.
 - Only mail accounts with messages.
- **Suspend domains until backup task is completed.** Select this option to prohibit users from making changes to content or settings of websites while they are being backed up.

Note: If you select this option, then, after restoring the data from this backup file, you will need to manually switch on every domain alias for every site that needs to have domain aliases. This can be done at **Websites & Domains** tab > *domain alias name* > **Switch On**.

4. Click **Back Up**.

When backing up is finished, the backup file will be saved to the repository you selected.

Backing Up and Restoring Databases (Windows)

If you are using a Windows-based customer account, then you can back up and subsequently restore databases, database user accounts, and data used by your websites.

You can:

- Back up your domain databases with all data and user accounts.
- Restore databases from backup files.
- Download, upload and remove database backup files.
- Recover users who became orphaned after the restoration.

Important: Panel does not back up stored procedures, views, and triggers. The backup utility ignores them and, therefore, they cannot be restored.

➤ *To back up databases:*

1. Go to the **Websites & Domains** tab > **Backup Manager** > **Database Backup Repository**.
2. Using the **Database** menu, select the databases you want to back up.
3. Click **Back Up**.
4. Specify the name of the backup file and click **OK**.
5. If you want to download the resulting backup file, click the file name on the next page after the backup process was finished. Specify the location where you want to save the file and click **Save**.
6. Click **OK**.

➤ *To restore a database:*

1. Log in to Control Panel.
2. Go to **Websites & Domains** tab > **Backup Manager** > **Database Backup Repository**, select the checkbox corresponding to the backup file you want to restore and click **Restore**.

If you do not have the backup file on your server, you can upload the backup file to the server repository from your local machine.

3. Confirm the restoration by selecting the corresponding checkbox and click **OK**.

➤ ***To upload a backup file to a backup repository:***

1. Go to Control Panel > **Websites & Domains** tab > **Backup Manager** > **Database Backup Repository**, and click **Upload Backup File**.
2. In the **Database name** menu, select the database in whose repository you want to upload the backup file.
3. Click **Browse...** and select the required backup file.
4. Leave the **Restore database backup immediately upon uploading** check box selected if you want the database contents to be restored immediately after the backup file is uploaded.
5. Click **OK**.

The database backup file will be uploaded to the backup repository of the specified database.

Scheduling Backups

➤ ***To schedule backing up of data:***

1. Go to the **Account** tab > **Back Up My Account and Websites** > **Scheduled Backup Settings**.
2. Select the **Activate this backup task** checkbox and specify the following:
 - When and how often to run the backup.
 - A prefix that should be added to the backup file name.
 - Splitting of the backup file. To create a multivolume backup, select the respective checkbox and specify volume size in megabytes. Note that volume size cannot exceed 4095 megabytes.
 - Location where to store the backup file. Select the repository where you would like to store the backup file.
 - Maximum number of backup files stored in the repository. Type a number if you want to recycle backup files: When this limit is reached, the oldest backup files are removed.
 - E-mail notification on backing up errors. If you want to send an e-mail notice when something goes wrong during backing up, type the e-mail address you need.
 - What data to back up. You can back up only account settings, or account settings and all related data.
 - **Suspend domains until backup task is completed**. Select this option to prohibit users from making changes to content or settings of websites while they are being backed up.
3. Click **OK**.

Managing Backup Files

Next in this section:

Uploading and Downloading Backup Files.....	554
Uploading and Downloading Database Backup Files (Windows).....	555

Uploading and Downloading Backup Files

Downloading Backup Files from Panel

To download a backup file from the Panel repository, choose the corresponding backup file name in **Account** tab > **Back Up My Account and Websites** and specify the location for the file. Before starting the download, Panel will prompt you to enter the backup password.

Uploading Backup Files to Panel

To upload a backup file to the Panel repository, use the **Account** tab > **Back Up My Account and Websites** > **Upload Files to Server Repository** wizard. Before starting the upload, Panel will prompt you to enter the following backup parameters:

- *Backup file location.*
- *Password.*
This is the password that you used for protecting the backup data. If you did not use password-protection, leave the corresponding field blank.

Note: If the password you provide is incorrect, Panel will warn you, but will upload the backup to the server anyway. During the backup restoration, you will be prompted to enter the password again.

Removing Backup Files

To remove a backup file from the Panel repository, select a checkbox corresponding to the backup file you want to remove in **Account** tab > **Back Up My Account and Websites** and click **Remove**.


Uploading and Downloading Database Backup Files (Windows)

➤ *To upload a backup file to backup repository:*

1. Go to the **Websites & Domains** tab > **Backup Manager** > **Database Backup Repository** and click **Upload Backup File**.
2. Select the database in whose repository you want to upload the backup file to in the **Database name** menu.
3. Click **Browse...** and select the required backup file.
4. Leave the **Restore database backup immediately upon uploading** checkbox selected if you want the database contents to be restored immediately after the backup file is uploaded.
5. Click **OK**.

The database backup file will be uploaded to the backup repository of the specified database.

➤ *To download a backup file from backup repository:*

1. Go to the **Websites & Domains** tab > **Backup Manager** > **Database Backup Repository**.
2. In the **Database** menu, select the database whose backup files you want to browse. Leave **All domain databases** selected if you want to browse backup files of all databases on a domain.
3. Click the icon  corresponding to the database backup file you want to download.
4. Select the location where you want to save the backup file and click **Save**.

The backup file will be downloaded from the backup repository.

➤ *To remove a backup file from backup repository:*

1. Go to the **Websites & Domains** tab > **Backup Manager** > **Database Backup Repository**.
2. In the **Database** menu, select the database whose backup files you want to remove. Leave **All domain databases** selected if you want to browse backup files of all databases on a domain.
3. Select a checkbox corresponding to the database backup file you want to remove. Click **Remove**, confirm removal and click **OK**.

Restoring Data

Next in this section:

Restoring Backups	556
Restoring Databases (Windows)	557

Restoring Backups

You can restore data from backup files kept in:

- *The Panel internal repository.*
To restore backup files from Panel repository, choose the backup file name you want to restore on the **Account** tab > **Back Up My Account and Websites** > **Server Repository** tab.
- *An external FTP repository.*
To restore backup files from Panel repository, choose the backup file name you want to restore on the **Account** tab > **Back Up My Account and Websites** > **Personal FTP Repository** tab.

After you choose the backup file, Panel will start the restoration wizard. You will be prompted to specify the following restoration parameters:

- **Types of data to be restored.**
- **Suspend website until restoration task is completed.** Select this if you want to avoid possible conflicts that may occur when users modify site content or settings while they are being restored.
- **Send an e-mail notice when restoration task is completed.** Type your e-mail address if you want the control panel to notify you when restoring is completed.
- **Conflicts resolution policy.** Specify what to do if any conflicts occur during restoration.
- **Backup security settings.** If the backup was protected with a password, enter the password into the **Password** field. Note that Panel is unable to check whether the password you enter is wrong: The backup will be successfully restored but the data will be corrupted. If you wish to reset user passwords, clear the **Provide the passwords** option.

If any errors or conflicts occur during restoration of data, the wizard will prompt you to select an appropriate resolution. Follow the instructions provided on the screen to complete the wizard.

Restoring Databases (Windows)

➤ ***If the database already exists and you only need to restore its contents:***

1. Go to the **Websites & Domains** tab > **Backup Manager** > **Database Backup Repository**.
2. Select the required backup file from the list and click **Restore Selected**.

If you do not have the backup file on the server, you can upload the backup file to the server repository from your local machine. For more information, refer to the section **Uploading, Downloading, and Removing Database Backup Files**.

3. Confirm the restoration by selecting the corresponding checkbox and click **OK**.

If you are restoring an MS SQL database, there is a possibility that some database users will be orphaned. In order to provide the ability to access and use the database for these users, you need to repair them. For more information, refer to the section **Recovering Orphaned Database Users**.

Next in this section:

Post-Restoration Database Repair..... 557

Post-Restoration Database Repair

If you are restoring an MS SQL database, there is a possibility that some database users will be orphaned. In order to provide the ability to access and use the database for these users, you need to repair them.

➤ ***To check if a database has orphaned users and to repair them:***

1. Go to **Websites & Domains** tab > **Databases** > **database name**.
2. If you see a warning saying that there are several orphaned users that should be repaired in order to function properly, you have orphaned users who need to be repaired.
3. To repair orphaned users, click the **Repair now** button corresponding to the users you want to repair.
4. Provide password for the users and click **Repair**.

If a user is supposed to be a system user without a password, run repair with empty password field.

Appendix A: Properties of Hosting Plans and Subscriptions

Properties of a hosting plan and subscription are grouped as follows:

- **Resources**

These are hosting resources provided with a plan. Includes validity period, policy on overusing resources, system resources like disk space and traffic, and service resources like websites, subdomains, mailboxes, databases and so on. For example, the Domains resources sets the number of domains that a customer can register and manage in Panel.

- **Permissions**

Includes provided services and privileges.

Note: Some permissions prevent settings of the following services from syncing (on page 306). See the details in the **Permissions** section.

- **Hosting Parameters**

Includes parameters of the provided hosting service.

- **PHP Settings**

Includes the customizable PHP settings.

- **Web Server** (service plan only)

Includes web server configuration settings that are applied to newly created domains.

- **Mail** (service plan only)

Includes parameters of the provided mail service.

- **DNS** (service plan only)

Specifies if the DNS zones of the subscription's domains should be master or slave.

Note: In case the **DNS zone management** privilege is provided, this parameter is not synced, and subscribers can set up this parameter on a per-domain basis.

- **Performance** (service plan only)

Includes parameters that affect performance of all services provided with the plan.

- **Logs & Statistics** (service plan only)

Includes the settings of how statistics and logs of a plan's subscriptions should be stored. Note that these settings are not synced between a plan and subscriptions. See **Logs & Statistics** (on page 574) for details on how to change some of these settings for subscriptions.

- **Applications**

Lets you select which applications should be available to subscribers.

Next in this section:

Visibility of Hosting Features in the Control Panel	560
Resources	560
Permissions.....	564
Hosting Parameters.....	568
Web Server (Apache).....	571
Mail	572
DNS	573
Performance.....	573
Logs & Statistics.....	574
Applications.....	574
Additional Services	574

Visibility of Hosting Features in the Control Panel

Since version 10.4, Panel hides from customers those hosting features that are not provided in their subscription. The visibility of GUI elements responsible for a certain feature is determined by permissions and resource limits of a subscription. Note that when you (as the administrator) log in to the customer's Control Panel, you see GUI elements regardless of customer's permissions. The table below explains GUI visibility logic.

	Visible to a Customer	Visible to the Administrator
Resource Limit > 0 Permission = True	Yes	Yes
Resource Limit > 0 Permission = False	No	Yes
Resource Limit = 0 Permission = True	No	No
Resource Limit = 0 Permission = False	No	No

For example, when the number of **Domains** in a subscription is 10 and the **Domains management** permission is off, a customer does not see the **Add New Domain** button in the Control Panel. Nevertheless, this button is available to the administrator that logs in to the customer's Control Panel.

Resources Without Numerical Limits

If the resource type is logical or in other words, it can be just switched on or off (such as scripting language support), its visibility is controlled by a certain permission only. For example, if the **Hosting settings management** permission is granted, a customer is able to toggle the support of various scripting languages for their site. If the permission is not granted, the customer sees the list of languages that are switched on for their site in the read only mode. The disabled languages *are not shown* in the list.

Resources

Resources (located at **Service Plans** > select a plan > **Resources** tab) define what system resources are provided with the subscription.

Overuse policy

Defines what happens if the subscription's usage of disk space and traffic reaches limit values:

- **Overuse is not allowed** will suspend the subscription only if you select the checkbox **Suspend subscription when its disk space or traffic usage goes beyond the limit**. If you do not select it, websites will not be suspended; only a notice will be sent to the subscribers.
You can set up sending of notifications as soon as usage of disk space or traffic reaches a particular value (the **Notify upon reaching** options), in order to prevent subscriptions from suspension. The notifications will be sent according to the server notifications policy.
- **Overuse is allowed** will let the subscription operate properly.
The option **When limit on usage of a resource is reached, send e-mail according to the server notification settings** triggers sending notifications according to the server notifications policy.

Note: The overuse policy does not apply to the limits set on size of mailboxes. Therefore, even if you enable overuse, be sure to allocate enough disk space to mailboxes.

Disk space

The total amount of disk space allocated to the subscription. It includes disk space occupied by all files related to the subscription: content of websites, databases, applications, mailboxes, log files, and backup files.

Traffic

The amount of data that can be transferred from the subscription's websites and FTP/Samba shares during a month.

Notify upon reaching

Available only if overuse is not allowed. This sets the soft quota for disk space or traffic usage in order to prevent subscriptions from suspension. When the quota is reached, the Panel sends notifications to users' e-mail addresses specified in **Settings** > **Notifications: Resource usage limits exceeded by subscription**.

Sites published with Presence Builder

The number of websites that can be published with Presence Builder.

Domains

The total number of domain names that the subscriber will be able to host within the subscription. This includes websites, web forwarding configurations that point to websites hosted on other servers, and domain names on which a website or web forwarding is not yet set up (domains with no hosting).

Mobile sites

The total number of websites that can be hosted with the UNITY Mobile online service, which optimizes sites for viewing on mobile devices. UNITY Mobile hosts the optimized site copies on their own servers.

How it works:

1. A user creates a website with the domain name `example.com` and clicks the link **Create Mobile Site** in the Control Panel.
2. The user is prompted to specify a domain name for access to the mobile site copy. The user specifies `mobile.example.com`.
3. The Panel connects to the UNITY Mobile hosting servers, sets up an account with UNITY Mobile for the domain name `mobile.example.com`.
4. The user's browser opens the UNITY Mobile website, where the user is automatically logged in to their account and prompted to import their website from the Panel-managed server.
5. After the site is imported and optimized for mobile viewing, it becomes accessible by the address `mobile.example.com`. The Panel's DNS server keeps a CNAME record pointing to the site on a UNITY Mobile server.

The user can now perform the following operations on mobile site using links in the Control Panel:

- Open site editor.
- Change mobile site name.
- Remove mobile site.

For more information about UNITY Mobile services, visit their website at <http://www.unitymobile.com>.

For instructions on managing mobile sites through the Control Panel, refer to the **Customer's Guide**, section **Setting Up Mobile Sites**.

Subdomains

The total number of subdomains that the subscriber will be able to host within the subscription.

Domain aliases

The total number of additional alternative domain names that the subscriber will be able to use for their websites.

Mailboxes

The total number of mailboxes that the subscriber can host within the subscription.

Mailbox size

The amount of disk space that is allocated to each mailbox in a subscription for storing e-mail messages and auto-reply attachment files.

Total mailboxes quota (available only for Windows hosting)

The total amount of disk space in megabytes available for all mailboxes within the subscription.

Mailing lists

The total number of mailing lists that the subscriber can host within the subscription.

Additional FTP accounts

The maximum number of FTP accounts used to access the files and folders created within a subscription. This number does not include an account that is always created during the subscription creation.

Databases (Unix hosting)

The total number of databases that can be created on the Panel database servers and used by the subscription's websites.

MySQL databases and Microsoft SQL Server databases (Windows hosting)

The maximum number of MySQL and Microsoft SQL Server databases respectively that can be created on the Panel database servers and used by the subscription's websites.

MySQL databases quota and Microsoft SQL databases quota (Windows hosting)

The maximum amount of disk space (in megabytes) that the subscription's MySQL or Microsoft SQL Server databases can occupy respectively.

Validity period/Expiration Date

The term for a subscription.

In service plan properties, it is **Validity period**: it is used only when a subscription is created: the Panel derives the subscription expiration date from it.

In subscription properties, it is **Expiration date**: At this date, the subscription will be suspended, meaning that all sites within the subscription will be suspended, their Web, FTP and mail services will no longer be accessible to the Internet users, and the subscriber and their users will not be able to log in to the Control Panel.

Subscriptions are not renewed automatically, so to bring a subscription's services back to operation, you will need to manually activate the subscription.

Java applications

The total number of Java applications that can be hosted on the subscription's websites.

Web users

The total number of personal Web pages that the subscriber can host for other users under their websites. This service is mostly used in educational institutions that host non-commercial personal pages of their students and staff. These pages usually have addresses like `http://example.com/~webuser`.

FrontPage accounts (Windows hosting)

The maximum number of Microsoft FrontPage accounts that the subscriber can create within the subscription.

Shared SSL links (Windows hosting)

The total number of shared SSL links that the subscriber can use within the subscription.

ODBC connections (Windows hosting)

The total number of ODBC connections that the subscriber can use within the subscription.

ColdFusion DSN connections (Windows hosting)

The total number of ColdFusion DSN connections that the subscriber can use within the subscription.

Permissions

Permissions (located at **Service Plans** > select a plan > **Permissions** tab) define what privileges and services are provided with the subscription.

DNS zone management

Allows the subscriber to manage the DNS zones of their domains.

Note: If this permission is granted, then the DNS service settings are not synced.

Hosting settings management

Allows modifying parameters of the hosting service provided with the subscription: changing hosting account features, setting up custom web server settings, and switching on or off support for programming and scripting languages, custom error documents, SSL support, and (Windows only) Microsoft FrontPage support. In addition, it allows you to toggle the following permissions: **Hosting performance settings management** and **Common PHP settings management**.

Note: If this permission is granted, then the mentioned hosting parameters are not synced.

Common PHP settings management

Allows the subscriber to adjust common PHP settings individually for each website (subdomain) in their subscription.

Note: If this permission is granted, then the common PHP settings are not synced.

Setup of potentially insecure web scripting options that override provider's policy. Allows the subscriber to override the hosting security policy, if it is applied by the provider.

Management of access to server over SSH (Linux hosting)

Allows the subscriber to access the server shell over SSH under their system user account. Also, lets the subscriber set up such hosting parameter as **SSH access to server shell under the subscription's system user**.

Note: If this permission is granted, then the mentioned hosting parameter is not synced.

Management of access to server over Remote Desktop (Windows hosting)

Allows the subscriber to access the server via Remote Desktop protocol.

Anonymous FTP management

Provides the anonymous FTP service, which lets the subscriber set up a directory shared over FTP protocol and available to anonymous users. A subscription should reside on a dedicated IP address in order to provide this service.

Scheduler management

Allows the subscriber to schedule running of scripts or utilities.

Spam filter management

Lets the subscriber customize filtering settings of the SpamAssassin spam filter.

Antivirus management

Allows the subscriber to change settings of the server-side protection of incoming and outgoing mail from viruses.

Data backup and restoration using the server repository

Allows the subscriber to back up and restore their websites, and use the storage on the server for keeping backups.

Data backup and restoration using a personal FTP repository

Allows the subscriber to back up and restore their websites, and use external FTP servers for storing their backups.

Web statistics management

Allows the subscriber to select which Web statistics engine should be used, and whether reports should be accessible via a specific password-protected directory.

Note: If this permission is granted, then the mentioned hosting parameter is not synced.

Log rotation management

Allows the subscriber to adjust the cleanup of processed log files for their sites. Also, allows the subscriber to remove log files.

Note: If this permission is granted, then the **Logs & Statistics** parameters (on page 574) are not synced.

Access to Application Catalog

Provides the subscriber with access to prepackaged applications that can be installed on websites. If you select this option, be sure to select the **PHP support** checkbox on the **Hosting Parameters** tab.

You can view a list of applications available from your provider by doing the following:

1. Set up your own website by using a plan or a custom subscription that grants access to the Application Catalog.
2. Go to the Server Administration Panel > **Subscriptions**, and click the **Manage Hosting** link corresponding to your domain name. The Control Panel will open in a new browser window or tab.
3. In the Control Panel, go to the **Applications** tab > **All Available Applications**.

There is also a page in the Server Administration Panel, where you can view and update installed applications, and purchase license keys for commercial applications at Parallels Online Store: **Tools & Utilities** > **Application Vault**.

For instructions on installing applications and license keys, refer to the **Customer's Guide**, section **Using Website Applications**.

Domains management

Allows the subscriber to add domains, create websites and set up web forwarding.

Subdomains management

Allows the subscriber to set up additional websites accessible by `<subdomain>.<domain>` addresses.

Domain aliases management

Allows the subscriber to set up additional alternative domain names for their websites.

Additional FTP accounts management

Allows the subscriber to manage FTP accounts for accessing the subscription's files and folders.

Java applications management

Allows the subscriber to install Java applications on their websites.

Mailing lists management

Allows the subscriber to use mailing lists provided by the GNU Mailman software.

Note: If this permission is granted, then the **Enable mailing lists** parameter (on page 572) is not synced.

Hosting performance settings management

Allows the subscriber to adjust performance PHP settings individually for each website (subdomain) in their subscription. In addition, lets the subscriber set up the limits on bandwidth usage and number of connections to their websites.

Note: If this permission is granted, then the following settings are not synced: PHP performance settings, **performance** settings (on page 573) for bandwidth usage and the number of connections.

IIS application pool management (Windows hosting)

Provides the subscriber with a dedicated IIS application pool and the means to manage it: enable or disable it, and set up the maximum amount of CPU power that the pool may use.

Note: If this permission is granted, then the **Logs & Statistics** parameter (on page 574) called **Use dedicated pool** is not synced.

Additional write/modify permissions management (Windows hosting)

Allows the subscriber to toggle the hosting parameter **Additional write/modify permissions**. These permissions are required if a subscriber's web applications use a file-based database (like Jet) located in the root of `httpdocs` folder. Please note that selecting this option might seriously compromise the websites' security.

Note: If this permission is granted, then the hosting parameter **Additional write/modify permissions** is not synced.

Shared SSL management (Windows hosting)

Provides the shared SSL service, and allows the subscriber to set up shared SSL links for their websites within the subscription.

Hard disk quota assignment

Allows the subscriber to set up the hosting parameter **Hard disk quota**.

Note: If this permission is granted, then the mentioned hosting parameter is not synced.

Database server selection

Allows subscribers to select a database server for their databases, as opposed to using the default database server. For details about default database servers, see the section **Hosting Parameters** (on page 568).

Access to advanced operations: Website Copying and Website Maintenance Mode

Specifies whether the website copying and maintenance mode are available to the subscriber in the **Control Panel > Websites & Domains > Show Advanced Operations**. If denied, the **Website Copying** and **Website Maintenance Mode** links are not available to the subscriber.

Password-protected directories management

Specifies whether the protected directories feature is available to the subscriber in the **Control Panel > Websites & Domains > Show Advanced Operations**. If denied, the **Password-protected directories** link is not available to the subscriber.

Ability to manage auxiliary user accounts

Specifies whether the subscriber can manage auxiliary user accounts on the **Control Panel > Users** tab. If denied, the **Users** tab is not available to the subscriber.

Allow activating APS apps using license keys from the Panel license pool

If granted, users will be able to install certain APS apps without the need to purchase app licenses from vendors. In this case, app license keys will be taken from the Panel license pool. Note that you cannot limit the number of app installations a user is allowed to perform. This permission is relevant only if your Panel license comes in a bundle with APS app licenses. Learn more about license bundles (on page 139).

Hosting Parameters

These parameters define the hosting service provided with the plan or subscription. The parameters can be found in:

- **Service Plans** > select a plan > **Hosting Parameters** tab
- **Subscriptions** > select a subscription > **Customize** > **Hosting Parameters** tab

Note: Unless specifically noted, the parameters are not synced if the **Hosting management** permission is granted to a subscription.

Enable hosting

Defines whether the hosting service is actually provided with the plan.

Turn off this option to make up a service plan that provides only mail service. Subscribers of such a plan will be able to have 'domains without hosting' which will serve mailboxes.

Status of websites in suspended subscriptions

Defines whether sites in suspended subscriptions should be available over the Internet and which hosting services should be available for these sites.

In Panel, a website can receive a new status in two ways:

- When the site owner or hosting provider changes the status individually for the site (in **Websites & Domains > Edit > Change status**). As long as the subscription stays *active*, services like mail are available for sites with any status, and these services can be managed by means of Panel. Learn more in **Website Status** (on page 400).

- After the subscription has been *suspended*. It can be suspended automatically (when its expiration date passes) or manually by the hosting provider (using the **Suspend** button in the subscription's settings). The DNS and mail services are available for sites in suspended subscriptions, but cannot be managed by means of Panel.

The setting **Status of websites in suspended subscriptions** enables you to specify the status that websites will receive when their subscription becomes suspended.

Websites in suspended subscriptions can have the following statuses:

- **Disabled.** Disabled websites have all associated hosting services disabled. Visitors see the *web server's default page* defined by the hosting provider.
Disabled websites are no longer hosted on the server: They are excluded from the web server configuration. However, the physical directories and files of disabled websites can be accessed using FTP clients and File Manager.

Important: In Panel versions earlier than 11.5 this status was called **Suspended**. After upgrading from earlier Panel versions to 11.5, all websites that had the *Suspended* status will receive the status *Disabled* in order to keep their correct behavior.

- **Suspended.** Suspended websites do not open in browsers. Visitors are redirected with the search engine friendly 503 HTTP code to the custom *maintenance page*.

Note: You can customize the maintenance page by using the **Edit maintenance error page** link in **Control Panel > Websites & Domains > domain name**. This link is displayed only if you select the **Custom error documents** checkbox in the site settings in **Websites & Domains > domain name > Edit**. Site owners can edit the maintenance page too.

Suspended websites remain hosted on the server, which means that the services such as mail are running and web server configuration for these websites is kept on the server.

- **Active.** The website works as usual.

Hard disk quota

Hard quota imposed on disk space in addition to the soft quota (set with the option **Notify upon reaching** (on page 560)). Hard disk quota will not allow writing more files to the web space when the limit is reached: users will get an "Out of disk space" error at an attempt to write files.

Note: (Linux hosting) Confirm that your operating system supports hard disk quota before you set any value other than **Unlimited**. In case you define a hard quota when it is not supported, you will get a synchronization conflict on all the plan's subscriptions.

SSL support

Allows setting up SSL encryption on websites hosted within the subscription.

Web statistics

Selects a statistics engine that will create reports on how the subscription's websites are visited: how many people visited a site, and which web pages they viewed.

The **accessible via password protected directory /plesk-stat/webstat** option allows a subscriber view website statistics at URLs like <https://example.com/plesk-stat/webstat> using their system user account login and password.

Note: This parameter is not synced if the **Web statistics management** permission is selected.

Custom error documents

Allows subscribers to design and use their own error pages that the web server returns with HTTP error codes.

SSH access to server shell under the subscription's system user (Linux/Unix hosting)

Allows subscribers to upload securely web content to the server through SSH.

Note: This parameter is not synced if the **Management of access to server over SSH** permission is selected.

Scripting

Support for programming and scripting languages that should be interpreted, executed or otherwise processed by a web server: Microsoft ASP.NET framework, PHP hypertext preprocessor (PHP), Common Gateway Interface (CGI), Perl, Python, Fast Common Gateway Interface (FastCGI), Microsoft or Apache Active Server Pages (ASP), Server Side Includes (SSI), ColdFusion, and Miva scripting required for running Miva e-commerce solutions.

To learn more about adjustable PHP settings, see the section **PHP Settings** (on page 571).

Additional write/modify permissions (Windows hosting)

This option is required if subscriber's web applications use a file-based database (like Jet) located in the root of `httpdocs` folder. Please note that selecting this option might seriously compromise the Web site security.

Allow web users to use scripts

Allows scripting at web pages available at URLs like `http://example.com/~<username>/<webpage>`, where `<username>` refers to a web user.

Web users are individuals who do not need their own domain names. This service is popular with educational institutions that host non-commercial personal pages of their students and staff.

FrontPage support (Windows hosting).

The options in the **FrontPage support** group allow subscribers to connect to the server and create websites with Microsoft Frontpage.

Default Database Server

Specifies default database servers of each supported type to be used within a plan. Customers will be able to create databases *only* on the default database servers. Note that if you disable a database server for an existing plan or subscription (the **None** option), the databases already used by customers will still be accessible.

Next in this section:

PHP Settings..... 571

PHP Settings

You can adjust the following PHP settings on the **Service Plans** > select a plan > **Hosting Parameters** tab:

- **PHP handler type.**
Learn how to choose the PHP handler that suits you best in the section **PHP Handlers** (on page 52).
- **PHP version.**

Since Panel 10.4, you can adjust PHP configuration individually for each hosting plan or subscription. For this purpose, Panel exposes a number of PHP configuration settings on the **PHP Settings** tab. To learn more about custom per-subscription PHP configuration, refer to the section **Custom PHP Configuration** (on page 54).

Web Server (Apache)

Web server settings (located at **Service Plans** > select a plan > **Web Server** tab) enable you to predefine web server configuration for all domains that will be created under a certain service plan.

Note: Web server settings can also be changed for each domain individually. Changes on the service plan level do not override custom settings of existing domains. Therefore, the changes you make in **Service Plans** > select a plan > **Web Server** take effect only for newly created domains.

To learn more about web server configuration, see **Apache Web Server (Linux)** (on page 28).

Directives for HTTP and Directives for HTTPS

To predefine Apache directives that will be used when the website is accessed over HTTP and HTTPS, use the **Directives for HTTP** and **Directives for HTTPS** fields. When editing the fields, use the syntax as in `httpd.conf`. For example, if you want to set a custom error page, add the line:

```
ErrorDocument 401 /my_error_page.html
```

nginx directives

To predefine nginx directives, use the **nginx directives** field. When editing the field, use the syntax as in `nginx.conf`. For example, if you want to pack all the proxied requests with gzip, add the line:

```
gzip_proxied any;
```

Mail

These parameters (located at **Service Plans** > select a plan > **Mail** tab) define the mail service provided with the plan.

Webmail

Provides the webmail service, which allows users of mailboxes within the subscription to work with their mail using a web-based mail application.

Enable mailing lists

Turns on the mailing lists service provided by the GNU Mailman software on the subscription's websites.

Note: This parameter is not synced if the permission **Mailing lists management** is selected.

Policy on mail for non-existent users

Defines how mail server should treat e-mail messages sent to e-mail addresses that are supposed to be registered under the subscription's domains but actually do not exist. The following options are available:

- **Bounce with message** returns the mail back to sender with a notice.
- **Forward to address** forwards the mail to another e-mail address.
- **Reject** silently rejects the mail without accepting it. This setting can decrease mail server load caused by a large amount of spam, which is often directed at randomly generated user names. However, this might be useful to spammers because scanning your mail server for valid e-mail addresses will speed up in such a case.
- **Redirect to external mail server with IP address** (on Windows hosting), forwards the mail to the specified mail server.

DNS

These parameters (located at **Service Plans** > select a plan > **DNS** tab) define how the DNS service running on the Panel-managed server will serve DNS zones for websites hosted on the plan.

Master

A master or primary name server stores locally the zone file it serves, while a secondary server only retrieves a copy of this file from the primary.

Slave

A slave or secondary server retrieves a copy of the zone file from the primary name server.

Performance

These system parameters (located at **Service Plans** > select a plan > **Performance** tab) define performance of all services provided with the plan.

Use dedicated IIS application pool (Windows hosting)

Enables the use of dedicated IIS application pool for web applications within the subscription. Using dedicated IIS application pool dramatically improves the stability of web applications due to worker process isolation mode. This mode gives each site hosted on the server a possibility to allocate a separate process pool for execution of its web applications. This way, malfunction in one application will not cause stopping of all the others. This is especially useful when you are using shared hosting package. The **Maximum CPU use (%)** option limits the amount of the server CPU that the pool can use.

Maximum bandwidth usage

Defines the maximum speed (measured in KB per second) that a domain can share between all its connections.

Connections limited to

Defines the maximum number of simultaneous connections to web server for all websites within the subscription. This setting is intended for preventing the websites from Denial of Service (DOS) attacks and excessive usage of bandwidth.

Logs & Statistics

These parameters (located at **Service Plans** > select a plan > **Logs & Statistics** tab) define how statistics and logs of a subscription should be stored.

Note: These settings in subscriptions are not synchronized with service plans.

Retain web and traffic statistics

Sets a period (in months) for which reports on the subscription's web statistics (generated by the selected web statistics component) and traffic statistics (generated by Panel) should be available.

Note: The setting **Retain web and traffic statistics** is not changed in subscriptions when you update it for a service plan. The only way to update this setting for each domain is changing it in the Panel database. See <http://kb.parallels.com/en/6246> for details.

Log rotation

Enables automatic cleanup and recycling of web server log files. You can also switch on compression of processed log files and sending them to a specific e-mail address.

Applications

Depending on the service plan, a number of prepackaged applications can be available to Panel users. You can install the apps on your own sites as well as provision them to your customers.

When setting up a hosting plan, you can select which of the apps should be provisioned to customers:

- To provide all available applications, on the **Permissions** tab, select the option **Access to Application Catalog**.
- To provide only selected applications, on the **Permissions** tab, select the option **Access to Application Catalog**, and then go to the **Applications** tab and select the option **Provide only applications that I select**. Use the button >> to add the selected applications to the plan.

Additional Services

If your provider configured Panel to provide custom additional services, then the **Additional Services** tab is shown in hosting plan properties. On this tab, you can select the services that you want to provide to subscribers.

Appendix B: Properties of Reseller Plans and Subscriptions

Properties of a reseller plan are grouped as follows:

- **Resources**
Includes policy on overusing and overselling of resources, the number of customer accounts a reseller can create, system resources like disk space and traffic, and service resources like websites, subdomains, mailboxes, databases, and so on.
- **Permissions**
Reseller permissions either denote the operations available to a reseller in the Panel, or define which services and privileges can be enabled in the service subscriptions of the reseller's customers. If a particular permission in a reseller subscription is Off, then a service subscription will not provide the corresponding service or a privilege. A disabled permission also means that a reseller is prohibited to perform the designated action in Control Panel. For example, if a reseller subscription does not provide a privilege to use Scheduler (**Scheduler management is Off**), then none of the reseller's subscribers will be able to use it, and neither will the reseller themselves when they go to the Control Panel.
- **IP addresses**
Defines IP addresses that will be allocated to resellers. It is important that a reseller has at least one IP address allocated to them, otherwise, they will not be able to create a single service subscription.
- **Applications**
Enables you to select the applications that will be available to subscribers.

Next in this section:

Resources.....	576
Permissions	577
IP Addresses	577
Applications	578

Resources

Overuse policy

Defines what happens to the reseller subscription if the total disk space and traffic usage by the reseller's service subscriptions (own reseller's service subscriptions and those belonging to the reseller's customers) reaches the limit values defined by the reseller plan.

- **Overuse is not allowed** will suspend the reseller subscription and all their customers only if you select the checkbox **Suspend reseller when their disk space or traffic usage goes beyond the limit**. If you do not select it, reseller subscriptions and their customers will not be suspended; only a notice will be sent to recipients specified in **Settings > Notifications: Resource usage limits exceeded by reseller account** option.

You can also set up sending notifications as soon as usage of disk space or traffic reaches a particular value (the **Notify upon reaching** options), in order to prevent subscriptions from suspension. The notifications will be sent to users and/or e-mail addresses specified at **Settings > Notifications: Resource usage limits exceeded by reseller account** option.

- **Overuse is allowed** will let the subscription operate properly.
The option **When limit on usage of a resource is reached, send email according to server notification settings** triggers sending notifications to users and/or e-mail addresses specified at **Settings > Notifications: Resource usage limits exceeded by reseller account** option.

Note: The overuse policy does not apply to the limits set on size of mailboxes. Therefore, even if you enable overuse, be sure to allocate enough disk space to mailboxes.

Overselling policy

Defines whether a reseller can sell more resources than allocated to them with the plan.

If overselling is allowed, a reseller is governed by actual resource usage instead of initial resource allocation. Overselling is a marketing strategy based on the following scheme: a reseller, who was allotted, for example, ten gigabytes of disk space, allocates five gigabytes of disk space for each of their customers, assuming that none of them will actually use all of their allocated disk space.

Customers

Defines the total number of customer accounts that a reseller can create.

Other Resources

Note: Other resources have the same meaning as the ones defined in the hosting plans and subscriptions. The only difference is that a reseller does not use the provided resources directly, but redistributes them by means of service subscriptions they create for their customers or for hosting their own websites.

Permissions

Reseller-specific privileges (the ones that do not affect service subscriptions they create for their customers) are as follows:

Ability to use remote API

Defines if a reseller can remotely manage websites through custom applications. The remote API is an interface that can be used for developing custom applications integrated with websites, which could be used, for instance, for automating setup of hosting accounts and provisioning of services for customers purchasing hosting services from your site. To learn more, refer to the Parallels Plesk Panel API documentation available at the PTN portal (<http://www.parallels.com/ptn/documentation/ppp/>).

Access to the Panel

Defines if a reseller can use the Panel graphical user interface.

Customer account creation

Defines if a reseller can create user accounts and subscriptions for their customers in the Panel.

Allow overselling

Defines if a reseller can set up overselling policy, meaning that a reseller can themselves define if overselling is allowed to them or not.

Other Permissions

Note: Meanings of the other permissions are the same as in the service subscriptions.

IP Addresses

These parameters define IP resources provided with the plan.

Allocate shared IP addresses

Defines shared IP addresses that will be available to a reseller.

Allocate dedicated IPv4 addresses and Allocate dedicated IPv6 addresses

Defines that a specified number of dedicated IP addresses of the corresponding type should be allocated to a reseller. The IPs are provisioned automatically: the required amount is taken from the number of free dedicated IP addresses in your IP pool.

Applications

Depending on the hosting plan, a number of prepackaged applications can be available to Panel users. You can install the apps on your own sites as well as provision them to your customers.

When setting up a hosting plan, you can select which of the apps should be provisioned to customers:

- To provide all available applications, on the **Permissions** tab, select the option **Access to Application Catalog**.
- To provide only selected applications, on the **Permissions** tab, select the option **Access to Application Catalog**, and then go to the **Applications** tab and select the option **Provide only applications that I select**. Use the button >> to add the selected applications to the plan.

Appendix C: Event Parameters Passed by Event Handlers

This section describes the parameters that can be used with handlers that you set up for specific Panel events.

Important: All variables used for passing the parameters on Linux systems must be typed in upper case (for example, `NEW_USERNAME`), and on Windows systems, in lower case (for example, `new_username`).

Next in this section:

Administrator information updated	581
Service stopped.....	581
Service started	581
Service restarted	581
IP address created	581
IP address updated	581
IP address deleted	581
Session settings updated	582
Customer account created.....	582
Customer account updated.....	582
Customer account deleted.....	582
Customer account status updated	583
Customer's interface preferences updated	583
Customer GUID updated	583
Reseller account created.....	583
Reseller account updated.....	584
Reseller account deleted	584
Reseller account status updated.....	584
Reseller's interface preferences updated.....	584
Reseller's IP pool updated.....	584
Disk space limit for reseller account reached.....	584
Traffic limit for reseller account reached	584
Disk space limit for subscription reached.....	585
Traffic limit for subscription reached	585
Default domain (the first domain added to a subscription/webpace) created....	585
Default domain (the first domain added to a subscription/webpace) updated...	586
Default domain (the first domain added to a subscription/webpace) deleted	586
Subscription owner changed	586
Default domain, status updated	586
Default domain, DNS zone updated	586
Default domain, GUID updated.....	586
Subdomain of a default domain created	586
Subdomain of a default domain updated	587

Subdomain of a default domain deleted.....	587
Default domain, alias created	587
Default domain, alias updated	588
Default domain, alias deleted	588
Default domain, alias DNS zone updated	589
Reseller account limits updated	589
Subscription limits updated.....	589
Panel user logged in.....	589
Panel user logged out.....	589
Panel user failed to log in	589
Panel user failed to log in through API.....	589
Mail account created	590
Mail account updated	590
Mail account deleted.....	590
Mailing list created.....	590
Mailing list deleted	591
Hosting settings created	591
Standard or frame forwarding hosting created	592
Hosting settings updated	593
Hosting settings deleted	593
Standard or frame forwarding hosting updated	593
Standard or frame forwarding hosting deleted	593
Web user account created.....	593
Web user account updated.....	594
Web user account deleted	594
Web application installed	594
Web application reconfigured	595
Web application uninstalled	595
Web application upgraded	595
License key updated.....	595
License key expired.....	595
Database server created	596
Database server updated	596
Database server deleted	596
Database created	596
Database deleted	596
Database user account created	597
Database user account updated	597
Database user account deleted	597
Parallels Plesk Panel component updated or added.....	598
Reseller plan created.....	598
Reseller plan updated.....	598
Reseller plan deleted.....	598
Service plan of reseller created	598
Service plan of reseller updated	598
Service plan of reseller deleted	599
Service plan of administrator created	599
Service plan of administrator updated	599
Service plan of administrator deleted.....	599
Additional FTP account created.....	600
Additional FTP account updated.....	600
Additional FTP account deleted	600
Server health status changed	601
Update available.....	601

Update installed..... 601

Administrator information updated

Service stopped

Service started

Service restarted

IP address created

IP address updated

IP address deleted

Parameter name and description	Environment variable name	Notes
IP address	OLD_IP_ADDRESS	Required

Session settings updated

Customer account created

Parameter name and description	Environment variable name	Notes
Login name	NEW_LOGIN_NAME	Required
Password	NEW_PASSWORD	
Contact name	NEW_CONTACT_NAME	Required
Company name	NEW_COMPANY_NAME	
Phone	NEW_PHONE	
Fax	NEW_FAX	
E- mail	NEW_EMAIL	
Address	NEW_ADDRESS	
City	NEW_CITY	
State/province	NEW_STATE_PROVINCE	
Postal/zip code	NEW_POSTAL_ZIP_CODE	
Country	NEW_COUNTRY	

Customer account updated

Customer account deleted

Parameter name and description	Environment variable name	Notes
Login name	OLD_LOGIN_NAME	Required

Customer account status updated

Customer's interface preferences updated

Customer GUID updated

Reseller account created

Parameter name and description	Environment variable name	Notes
Login name	NEW_LOGIN_NAME	Required
Contact name	NEW_CONTACT_NAME	Required
Password	NEW_PASSWORD	
Company name	NEW_COMPANY_NAME	
Phone	NEW_PHONE	
Fax	NEW_FAX	
E- mail	NEW_EMAIL	
Address	NEW_ADDRESS	
City	NEW_CITY	
State/province	NEW_STATE_PROVINCE	
Postal/zip code	NEW_POSTAL_ZIP_CODE	
Country	NEW_COUNTRY	

Reseller account updated

Reseller account deleted

Parameter name and description	Environment variable name	Notes
Login name	OLD_LOGIN_NAME	Required

Reseller account status updated

Reseller's interface preferences updated

Reseller's IP pool updated

Disk space limit for reseller account reached

Parameter name and description	Environment variable name	Notes
Contact name	OLD_CONTACT_NAME	Required
Disk space limit	OLD_MAXIMUM_DISK_SPACE	

Traffic limit for reseller account reached

Parameter name and description	Environment variable name	Notes
Contact name	OLD_CONTACT_NAME	Required
Traffic usage limit	OLD_MAXIMUM_TRAFFIC	

Disk space limit for subscription reached

Parameter name and description	Environment variable name	Notes
Subscription's domain name	OLD_DOMAIN_NAME	Required
Disk space limit	OLD_MAXIMUM_DISK_SPACE	

Traffic limit for subscription reached

Parameter name and description	Environment variable name	Notes
Subscription's domain name	OLD_DOMAIN_NAME	Required
Traffic usage limit	OLD_MAXIMUM_TRAFFIC	

Default domain (the first domain added to a subscription/webospace) created

Parameter name and description	Environment variable name	Notes
Domain name	NEW_DOMAIN_NAME	Required

Default domain (the first domain added to a subscription/webpace) updated

Default domain (the first domain added to a subscription/webpace) deleted

Parameter name and description	Environment variable name	Notes
Domain name	NEW_DOMAIN_NAME	Required

Subscription owner changed

Default domain, status updated

Default domain, DNS zone updated

Default domain, GUID updated

Subdomain of a default domain created

Parameter name and description	Environment variable name	Notes
Subdomain name	NEW_SUBDOMAIN_NAME	Required
Parent domain name	NEW_DOMAIN_NAME	Required
FTP account login	NEW_SYSTEM_USER_TYPE	
Subdomain owner's login name	NEW_SYSTEM_USER	

Hard disk quota	NEW_HARD_DISK_QUOTA	
SSI support	NEW_SSI_SUPPORT	
PHP support	NEW_PHP_SUPPORT	
CGI support	NEW_CGI_SUPPORT	
Perl support	NEW_MOD_PERL_SUPPORT	
Python support	NEW_MOD_PYTHON_SUPPORT	
ColdFusion support	NEW_COLDFUSION_SUPPORT	
Apache ASP support	NEW_APACHE_ASP_SUPPORT	Only on Linux platforms.
ASP support	NEW_ASP_SUPPORT	Only on Windows platforms.
Hard quota on disk space	NEW_HARD_DISK_QUOTA	
Miva scripting support	NEW_MIVA_SUPPORT	
FastCGI support	NEW_MOD_FASTCGI_SUPPORT	
SSL support	NEW_SSL_SUPPORT	

Subdomain of a default domain updated

Subdomain of a default domain deleted

Parameter name and description	Environment variable name	Notes
Parent domain name	OLD_DOMAIN_NAME	Required
Subdomain name	OLD_SUBDOMAIN_NAME	Required

Default domain, alias created

Parameter name and description	Environment variable name	Notes
Domain alias name	NEW_DOMAIN_ALIAS_NAME	Required

Synchronization of DNS zone with a primary domain	NEW_DNS	
Domain alias switched on or off	NEW_STATUS	
Web service for domain alias is on or off	NEW_DOMAIN_ALIAS_WEB	
Mail service for domain alias is on or off	NEW_DOMAIN_ALIAS_MAIL	
Support for accessing web applications in Java for domain alias visitors (on or off)	NEW_DOMAIN_ALIAS_TOMCAT	

Default domain, alias updated

Default domain, alias deleted

Parameter name and description	Environment variable name	Notes
Domain alias name	OLD_DOMAIN_ALIAS_NAME	Required
Domain ID number	OLD_DOMAIN_ID	

Default domain, alias DNS zone updated

Reseller account limits updated

Subscription limits updated

Panel user logged in

Panel user logged out

Panel user failed to log in

Parameter name and description	Environment variable name	Notes
User name	COMP_LOGIN_NAME	

Panel user failed to log in through API

Parameter name and description	Environment variable name	Notes
User name	COMP_LOGIN_NAME	

Mail account created

Parameter name and description	Environment variable name	Notes
E-mail address	NEW_MAILNAME	Required (in the format address@example.com)

Mail account updated

Mail account deleted

Parameter name and description	Environment variable name	Notes
E-mail address	OLD_MAILNAME	Required (in the format address@example.com)

Mailing list created

Parameter name and description	Environment variable name	Notes
Domain name	NEW_DOMAIN_NAME	Required

Mailing list e-mail address	NEW_MAIL_LIST_NAME	Required
Mailing list switched on	NEW_MAIL_LIST_ENABLED	

Mailing list deleted

Parameter name and description	Environment variable name	Notes
Domain name	OLD_DOMAIN_NAME	Required
Mailing list e-mail address	OLD_MAIL_LIST_NAME	Required
Mailing list switched on	OLD_MAIL_LIST_ENABLED	

Hosting settings created

Parameter name and description	Environment variable name	Notes
Domain name	NEW_DOMAIN_NAME	Required
IPv4 address	NEW_IP_ADDRESS	
IPv6 address	NEW_IPV6_ADDRESS	
IP type	NEW_IP_TYPE	
System user's login name	NEW_SYSTEM_USER	
System user's password	NEW_SYSTEM_USER_PASSWORD	
Access to the server over SSH (on Linux systems) or Remote Desktop (on Windows systems)	NEW_SYSTEM_SHELL	
MS FrontPage support	NEW_FP_SUPPORT	
MS FrontPage over SSL support	NEW_FPSSL_SUPPORT	
MS FrontPage authoring	NEW_FP_AUTHORIZING	
MS FrontPage admin login	NEW_FP_ADMIN_LOGIN	

MS FrontPage admin password	NEW_FP_ADMIN_PASSWORD	
SSI support	NEW_SSI_SUPPORT	
PHP support	NEW_PHP_SUPPORT	
CGI support	NEW_CGI_SUPPORT	
Perl support	NEW_MOD_PERL_SUPPORT	
Apache ASP support	NEW_APACHE_ASP_SUPPORT	Only on Linux systems
ASP support	NEW_ASP_SUPPORT	Only on Windows systems
SSL support	NEW_SSL_SUPPORT	
Web statistics program	NEW_WEB_STATISTICS	
Custom error documents	NEW_CUSTOM_ERROR_DOCUMENTS	
Hard quota on disk space	NEW_HARD_DISK_QUOTA	

Standard or frame forwarding hosting created

Parameter name and description	Environment variable name	Notes
Domain name	NEW_DOMAIN_NAME	Required
IPv4 address	NEW_IP_ADDRESS	
IPv6 address	NEW_IPV6_ADDRESS	
Forwarding type	NEW_FORWARDING_TYPE	
URL	NEW_URL	

Hosting settings updated

Hosting settings deleted

Parameter name and description	Environment variable name	Notes
Domain name	OLD_DOMAIN_NAME	Required

Standard or frame forwarding hosting updated

Standard or frame forwarding hosting deleted

Parameter name and description	Environment variable name	Notes
Domain name	OLD_DOMAIN_NAME	Required
Forwarding type	OLD_FORWARDING_TYPE	

Web user account created

Parameter name and description	Environment variable name	Notes
Domain name	NEW_DOMAIN_NAME	Required
Web user name	NEW_WEBUSER_NAME	Required
SSI support	NEW_SSI_SUPPORT	
PHP support	NEW_PHP_SUPPORT	

CGI support	NEW_CGI_SUPPORT	
Perl support	NEW_MOD_PERL_SUPPORT	
Python support	NEW_MOD_PYTHON_SUPPORT	
Apache ASP support	NEW_APACHE_ASP_SUPPORT	Only on Linux systems
ASP support	NEW_ASP_SUPPORT	Only on Windows systems
Hard disk quota	NEW_HARD_DISK_QUOTA	

Web user account updated

Web user account deleted

Parameter name and description	Environment variable name	Notes
Domain name	OLD_DOMAIN_NAME	Required
Web user name	OLD_WEBUSER_NAME	Required

Web application installed

Parameter name and description	Environment variable	Notes
Health monitor parameter (the same value for new and old)	NEW_SITEAPP_NAME	Required
Domain or subdomain	NEW_SITEAPP_DOMAIN_TYPE	Required
URL relative to the domain/subdomain, by which the application is accessible on the Web	NEW_SITEAPP_INSTALL_PREFIX	Required

Web application reconfigured

Web application uninstalled

Parameter name and description	Environment variable	Notes
Health monitor parameter (the same value for new and old)	OLD_SITEAPP_NAME	Required
Domain or subdomain	OLD_SITEAPP_DOMAIN_TYPE	Required
URL relative to the domain/subdomain, by which the application is accessible on the Web	OLD_SITEAPP_INSTALL_PREFIX	Required

Web application upgraded

License key updated

License key expired

Parameter name and description	Environment variable name	Notes
License key number	OLD_LICENSE	Required

Database server created

Parameter name and description	Environment variable name	Notes
Database server's IP address	NEW_DATABASE_SERVER	Required

Database server updated

Database server deleted

Parameter name and description	Environment variable name	Notes
Database server's IP address	OLD_DATABASE_SERVER	Required

Database created

Parameter name and description	Environment variable name	Notes
Database server's IP address	NEW_DATABASE_SERVER	Required
Database name	NEW_DATABASE_NAME	Required

Database deleted

Parameter name and description	Environment variable name	Notes
Database server's IP address	OLD_DATABASE_SERVER	Required
Database name	OLD_DATABASE_NAME	Required

Database user account created

Parameter name and description	Environment variable name	Notes
Database server's IP address	NEW_DATABASE_SERVER	Required
Database identification number	NEW_DATABASE_ID	Required
Database user name	NEW_DATABASE_USER_NAME	Required
Database user password	NEW_DATABASE_USER_PASSWORD	

Database user account updated

Database user account deleted

Parameter name and description	Environment variable name	Notes
Database server's IP address	OLD_DATABASE_SERVER	Required
Database identification number	OLD_DATABASE_ID	Required
Database user name	OLD_DATABASE_USER_NAME	Required
Database user password	OLD_DATABASE_USER_PASSWORD	

Parallels Plesk Panel component updated or added

Reseller plan created

Parameter name and description	Environment variable name	Notes
Reseller plan ID	NEW_TEMPLATE_ID	Required

Reseller plan updated

Reseller plan deleted

Parameter name and description	Environment variable name	Notes
Reseller plan ID	OLD_TEMPLATE_ID	Required

Service plan of reseller created

Parameter name and description	Environment variable name	Notes
Plan ID	NEW_DOMAIN_TEMPLATE	Required

Service plan of reseller updated

Parameter name and description	Environment variable name	Notes
Plan ID	OLD_DOMAIN_TEMPLATE	Required

Service plan of reseller deleted

Parameter name and description	Environment variable name	Notes
Plan ID	OLD_DOMAIN_TEMPLATE	Required

Service plan of administrator created

Parameter name and description	Environment variable name	Notes
Plan ID	NEW_ADMIN_TEMPLATE	Required

Service plan of administrator updated

Parameter name and description	Environment variable name	Notes
Plan ID	OLD_ADMIN_TEMPLATE	Required

Service plan of administrator deleted

Parameter name and description	Environment variable name	Notes
Plan ID	OLD_ADMIN_TEMPLATE	Required

Additional FTP account created

Note: This event is relevant only for additional FTP accounts - the ones that created after the subscription creation in addition to the main account. If you want to track the creation of the main FTP account - the one that is created simultaneously with a subscription, you should use the **Hosting settings created** (on page 591) event.

Parameter name and description	Environment variable name	Notes
Domain name	NEW_DOMAIN_NAME	Required
Home directory	NEW_HOME_DIRECTORY	Required
System user name	NEW_SYSTEM_USER	
System user password	NEW_SYSTEM_USER_PASSWORD	

Additional FTP account updated

Additional FTP account deleted

Parameter name and description	Environment variable name	Notes
Domain name	OLD_DOMAIN_NAME	Required
Home directory	OLD_HOME_DIRECTORY	Required
System user name	OLD_SYSTEM_USER	
System user password	OLD_SYSTEM_USER_PASSWORD	

Server health status changed

Update available

Parameter name and description	Environment variable name	Notes
Update version	COMP_PATCH_VERSION	

Update installed

Parameter name and description	Environment variable name	Notes
Update version	COMP_PATCH_VERSION	