



PLESK 7 RELOADED

ADMINISTRATOR'S MANUAL

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

Linux is a registered trademark of Linus Torvalds. RedHat is a registered trademark of Red Hat Software, Inc. All other trademarks and copyrights are the property of their respective owners.

13800 Coppermine Road, Suite 112, Herndon, VA, 20171 USA, Ph.: 703 815-5670, Fax.: 703 815-5675

Table of Contents

1. About Plesk 7 Reloaded	1
Plesk 7 Reloaded Capabilities	1
Additional Benefits	4
Plesk Interface Specific Features	5
2. Configuring Your System	7
Configuring Access Policy	7
Setting Session Security Parameters	9
Setting System Date and Time	10
Setting Up Server-wide Mail and Spam Filtering	12
Configuring Mailman	17
Enabling ColdFusion Support	18
Setting Up Dr.Web Antivirus Protection	18
Setting Up PostgreSQL Administrator's Account	19
Registering Your Server and Managing Access to Additional Services	20
Managing Control Panel SSL Certificates	22
Setting System-wide Preferences and Logo	28
Tracking User Actions	30
Using Event Manager	31
Enabling E-mail Notification	42
Configuring the Help Desk	45
3. Performing Administrative Tasks	49
Editing Administrator's Information and Password	49
Starting and Stopping Plesk Services	50
Managing Server IP Addresses	51
Managing the DNS Zone Template	55
Managing Client Templates	58
Managing Domain Templates	60
Managing Custom Buttons	64
Managing Skins	65
Managing Virtual Host Skeleton	66
Scheduling Crontab Tasks	67
Scheduling Report Deliveries	69
Using Application Vault	70
Managing User Sessions	74
Operating Help Desk	75
Master Feature	77
Viewing Server Statistics	82
Viewing Information on Plesk Components	83
Submitting a Request for Online Server Support	83
Updating Plesk	84
License Management	85
Rebooting the System	90

Shutting Down the System	90
4. Managing User Accounts	91
Creating a New Client Account	91
Editing Client Information	102
Viewing the Client Report and Statistics	103
Deactivating/Activating a Client Account	106
Performing Group Operations on Accounts	106
Removing Client Accounts	108
5. Administering Domains	109
Creating a Domain	109
Managing Hosting	112
Setting Domain Level Limits	119
Editing Domain Preferences	119
Customizing DNS Settings	120
Managing Mail	124
Managing Mailing Lists	136
Setting Up a Domain User Account	138
Registering a Domain with MPC	139
Accessing Additional Services (Extras)	139
Managing Databases	140
Domain SSL Certificates Repository Management	142
Managing Tomcat Web Applications	149
Managing Web Users	152
Managing Subdomains	154
Managing Protected Directories	155
Managing Anonymous FTP Access	158
Managing Log Files and Log Rotation	159
Using File Manager	161
Using the Domain Application Vault	164
Accessing Site Builder	165
Accessing Microsoft FrontPage Web Administrator	165
Backing Up and Restoring Domains	166
Deactivating/Activating a Domain	168
Performing Group Operations on Domains	169
Removing Domains	171
6. Using Plesk Migration Manager	173
Overview	173
Uploading Migration Agent To Remote Host	173
Viewing Information on Source Host	174
Migrating All Objects	174
Selecting Objects For Migration	175
Stopping Migration	176
A. Plesk Advanced Features	177
Creation Utilities	177
Customizable httpd.include per domain	190
Global access control list in named.conf	190
Chili!Soft ASP support	191

Restoring mail configuration	193
Manageable Tomcat connectors ports	193
B. Glossary of Terms	195

Chapter 1. About Plesk 7 Reloaded

Plesk is a complete hosting automation solution specifically designed to allow quick deployment and simplified management of a Linux based server. It delivers the stability demanded by Hosting Service Professionals while providing the self administration interfaces and end user access for mail, domain, reseller and server level administration.

Plesk auto-installs in minutes and lets non-technical personnel perform a wide variety of administrative tasks — from creating new e-mail accounts to managing entire domains — all with point-and-click simplicity.

The perfect solution for both dedicated server and shared domain management, Plesk deploys and configures all of the systems you need to run a webserver. Tiered login levels provided encrypted and secure access to for system administrators and domain resellers as well as their clients and domain owners. Plesk effectively lowers the threshold for non IT personnel to use, create and manage a Linux based system.

Plesk 7 Reloaded Capabilities

Plesk provides four tiers of administration: admin, client, domain, and mail name user. All can perform various tasks at remote locations via any standard Internet browser. The following capabilities are provided:

- System Management
 - IP addresses management
 - System time setting
 - Server level statistics retrieval
 - Server support request submission
 - License keys management
 - Plesk software updating
 - Power management: hardware reboot and shutdown
- Services Management
 - Manage system services and schedule Crontab tasks
 - Set up server-wide mail limits, mail relay capabilities and mail blockers
 - Enable support for external mail abuse prevention system (MAPS)
 - Enable and configure the integrated SpamAssassin mail filter
 - Enable the server-wide antivirus protection for filtering users' mailboxes.
 - Use the configurable DNS zone templates to simplify further setting up DNS zone records for new domains
 - Manage SSL certificates repository
 - Change the PostgreSQL administrative credentials
 - Add value to the hosting services offered with the Application Vault,

which houses various useful application packages that can be easily deployed on any domain hosted on server.

- Enable support for ColdFusion scripting
- Use skeletons for defining the structure of new virtual hosts
- Control Panel Management
 - Co-brand using company logo and link
 - Download and upload control panel skins.
 - Set up control panel access security and adjust sessions time settings
 - Allow discounted domain registration and SSL certificate purchasing
 - Customize control panel interface appearance, select language, skin, paging options, and add customizable buttons.
 - Adjust the server-wide statistics calculation to meet your requirements
 - Set up the notification system, which will inform you of the ongoing system events
 - Set up system-wide client and domain templates intended to simplify new client account and domain creation procedures with automatic assignment of all necessary restrictions
 - Track various user actions performed within the system
 - Use the Event Manager feature to set up data interchange between Plesk and external systems
- Centralized management of multiple Plesk enabled servers by means of Master feature
- Simplified migration of domains and user accounts from other hosting platforms by means of Migration Manager feature.
- User sessions management
- Integrated Help Desk solution with an easy to use interface
- Additional security measure allowing to restrict access to control panel from certain IPs.
- Client Management
 - Create, edit, and delete client accounts
 - Allow reseller capabilities
 - Set up various limits for client accounts.
 - Retrieve statistics and reports on resource usage
 - Perform group operations on client accounts
- My.Plesk.Com Service Management
 - Manage access to additional server and domain tools purchasing
- Domains and hosting accounts management
 - Create, edit and delete domains and hosting accounts
 - Set up web and ftp server allowances, support for scripting capabilities
 - Set up domain level resource usage limits
 - Manage mail, web and domain user accounts and services
 - Manage DNS zones
 - Backup and restore domain data

- Manage mailing lists
- Handle log files and log rotation
- Operate files and directories using file manager
- Create site content using Site Builder
- Deploy ste applications and java servlets on domains

Additional Benefits

Ease of Use

Plesk users do not need to know the operating system or be a programmer in order to use Plesk. Also, the Plesk software is easy to install. Plesk must be installed on a clean server in one dedicated host. The installation procedure is automated, informing you of system changes and progress at each step. There are no complex commands to learn and no technical information to know.

As soon as Plesk is installed, both administrators and clients are ready to manage the system. Plesk provides great flexibility to the user, enabling him/her to remotely access and administer servers at anytime. The default settings provided for opening accounts and domains can be changed with the click of a button. With Plesk, each client can create his/her own settings and make his/her own adjustments.

Security

Plesk uses extensive security measures to assure your system of the highest possible integrity and protection. It should be noted however that this is limited to Plesk and the software it installs. The security of the server operating system is considered the responsibility of the system administrator and is not part of the Plesk installation and/or setup.

- Plesk uses the secure HTTP (HTTPS) protocol. All documents and communications between users and the server are fully encrypted and secure.
- Plesk provides a free self-signed secure socket layer (SSL) certificate that enables secure transactions between a remote user and Plesk. However, this certificate is not from an "official" authority and will not be recognized by the web browser as being valid for the login URL, which results in warning messages. If you wish to use an authentic SSL certificate for the Control Panel you can. Certificates can be purchased directly through the Plesk control panel or by contacting a certificate-signing authority directly.
- When creating physical hosting with PHP support, you are unable to start an external program from the PHP script. It is impossible to read or write files above the user's home directory.
- There is a possibility of entering different IP-addresses for A domain record and domain hosting address (which is added into web server configuration file) to ensure that the server functions properly behind the firewall.

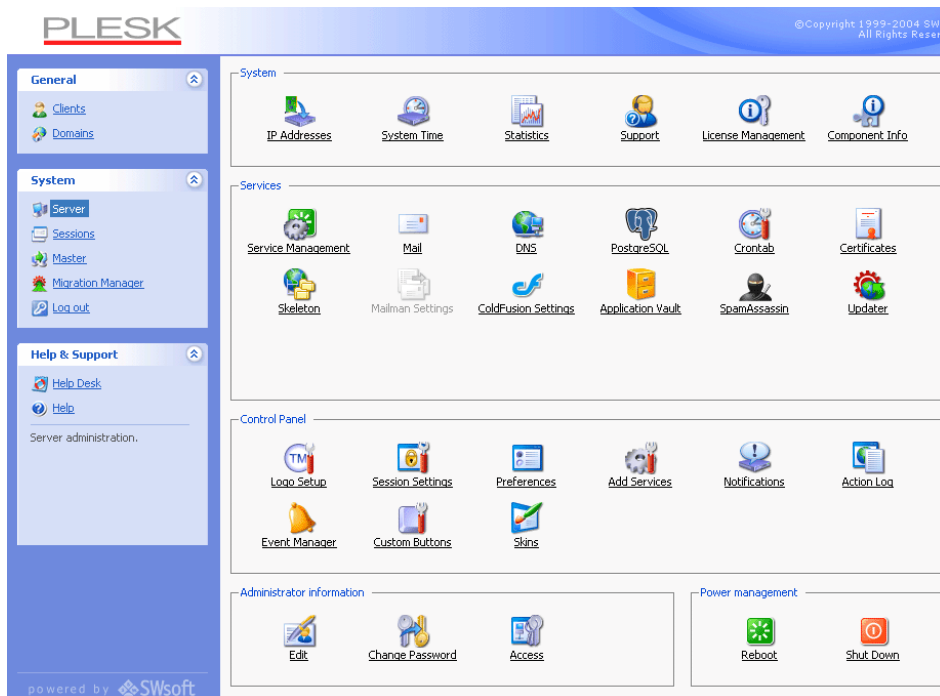
- Plesk provides additional security measures, allowing the administrator to restrict control panel access from certain IP addresses.

Plesk Interface Specific Features

This section focuses on description of the specific features of Plesk web-based interface.

Navigation

The control panel interface is divided into two main parts. The navigation pane occupies the left part. In the right part you can operate particular Plesk component selected from the navigation pane.



- The Clients shortcut opens the list of client accounts, and gives you access to user management functions.
- The Domains shortcut opens the list of domains allowing you to administer them.
- The Server shortcut gives you access to the server administration functions.
- The Sessions shortcut is used for managing currently active user sessions.
- The Master function is used for centralized management of Plesk enabled servers.

- The Migration Manager is a tool that allows migrating user accounts and domains from other hosting platforms.
- The Log out shortcut ends your control panel session.
- The Help Desk shortcut is used for accessing the integrated help desk system.

Pathbar

When you start your Plesk session, the path (chain of links) appears in the right part at the top of the screen. These links reflect your actual “location” within Plesk system. By clicking on the links, you can be one or more (depending on your “location”) levels up.

You can also use the Up Level button located at the upper right corner of the screen to go one level up or return to the previous screen.

Help

The Help shortcut located in the navigation pane provides you with context help. A help page is displayed in a separate window.

Below the Help shortcut is the area displaying a short context help tip. Basically, it provides a brief description of the current screen or operations available. When you hover the mouse pointer over a system element or status icon, it displays the additional information.

Working with Lists of Objects

You may have considerable number of objects within Plesk system. In order to facilitate working with the different lists of objects (for example, Lists of Domains, Client Accounts, etc.), the special tools are provided: Search and Sorting.

To search in a list, enter a search pattern into the Search field, and click Search. All matching items will be displayed in a reduced list. To revert to the entire list of objects, click Show All.

To sort a list by a certain parameter in ascending or descending order, click on the parameter's title in the column heading. The order of sorting will be indicated by a small triangle displayed next to the parameter's title.

Chapter 2. Configuring Your System

After you have installed Plesk software on your server you need to configure your system and set up all services required for its operation. In order to configure your Plesk managed server via the control panel follow the instructions provided in this chapter.

Configuring Access Policy

To alleviate security concerns it is recommended that you use a security measure, allowing to restrict access to control panel with administrator privileges from certain IP's. You can make use of this function by creating a list of IP addresses to which a restriction policy will be applied, two modes are available:

1. Allow access from all IP's except those added to the list.
2. Deny access from IP's, which are not in the list.

Notes on access restriction policies

If the second policy is used, it becomes impossible to remove all records from the list. When you attempt to remove the last record, the restriction policy mode is switched automatically to mode 1.

When you attempt to switch to the mode 2 with empty list, you are warned of impossibility of such action.

You will be informed if access from your IP address becomes unavailable due to your restriction policy misconfiguration.

Managing control panel access

To use the access restriction function, select the Server shortcut in the navigation pane. The Server administration page will open. Click the




Access icon on the Server administration page. The Access restriction management page will open:

Server >

IP Access restriction management Up Level

Tools


Add Network

Preferences

Control panel access with administrator's privileges

Allowed, excluding the networks in the list.
 Denied from the networks that are not listed.

Networks

Networks (1)

IP Address ▲	Subnet Mask	☐
111.111.111.111	255.255.255.0	☐

To add a network to the list:

1. Click the Add Network icon. The Network editing page will open:

Network

Subnet or IP address * . . .

Subnet mask . . .

* Required fields

2. Specify the network IP address and subnet mask, and then click OK.

To remove a network IP from the list, select a corresponding checkbox and click Remove Selected.


To edit a network ip or subnet mask, select the ip address in the list, and you will be taken to the editing page.

To set the policy mode, select the appropriate radio button and click Set. A confirmation box will open, prompting you to confirm the mode change. Click OK.

IMPORTANT

By default Plesk allows multiple simultaneous sessions for several users logged into the control panel using the same login and password combination. This feature might be useful when delegating the 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 sessions expires. Being the administrator you can choose to disable this capability.

To disable multiple sessions, follow these steps:

1. On the Server administration page click  Preferences.
2. Deselect the Allow multiple sessions under administrator's login checkbox.
3. Click OK.

Setting Session Security Parameters

You can set the following parameters for any user session in Plesk:

- **Session idle time:** the allowable idle time for a user session. Should a user session remain idle for a length of time exceeding that specified as the session idle time, Plesk terminates the current session.
- **Invalid login interval:** an interval between two invalid login attempts within which the invalid login attempts counter is increased. If the time between two invalid login attempts exceeds this value, then the invalid login counter is reset back to 0.
- **Invalid login attempts:** the maximum number of invalid login attempts allowed. Once a user has exceeded this value, he/she is locked out for the time specified as the Invalid login lock time.
- **Invalid login lock time:** the lockout time for a user once the invalid login attempts counter has exceeded its maximum limit. Upon completion of the lockout time, the invalid login attempts counter is reset to zero and the user is again given the ability to login to Plesk.

In order to change the session security parameters, follow these steps:

1. Select the  Session Settings icon on the Server administration

page. The Sessions Settings page appears:

Tools



Default

Preferences

Session idle time *	<input type="text" value="30"/>	Minutes
Invalid login interval *	<input type="text" value="3"/>	Minutes
Invalid login attempts *	<input type="text" value="3"/>	
Invalid login lock time *	<input type="text" value="30"/>	Minutes


* Required fields

2. Adjust the settings as desired.
3. Click OK to submit.

To reset the session parameters, click Default.

Setting System Date and Time

You can set manually the server date and time through the interface and enable server time synchronization with the Network Time Protocol (NTP) server. To manage the system date and time settings, follow these steps:

1. Click the  System Time icon on the Server administration page. The

system date and time management page will open:

System Date and Time

Year	<input type="text" value="2004"/>	Hours	<input type="text" value="02"/>
Month	<input type="text" value="07"/>	Minutes	<input type="text" value="53"/>
Day	<input type="text" value="12"/>	Seconds	<input type="text" value="27"/>

Time zone

Your time zone

Synchronize system time

Domain name or IP

2. Edit the time and date settings as desired, and click Set.
3. Select your time zone from the list, and click Set.
4. To synchronize your server time with that of a server running the Network Time Protocol, select the Synchronize system time checkbox. Once this checkbox is checked, this function is enabled.
5. Enter a valid IP address or a domain name and click Set.

i NOTE

Enabling the Synchronize system time function will override any time and date you manually enter in the System Date and Time fields. It is also important to be sure the domain name or IP address you enter for synchronization is a valid NTP server. If not, this function will not work and your server will continue running with its current time settings.

Setting Up Server-wide Mail and Spam Filtering

Configuring Mail

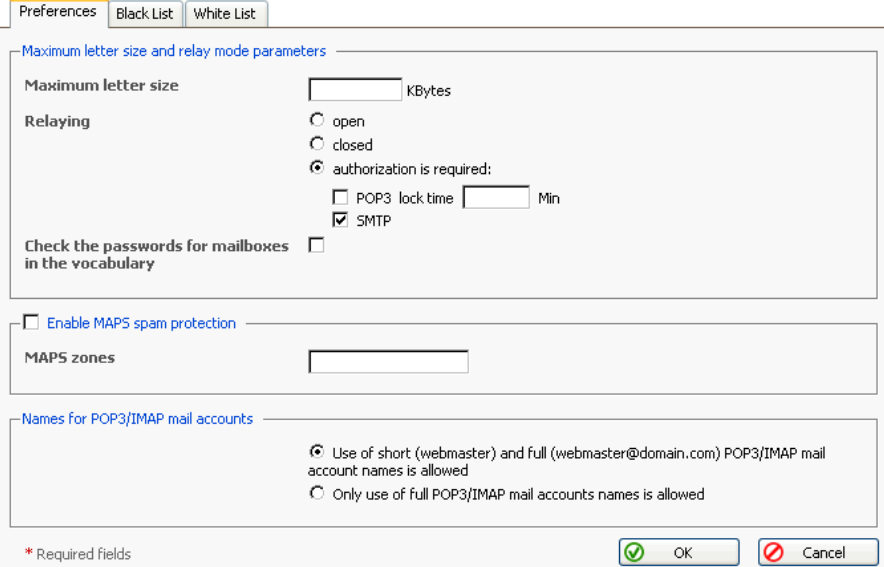
You can configure the following server-wide mail system settings:

- The maximum allowable size of any e-mail received on the server.
- Relaying mode. Relaying affects only the mail sending, it does not in any way change the way mail is received on the server. Mail relaying can work in one of three modes: open relay, closed relay and relay with authorization.
 - Open relay - selecting this allows any host computer to utilize the mail services of any domain on the server, to send and/or receive mail. In this mode, no password is required.
 - Closed relay - selecting this only allows mail to be sent and received locally (to and from domains residing on the server). The only exception would be hosts specified as allowable relay hosts in the White list.
 - Authorization required - selecting this allows any host computer to utilize the mail services of a domain on the server, provided that a valid username and password are used to authenticate the mail user.
 - POP3 - requires a POP3 login before sending mail. The lock time field sets the allowed time given for sending mail after login. During the lock time, any e-mail sent from the initial IP address will be accepted without requiring a password to be re-entered.
 - SMTP - smtp authentication (the Plesk mail system supports LOGIN, CRAM-MD5 and PLAIN methods of smtp authorization) requires a password every time you send an e-mail.
- White List. Use it to define several IP-addresses with masks from which mail will always be accepted.
- Black List. Use it to define the mail domains from which you do not allow mail to be received.
- MAPS spam protection. Enable the external mail abuse prevention system, which can help you defend your customers from abuse by spammers.
- Type of mail account names that can be used on the server.

In order to configure the mail system, follow these steps:

1. Click the  Mail icon on the Server administration page. The Mail

system management page will open:



The screenshot shows a web interface for mail system configuration. At the top, there are three tabs: 'Preferences' (selected), 'Black List', and 'White List'. Below the tabs, there are three main sections:

- Maximum letter size and relay mode parameters:**
 - 'Maximum letter size' is a text input field followed by 'KBytes'.
 - 'Relaying' has three radio buttons: 'open', 'closed', and 'authorization is required:'. The 'authorization is required:' option is selected.
 - Under 'authorization is required:', there are two checkboxes: 'POP3 lock time' (unchecked) followed by a text input field and 'Min', and 'SMTP' (checked).
 - 'Check the passwords for mailboxes in the vocabulary' is an unchecked checkbox.
- Enable MAPS spam protection:**
 - 'Enable MAPS spam protection' is an unchecked checkbox.
 - 'MAPS zones' is a text input field.
- Names for POP3/IMAP mail accounts:**
 - There are two radio buttons: 'Use of short (webmaster) and full (webmaster@domain.com) POP3/IMAP mail account names is allowed' (selected), and 'Only use of full POP3/IMAP mail accounts names is allowed'.

At the bottom left, there is a note: '* Required fields'. At the bottom right, there are two buttons: 'OK' (with a green checkmark icon) and 'Cancel' (with a red X icon).

2. To set the maximum letter size allowed on the server, click in the Maximum letter size input box and enter the desired value in Kilobytes.
3. To set the mail system relay mode, select a corresponding radio button. For relaying that requires authorization, select the Authorization is required radio button. You must then select an authorization type, which can be POP3, SMTP or both.
 - POP3 - Click in the checkbox next to POP3 to enable this mode of authorization. You must then set the lock time; the default setting is 20 minutes.
 - SMTP - Click in the checkbox next to SMTP to enable this authorization mode.
4. To prevent mail users from using the passwords that are easy to guess, use the feature Check the passwords for mailboxes in the dictionary.
5. To enable the external Mail Abuse Prevention System (MAPS) select the Enable MAPS spam protection checkbox, enter the MAPS zone name in the MAPS zones field.
6. To define the mail name type that you want to be used for the POP3/IMAP accounts, select a required radio button. Two options are provided: 1) use of both short (e.g. webmaster) and full (e.g. webmaster@domain.com) mail

names, and 2) use of full mail names only.


7. To manage the server-wide black list of blocked mail domains, select the Black List tab. To manage the white list, click White List.
8. When done configuring, click OK.

Configuring the Server-wide Spam Filter

For the purpose of filtering spam out of incoming mail you can use the integrated spam filter software SpamAssassin (<http://www.spamassassin.org/>).

SpamAssassin is a mail filter, which attempts to identify spam. Using its rule base, it uses a wide range of heuristic tests on mail headers and body text to identify "spam", also known as unsolicited commercial email. Once identified, the mail can then be optionally tagged as spam for later filtering using the user's own mail user-agent application. SpamAssassin is a third party product integrated with Plesk. For more information on the product please refer to its web location.

Plesk allows for setting up and using black lists and white lists for filtering mail at the server level as well as at the user level.

To access the server-wide spam filter settings, click the  SpamAssassin

icon on the Server administration page. The Spam filter configuration page will open:

The screenshot displays a configuration interface for a spam filter, organized into five sections:

- Usage policy settings:** Contains two checkboxes: "Server wide settings" and "Personal settings", both of which are checked. A "Set" button with a green checkmark is located at the bottom right.
- Server settings:** Includes a text input field for "Hits required for spam" containing the number "7". Below it, "Modify spam mail subject" is checked, with a "by tag" dropdown menu showing "*****SPAM*****". A "Set" button with a green checkmark is at the bottom right.
- Server-wide black list:** Features an "Email pattern" text input field and a list box for "Always mark as spam mail from address". The list box is currently empty. "Add" and "Remove" buttons are at the bottom right.
- Server-wide white list:** Features an "Email pattern" text input field and a list box for "Never mark as spam mail from address". The list box is currently empty. "Add" and "Remove" buttons are at the bottom right.
- Server-wide ignore list:** Features an "Email pattern" text input field and a list box for "Do not filter mail for these accounts". The list box is currently empty. "Add" and "Remove" buttons are at the bottom right.

You have a choice of filtering all the incoming mail at the server level as well as letting the users set up specific rules for filtering mail specifically for their own mail accounts. This is managed through the spam filter usage policies, where you can enable or disable the option of filtering mail at the server level and the option of letting users filter their mail.

1. To enable filtering mail on the server, check the Server wide settings checkbox;
2. To enable users set up their own filtering rules and filter mail for their own mail accounts, check the Personal settings checkbox;
3. Click Set to save the changes.

In order to recognize a mail message as spam it needs to score a certain amount of hits. The hits are scored according to the internal SpamAssassin settings and based on the contents of the mail messages and its subject. You

can change the sensitivity of the spam filter by varying the amount of hits required for marking a message as spam. The more hits are required the less sensitive the filter is, and vice versa – the less hits are required the more sensitive the filter is.

1. The default amount of hits is set to 7. If you wish to change this value, click into the Hits required for spam input box and type in the new value.
2. Click Set to save the changes.

Messages recognized as spam are marked correspondingly so that they can be easily visually identified. In particular, a special string is added to the subject of the message (e.g., by default the string *****SPAM***** will be added to the spam messages subjects). You can change this string (or tag) to whatever you like, or even to disable this option.

1. In order to activate/deactivate the option of modifying the spam messages subject, check the Modify spam mail subject;
2. To change the text of the string, click into the input field and enter the new text;
3. Click Set to save the changes.

Note, that even if this option is not enabled, a header "X-Spam: Yes" will be added to the headers of any mail message recognized as spam.

Black list is a list of E-mail addresses, which are automatically considered as sending unsolicited mail – spam. Therefore, all messages coming from the E-mail addresses that match those specified in the black list will automatically be marked as spam.

You can add to the black list either exact E-mail addresses or patterns, using wildcards (*), e.g.: entry *@spammers.online.com will cause all messages coming from the domain spammers.online.com be marked as spam, regardless of what the exact mail name is).

NOTE

All the incoming mail will be filtered according to the server-wide black list settings. Mail users will receive their mail already processed according to them. Should any messages be coming from the addresses specified in the server-wide black list, the users will receive them already marked as spam (of course, if the Modify spam mail subject option was enabled).

1. Enter the E-mail address or pattern into the Email pattern input field;
2. Click Add to add the new entry to the black list.

White list contains E-mail addresses, which are automatically considered as trustworthy. Therefore, all messages coming from the E-mail addresses that match those specified in the white list will never be marked as spam.

You can add to the white list either exact E-mail addresses or patterns, using wildcards (*), e.g.: entry *@your-company.com will cause all messages coming from the domain your-company.com not be marked as spam, regardless of the content of a message).

NOTE

All the incoming mail will be filtered according to the server-wide white list settings. Mail users will receive their mail already processed according to them. Should any messages be coming from the addresses specified in the server-wide white list, the users will receive them as sent from a trustworthy address, not a spam.

1. Enter the E-mail address or pattern into the Email pattern input field;
2. Click Add to add the new entry to the white list.


Ignore list contains E-mail addresses, no mail for which is to be filtered. You can add only the e-mail addresses registered in the control panel. All the messages coming to the E-mail addresses specified in the ignore list will not be processed by the spam filter at all.

1. Enter the E-mail address or pattern into the Email pattern input field;
2. Click Add to add the new entry to the ignore list.

This concludes setting up the server-wide spam mail filter. All the incoming mail will be processed according to these settings, and the users will receive their mail already processed by the filter. Further, if allowed (the Personal settings checkbox checked), the users can set up their own filtering rules and process the mail for their mail accounts according to them.

Configuring Mailman


For the initial mailman component configuration (applicable only to mailman versions 2.1.2 and later) follow these steps:

1. Click the  Mailman Settings icon on the Server administration page.
2. Supply the mailing list administrator's email and password.
3. Click OK.

Once the mailman configuring is completed, this icon is displayed in gray.

Enabling ColdFusion Support

To enable ColdFusion scripting support for virtual domains, follow these steps:

1. Click the  ColdFusion Settings icon at the Server administration page.
2. Select the desired installation configuration (Server Configuration or J2EE), and specify the destination directory.
3. Click OK.

Setting Up Dr.Web Antivirus Protection

Light version of the award-winning Dr Web antivirus filtering program is included in the default installation of Plesk. The license supports up to 15 mail accounts free of charge and can be upgraded to a version that will handle an unlimited number of mail accounts on a system. To obtain a license key for a larger number of mailboxes, please, contact sales@sw-soft.com

Installing Dr.Web Packages

If you do not have the Dr.Web packages installed on your server, follow these steps:

1. Install the RPM packages `drweb` and `drweb-qmail` from the Plesk distribution. The packages are located in `/opt/drweb` directory.
2. Change your working directory to the location where the Plesk distribution resides.
3. Run the following commands:

```
#rpm -i ./opt/drweb-4.31.4-plesk.glibc.2.2.i586.rpm
```

```
#rpm -i ./opt/drweb/drweb-qmail-4.31-rh9.build040617.14.i586.rpm
```


Once the required packages are installed, the Dr.Web service will start automatically.

Enabling Antivirus Checking For Mailboxes

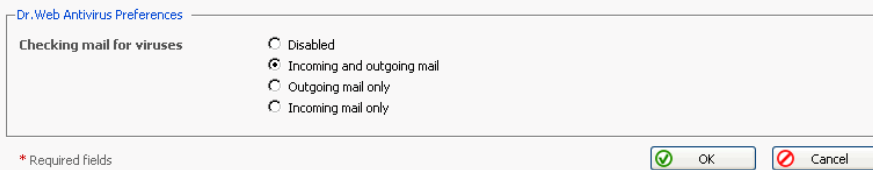
For a user's mailbox you can enable the antivirus scanner to work in one of the following modes: checking incoming and outgoing mail, checking outgoing mail only, and checking only incoming mail.

When antivirus scanning is enabled, all e-mail messages containing viruses are intercepted and placed to the directory `/var/drweb/infected`. You should clean this directory from time to time.

To enable antivirus scanning for a specific mailbox, follow these steps:

1. Access the mail name management functions, and click  Dr.Web.

The antivirus preferences page will appear:



2. Select a required scanning mode and click OK.


Updating Antivirus Database

To update the antivirus database on demand, run the command `# /opt/drweb/update/update.pl`

It is recommended that you add this command to the Crontab in order to have the antivirus database automatically updated.

Setting Up PostgreSQL Administrator's Account


To set the database administrator's login and password follow these steps:

1. Click the  PostgreSQL icon on the Server administration page. The Databases administrator credentials setup page will open.
2. To set the database administrator's login click into the appropriate text input field and type in the login name.
3. To change the password for an existing database, first enter the old password into the Old Password field, type the new password in the New Password and Confirm Password fields.
4. Click OK to submit.

Registering Your Server and Managing Access to Additional Services

As the administrator (server owner) you can get commissions on purchases made by your customers via My.Plesk.com service: domain registration, renewal, transfers, purchases of SSL certificates and third-party tools or services. To do this, you need to create a My.Plesk.com account and register your server (Plesk instance) with it. After that you will be able to track the purchases made by your customers via MPC and earn commissions. You can register multiple servers with a single My.Plesk.com account.

To enable/disable access to the My.plesk.com services from the control panel, follow these steps:

1. On the Server administration page click  Add Services. The

Additional Services Setup page appears:



Server >
Set up additional services [Up Level](#)

Tools

 Register


Preferences

Allow domain registration	<input checked="" type="checkbox"/>
Allow certificate purchasing	<input checked="" type="checkbox"/>
Allow extra services	<input checked="" type="checkbox"/>

* Required fields

2. Select (or deselect) the checkbox corresponding to the service you wish to activate (or deactivate).
3. Click OK to submit changes.

To register your server with MPC, follow these steps:

1. Click  Register. The MPC Login page will open in a new browser window.
2. Enter your Login name and Password in the fields provided, click Log In to enter. You will be taken to the page My Commissions, and prompted to register your server.
3. Click the button Register Server Now. The Server Registration page will

open displaying your Plesk software license key number and your IP address.

4. Click OK to confirm your server registration.


Managing Control Panel SSL Certificates

An SSL certificate represents a set of rules used when exchanging encrypted information between two computers. Certificates ensure secure communications; this is especially important when handling e-commerce transactions and other private transmittals. Only authorized users can access and read an encrypted data stream.

Notes on Certificates:

- A default SSL certificate is uploaded automatically for the control panel. However, this certificate will not be recognized by a browser as one that is signed by a certificate signing authority. The default SSL certificate can be replaced by either a self-signed certificate or one signed by a recognized certificate-signing authority.
- You can acquire SSL certificates from various sources. We recommend using the certificate signing request (CSR) option within Plesk. You can also purchase the certificate through the My.Plesk.com (MPC) web site.
- If using a SSL certificate issued by a certificate authority other than Thawte or Verisign, a rootchain certificate is required to appropriately identify and authenticate the certificate authority that has issued your SSL certificate.
- Once you have obtained a SSL certificate or a certificate part, you can upload it through Plesk using the instructions, which follow in this section.

Accessing the Control Panel SSL Certificates Repository


To access the Control Panel certificates repository, click the  Certificates


icon at the Server administration page. The certificates repository page will open displaying the list of available certificates:


Server >

Certificates Up Level

Tools


[Add Certificate](#)


[View Certs](#)







[Download](#)

Find the appropriate private key to the certificate

Certificate

Certificates

SSL certificates (1)

R	K	C	A	Certificate Name	Used	
				default certificate	2	

The four icons, preceding the certificate name in the list, indicate the present parts of a certificate. The icon displayed in the R column indicates that the Certificate Signing request part is present in the certificate, the icon in the K column indicates that the private key is contained within the certificate, the icon in the C column indicates that the SSL certificate text part is present and the icon in the A column indicates that CA certificate part is present. The number in the Used column indicates the number of IP addresses the certificate is assigned to.

Uploading a certificate file with finding the appropriate private key


After you have received your signed SSL certificate from the certificate authority you can upload it from the Certificate repository page. First make sure that the certificate file has been saved on your local machine or network. Use the Browse button to locate the certificate. Click Send File. The existing certificate with appropriate private key will be found and the certificate part will be added to the repository.

Changing certificate name


To change a certificate name follow these steps:

1. At the certificate repository page, select a certificate from the list. You will be taken to the SSL certificate properties page.
2. Click in the Certificate name field and edit the name as desired.
3. Click Set.

Viewing purchased certificates

After you have purchased your certificates through the control panel you can utilize the  View Certs function to view the information about your SSL certificate(s).

Downloading a certificate from repository to the local machine

To download the certificate to the local machine, click the  icon, corresponding to the required certificate. Select the location when prompted, specify the file name and click Save to save it.



Removing a certificate from repository

To delete one or more certificates from the repository, at the certificate repository page, select the corresponding checkboxes and click Remove Selected.


Downloading the certificate currently installed at the Control Panel

To download the currently installed Control Panel certificate to the local machine, click the  Download icon. Select the location when prompted, specify the file name and click Save to save it.

Setting the Control Panel certificate

To set up a certificate for your Control Panel, select a certificate by checking an appropriate checkbox, then click  Setup. To make a certificate the one used by default, click  Default.

Adding a certificate to the repository

To add a certificate to repository, click the  Add Certificate icon at the

Control panel certificate repository page. The SSL certificate creation page will open. On this page you can generate a self-signed certificate, certificate-signing request, purchase a SSL certificate, and add the certificate parts to an existing certificate.

Generating a self-signed certificate

To generate a self-signed certificate follow these steps:

1. Specify the certificate name.
2. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop-down list.
3. Select a country from the drop-down list
4. Specify the state or province, location (city).
5. Enter the appropriate organization name and department/division in the field provided.
6. Enter the Domain Name for which you wish to generate the self-signed certificate.
7. Specify the E-mail address.
8. Click the Self-Signed button. Your self-signed certificate will be immediately added to the repository.

Generating a Certificate Signing Request

To generate a certificate signing request (CSR) follow these steps:

1. Specify the certificate name.
2. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop-down list.
3. Select a country from the drop-down list
4. Specify the state or province, location (city).
5. Enter the appropriate organization name and department/division in the field provided.
6. Enter the Domain Name for which you wish to generate the certificate signing request.
7. Click the Request button. A certificate signing request will be generated and added to the repository. You will be able to add the other certificate parts later on.

Purchasing a Certificate


To purchase a new certificate follow these steps:

1. Specify the certificate name.
2. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop-down list.
3. Select your country from the drop-down list.
4. Enter your State or Province, your Location (City), Organization Name (Company), organization department (division name)
5. Enter the Domain Name for which you wish to purchase a SSL certificate.
6. Enter the domain owner's e-mail address in the appropriate field.
7. Select the Buy Cert button. You will be taken step by step through the purchase procedure. It is important to note that you must make sure that all the provided information is correct and accurate, as it will be used to generate the private key.

When using Plesk to purchase your SSL certificate you will receive the certificate file via e-mail from the certificate signing authority. Follow the instructions in the "Uploading a certificate file with finding the appropriate private key" section to upload the certificate to the repository.

Uploading certificate parts

If you have already obtained a certificate containing private key and certificate part (and may be CA certificate), follow these steps to upload it:

1. At the certificate repository page, click the  Add Certificate icon. You will be taken to the SSL certificate creation page.
2. In the Upload certificate files section of the page, use the Browse button to locate the appropriate certificate file or a required certificate part.

NOTE

Your certificate can be contained within one or several files, so you may upload the certificate by parts or as a single file, selecting it in several fields (Plesk will recognize the appropriate certificate parts and upload them correspondingly).

3. Click Send File. This will upload your certificate parts to the repository.

You can upload an existing certificate in two ways:

1. Choose a file from the local network and click the Send File button (.TXT

files only).

2. Type in or paste the certificate text and private key into the text fields and click the Send Text button.

Uploading a CA certificate

For the certificates purchased through certificate signing authorities other than Verisign or Thawte you will receive what is typically called a CA Certificate, or rootchain certificate. The CA Certificate is used to appropriately identify and authenticate the certificate authority, which has issued your SSL certificate. To upload your CA Certificate, follow these steps:

1. At the certificate repository page, select a certificate from the list. You will be taken to the SSL certificate properties page.
2. Use the Browse button, within the section related to the certificate uploading, to locate the appropriate CA Certificate file.
3. Click Send File. This will upload your CA Certificate to the repository.

You can upload an existing certificate in two ways:

1. Choose a file from the local network and click the Send File button (.TXT files only).
2. Type in or paste the CA certificate text into the text field and click the Send Text button.

Generating a CSR using an existing private key

A situation may occur in some cases, that you have a certificate in the repository, which has only the private key part and the other parts are missing due to some reasons. To generate a new Certificate Signing Request using the existing private key, follow these steps:

1. At the certificate repository page, select from the list a certificate, which has the private key part only. You will be taken to the SSL certificate properties page.
2. Click Request.

Removing a certificate part

After you have uploaded a CA certificate part (rootchain certificate), you are able to remove it. To do so, follow these steps:

1. At the certificate repository page, select a certificate from the list. You will

be taken to the SSL certificate properties page.


2. Click the Remove button located next to the CA certificate field.

Setting System-wide Preferences and Logo

You can set the following system-wide preferences:

- The number of lines displayed on the pages containing lists (i.e.: list of domains, list of clients, etc.),
- The length of interface buttons.
- Default interface language and skin that will be used for control panel sessions initiated by other users,
- Administrator's interface language and skin,
- Allowance of multiple simultaneous sessions under administrator's login,
- Your hostname,
- Apache restart interval: defining this might help decrease the Apache web server downtime, especially, if you have a large number of user accounts and domains hosted on server.
- Server-wide statistics parameters.

To set the server-wide preferences follow these steps:

1. Click the  Preferences icon on the Server administration page. The

Server preferences page appears:

The image shows two screenshots of the Plesk Preferences dialog box. The top screenshot shows the following settings:

- Display: 50 lines per page
- Button label length: 12
- Default locale: English
- Default skin: WinXP Blue
- Administrator's interface language: English
- Administrator's interface skin: WinXP Blue
- Allow multiple sessions under administrator's login:

The bottom screenshot shows the following settings:


- Full hostname: hostname.com
- Apache restart interval: 600 Seconds
- Retain traffic statistics for: 3 Months
- Include in the disk space usage calculation: log files, databases, mailboxes, web applications, mailing lists, domain backup files
- Include in the traffic calculation: inbound and outbound traffic, only inbound traffic, only outbound traffic

At the bottom of the dialog box, there is a note: "* Required fields" and buttons for "OK" and "Cancel".

2. Adjust the settings as required, and click OK to submit.

Setting Up Your Logo

You may replace the default Plesk logo in the top banner area with your own logo. This provides you with a customized look for your interface. Also, it enables you to hyperlink the logo to your organization's web site. To change the logo on the interface, follow these steps:

1. Click the  Logo Setup icon on the Server administration page. The

Logo Setup page appears:

The image shows the "Set up logo properties" dialog box with the following fields and buttons:

- Choose new logo file: [Text box] Browse...
- Enter new URL for logo *: http://www.sw-soft.com
- Buttons: Default Logo, OK, Cancel

At the bottom left, there is a note: "* Required fields".

2. Click in the Choose new logo file text box and enter the name of the logo

file you wish to use, or click the Browse... button and locate the desired file.

NOTE

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.

3. You have the option to create a hyperlink that activates when a user clicks on your logo. The link may take the user to a corporate URL or other web site. Click in the Enter new logo link URL box. Type in the URL.
4. Click OK to submit.

If you change your mind and wish to revert to the Plesk logo, use the Default Logo button.


Tracking User Actions

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 later on. The following system events (actions) can be logged:

- Administrator information changed
- System service restarted, started, or stopped
- IP address added, removed, changed
- Client account created, deleted, personal or system information changed,
- The status of client account changed (enabled/disabled)
- Client's interface preferences changed
- Client's IP pool changed,
- The limit on disk space is reached for a client account,
- The limit on traffic is reached for a client account,
- The limit on disk space is reached for a domain,
- The limit on traffic is reached for a domain,
- Domain user account properties changed,
- Domain created, deleted, settings changed,
- Domain status changed (enabled/disabled),
- DNS zone updated for a domain,
- Subdomain created, deleted, settings changed,
- Client account limits changed,
- Client's permissions changed,
- Domain limits changed,
- Users logged in and out of the Control Panel,
- Mail names created, deleted, changed,
- Mailing list created, deleted, changed,
- Physical hosting created, deleted, changed,

- Web user account created, deleted, changed,
- Site application installed, reconfigured, uninstalled,
- Site application package installed, uninstalled,
- License key updated.

To configure the action log settings, follow these steps:

1. Click the  Action Log icon on the Server administration page. The Action log settings page will open.
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. To retain all action log records, select the Do not remove records option.
4. To apply all the changes made, click OK.

To download the action log to the local machine, 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. Select the location, and click Save.

To clear the action log, use the Clear Log button.

Using Event Manager

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

Adding an Event Handler

For instance, let's create an event handler for the 'client account creation' event. The handler will accept a client name as the first parameter, and the client's login as the second. For simplicity we will use a shell-script called test-handler.sh that looks as follows:

```
-----  
#!/bin/bash  
echo "-----" >> /tmp/event_handler.log  
/bin/date >> /tmp/event_handler.log #  
information on the event date and time
```


```

/usr/bin/id                >> /tmp/event_handler.log #
information on the user, on behalf of which the script was
executed (to ensure control)
echo "client created" >> /tmp/event_handler.log #
information on the created client account
echo "name: $1"         >> /tmp/event_handler.log # client's
name
echo "login: $2"        >> /tmp/event_handler.log # client's
login
echo "-----" >> /tmp/event_handler.log
-----

```

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

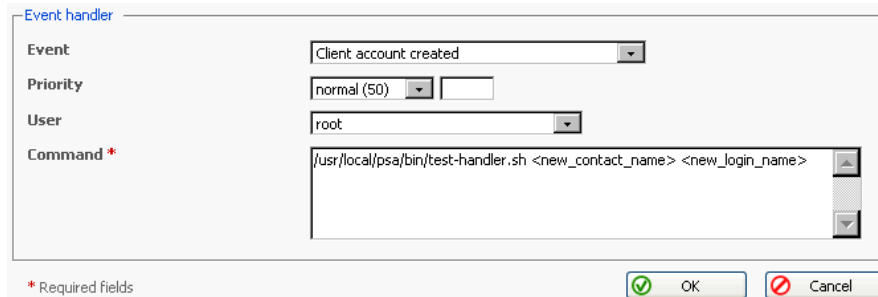
Suppose, that our script is located in the directory `/usr/local/psa/bin` (for instance). Let's register it by creating an event handler via the control panel:

1. Select the Server shortcut in the navigation pane.
2. Click the  Event Manager icon on the Server administration page.

The Event Manager page will appear.

3. Click the  Add New Event Handler icon. The event handler setup

page appears:



4. Select the event, you wish to assign a handler to in the Event drop-down box.
5. 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. Note, 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).
6. Select the system user, on behalf of which the handler will be executed.
7. 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`
`<new_contact_name> <new_login_name>`

8. 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 login of the created client respectively. The entire list of available parameters is provided in the following section. You should keep in mind that with the removal operations, the parameters of type `new_xxx` contain an empty string. And with creation operations the parameters of type `old_xxx` contain an empty string.

Now if you login to your Plesk control panel and create a new client, specifying the value 'Some Client' in the 'Contact name' field, and 'some_client' in the field 'Login', the handler will be invoked, and the following records will be added to the `/tmp/event_handler.log`:

```
-----
Sat Jun 26 21:46:34 NOVT 2004
uid=0(root) gid=0(root) groups=0(root)
client created
name: Some client
login: some_client
-----
```

If you want to specify one or few handlers more, repeat the actions above for another handler.

Removing Event Handlers

In order to remove one or several event handlers, in the list of handlers select the corresponding checkboxes and click Remove selected.

Available Event Handler Parameter Templates

The parameter templates that can be used when setting up an event handler are presented in the table below:

Table 2.1.

Component name/description	Command line parameter		Notes
	Old component value	New component value	
For the events 'Client account created', 'Client account updated', 'Client account removed'			
Login Name	old_login_name	new_login_name	required
Contact Name	old_contact_name	new_contact_name	required
Company Name	old_company_name	new_company_name	
Phone	old_phone	new_phone	
Fax	old_fax	new_fax	
E-mail	old_email	new_email	
Address	old_address	new_address	
City	old_city	new_city	
State/Province	old_state_province	new_state_province	
Postal/ZIP Code	old_postal_zip_code	new_postal_zip_code	
Country	old_country	new_country	
For the events 'Domain created', 'Domain updated', 'Domain deleted'			
Domain Name	old_domain_name	new_domain_name	required
For the events 'Subdomain created', 'Subdomain updated', 'Subdomain deleted'			
Subdomain Name	old_subdomain_name	new_subdomain_name	required
Parent Domain Name	old_domain_name	new_domain_name	required
FTP account	old_system_user_type	new_system_user_type	
Subdomain owner's login name	old_system_user	new_system_user	
Hard disk quota	old_hard_disk_quota	new_hard_disk_quota	
SSI support	old_ssi_support	new_ssi_support	
PHP support	old_php_support	new_php_support	
CGI support	old_cgi_support	new_cgi_support	
Perl support	old_mod_perl_support	new_mod_perl_support	

Component name/description	Command line parameter		Notes
	Old component value	New component value	
Python support	old_mod_python_support	new_mod_python_support	
ColdFusion support	old_coldfusion_support	new_coldfusion_support	
Apache::ASP support	old_apache_asp_support	new_apache_asp_support	
SSL support	old_ssl_support	new_ssl_support	
For the events 'Physical hosting created', 'Physical hosting updated'			
Domain Name	old_domain_name	new_domain_name	required
IP Address	old_ip_address	new_ip_address	
IP Type	old_ip_type	new_ip_type	
System User	old_system_user	new_system_user	
System User Password	old_system_user_password	new_system_user_password	
Shell Access	old_system_shell	new_system_shell	
FP Support	old_fp_support	new_fp_support	
FP-SSL Support	old_fpssl_support	new_fpssl_support	
FP Authoring	old_fp_authoring	new_fp_authoring	
FP Admin Login	old_fp_admin_login	new_fp_admin_login	
FP Admin Password	old_fp_admin_password	new_fp_admin_password	
SSI Support	old_ssi_support	new_ssi_support	
PHP Support	old_php_support	new_php_support	
CGI Support	old_cgi_support	new_cgi_support	
Mod Perl Support	old_mod_perl_support	new_mod_perl_support	
Apache ASP Support	old_apache_asp_support	new_apache_asp_support	
SSL Support	old_ssl_support	new_ssl_support	
Web Statistics	old_web_statistics	new_web_statistics	

Component name/description	Command line parameter		Notes
	Old component value	New component value	
Custom Error Documents	old_apache_error_documents	new_apache_error_documents	
Hard Disk Quota	old_hard_disk_quota	new_hard_disk_quota	
For the event 'Physical hosting deleted'			
Domain Name	old_domain_name	new_domain_name	required
For the events 'Mail name created', 'Mail name deleted'			
Mail name	old_mailname	new_mailname	required (in the format mailname@domain)
For the event 'Mail name updated'			
Mail name	old_mailname	new_mailname	required (in the format mailname@domain)
Mailbox	old_mailbox	new_mailbox	
Password	old_password	new_password	
Mailbox Quota	old_mailbox_quota	new_mailbox_quota	
Redirect	old_redirect	new_redirect	
Redirect Address	old_redirect_address	new_redirect_address	
Mail Group	old_mail_group	new_mail_group	
Autoresponders	old_autoresponders	new_autoresponders	
Mail User Control Panel Access	old_mail_controlpanel_access	new_mail_controlpanel_access	
For the event 'Web user deleted'			
Domain Name	old_domain_name	new_domain_name	required
Web user Name	old_webuser_name	new_webuser_name	required
For the events 'Web user created', 'Web user updated'			
Domain Name	old_domain_name	new_domain_name	required
Web User Name	old_webuser_name	new_webuser_name	required

Component name/description	Command line parameter		Notes
	Old component value	New component value	
Web User Password	old_webuser_password	new_webuser_password	
SSI Support	old_ssi_support	new_ssi_support	
PHP Support	old_php_support	new_php_support	
CGI Support	old_cgi_support	new_cgi_support	
Mod Perl Support	old_mod_perl_support	new_mod_perl_support	
Mod Python Support	old_mod_python_support	new_mod_python_support	
Apache ASP Support	old_apache_asp_support	new_apache_asp_support	
Hard Disk Quota	old_hard_disk_quota	new_hard_disk_quota	
For the event 'Client limits updated'			
Contact Name	old_contact_name	new_contact_name	required
Maximum Number of Domains	old_maximum_domains	new_maximum_domains	
Maximum Amount of Disk Space	old_maximum_disk_space	new_maximum_disk_space	
Maximum Amount of Traffic	old_maximum_traffic	new_maximum_traffic	
Maximum Number of Web Users	old_maximum_webusers	new_maximum_webusers	
Maximum Number of Databases	old_maximum_databases	new_maximum_databases	
Maximum Number of Mailboxes	old_maximum_mailboxes	new_maximum_mailboxes	
Mailbox Quota	old_maximum_mailbox_quota	new_maximum_mailbox_quota	
Maximum Number of Mail Redirects	old_maximum_mail_redirects	new_maximum_mail_redirects	
Maximum Number of Mail Groups	old_maximum_mail_groups	new_maximum_mail_groups	

Component name/description	Command line parameter		Notes
	Old component value	New component value	
Maximum Number of Mail Autoresponders	old_maximum_mail_autoresponders	new_maximum_mail_autoresponders	
Maximum Number of Mailing Lists	old_maximum_mail_lists	new_maximum_mail_lists	
Maximum Number of Web Applications	old_maximum_tomcat_web_applications	new_maximum_tomcat_web_applications	
Expiration Date	old_expiration_date	new_expiration_date	
For the event 'Domain limits updated'			
Domain Name	old_domain_name	new_domain_name	required
Maximum Amount of Disk Space	old_maximum_disk_space	new_maximum_disk_space	
Maximum Amount of Traffic	old_maximum_traffic	new_maximum_traffic	
Maximum Number of Web Users	old_maximum_webusers	new_maximum_webusers	
Maximum Number of Databases	old_maximum_databases	new_maximum_databases	
Maximum Number of Mailboxes	old_maximum_mailboxes	new_maximum_mailboxes	
Mailbox Quota	old_maximum_mailbox_quota	new_maximum_mailbox_quota	
Maximum Number of Mail Redirects	old_maximum_mail_redirects	new_maximum_mail_redirects	
Maximum Number of Mail Groups	old_maximum_mail_groups	new_maximum_mail_groups	
Maximum Number of Mail Autoresponders	old_maximum_mail_autoresponders	new_maximum_mail_autoresponders	
Maximum Number of Mailing Lists	old_maximum_mail_lists	new_maximum_mail_lists	
Maximum Number of Web Applications	old_maximum_tomcat_web_applications	new_maximum_tomcat_web_applications	

Component name/description	Command line parameter		Notes
	Old component value	New component value	
Expiration Date	old_expiration_date	new_expiration_date	
For the events 'Mailing list created', 'Mailing list updated', 'Mailing list deleted'			
Domain Name	old_domain_name	new_domain_name	required
Mailing list name	old_mail_list_name	new_mail_list_name	required
Mailing list enabled	old_mail_list_enabled	new_mail_list_enabled	
For the events 'Control panel user logged in', 'Control panel user logged out'			
Contact Name	old_contact_name	new_contact_name	
For the event 'Domain user account updated'			
Allow domain user access	old_allow_domain_user_access	new_allow_domain_user_access	
Login Name	old_login_name	new_login_name	required
Domain Name	old_domain_name	new_domain_name	required
Contact Name	old_contact_name	new_contact_name	
Company Name	old_company_name	new_company_name	
Phone	old_phone	new_phone	
Fax	old_fax	new_fax	
E-mail	old_email	new_email	
Address	old_address	new_address	
City	old_city	new_city	
State/Province	old_state_province	new_state_province	
Postal/ZIP Code	old_postal_zip_code	new_postal_zip_code	
Country	old_country	new_country	
For the events 'Site application installed', 'Site application reconfigured', Site application uninstalled'			
Site application package name	old_site_application_package_name	new_site_application_package_name	required
Domain type (domain or	old_site_application_domain_type	new_site_application_domain_type	required

Component name/description	Command line parameter		Notes
	Old component value	New component value	
subdomain)			
Installation path (httpdocs or httpsdocs)	old_site_application_directory	new_site_application_directory	required
Installation path within the destination directory	old_site_application_installation_prefix	new_site_application_installation_prefix	required
For the events 'Site application package installed', 'Site application package uninstalled'			
Site application package name	old_site_application_package_name	new_site_application_package_name	required
For the events 'Service stopped, started, or restarted'			
Service	old_service	new_service	required
For the events 'IP address created, changed, or deleted'			
IP address	old_ip_address	new_ip_address	required
IP mask	old_ip_mask	new_ip_mask	
Interface	old_interface	new_interface	
IP type	old_ip_type	new_ip_type	
For the events 'Forwarding created, changed, deleted'			
Domain name	old_domain_name	new_domain_name	required
Forwarding type	old_forwarding_type	new_forwarding_type	
URL	old_url	new_url	
For the event 'Administrator information changed'			
Login name	old_login_name	new_login_name	required
Contact name	old_contact_name	new_contact_name	
Company name	old_company_name	new_company_name	
Phone number	old_phone	new_phone	
Fax	old_fax	new_fax	

Component name/description	Command line parameter		Notes
	Old component value	New component value	
E-mail	old_email	new_email	
Address	old_address	new_address	
City	old_city	new_city	
State/Province	old_state_province	new_state_province	
Postal/Zip code	old_postal_zip_code	new_postal_zip_code	
Country	old_country	new_country	
For the events 'Site application installed, reconfigured, uninstalled'			
Site application name	old_package_name	new_package_name	required
For the events 'Client status updated'			
Contact name	old_contact_name	new_contact_name	required
Login name	old_login_name	new_login_name	required
Status	old_status	new_status	
For the events 'Client preferences updated'			
Contact name	old_contact_name	new_contact_name	required
Login name	old_login_name	new_login_name	required
Page size	old_lines_per_page	new_lines_per_page	
Interface skin	old_interface_skin	new_interface_skin	
For the event 'Client's IP pool changed'			
Contact name	old_contact_name	new_contact_name	required
IP address	old_ip_address	new_ip_address	required
Status	old_status	new_status	
For the event 'Limit on disk space reached for the client account'			
Disk space limit	old_maximum_disk_space	new_maximum_disk_space	required
For the events 'Limit on traffic reached for the client account'			
Traffic limit	old_maximum_traffic	new_maximum_traffic	


Component name/description	Command line parameter		Notes
	Old component value	New component value	
For the events 'Domain status changed'			
Domain name	old_domain_name	new_domain_name	required
Domain status	old_status	new_status	
For the event 'DNS zone updated for domain'			
Domain name	old_domain_name	new_domain_name	required
For the event 'Limit on disk space reached for domain'			
Disk space limit	old_maximum_disk_space	new_maximum_disk_space	
For the event 'Limit on traffic reached for domain'			
Traffic limit	old_maximum_traffic	new_maximum_traffic	
For the event 'License key update'			
License key number	old_license	new_license	Required
License key type (Plesk, additional)	old_license_type	new_license_type	
License key name (for additional keys)	old_license_name	new_license_name	

Enabling E-mail Notification

You can configure Plesk so as to notify you or other control panel users by e-mail of the following system events:

- client account creation,
- client account expiration,
- new domain creation,
- domain expiration,
- account limits exceeded,
- trouble ticket submitted,
- trouble ticket commented,
- trouble ticket closed,
- trouble ticket reopened.












To enable e-mail notifications, follow these steps:

1. On the Server administration page click the  Notifications icon. The

Notification Subscription page appears:

[Server >](#)

Notification subscription [Up Level](#)

Event	Send notice to:				Text
	admin	client	domain user	e-mail address	
Client Account Creation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/> <input type="text"/>	
Client Account Expired	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/> <input type="text"/>	
Client Account Expiration Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/> <input type="text"/>	
Domain Creation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/> <input type="text"/>	
Domain Expired	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="text"/>	
Domain Expiration Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="text"/>	
Account Limit Notices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="text"/>	
Ticket Created	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="text"/>	
Ticket Commented	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="text"/>	
Ticket Closed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="text"/>	
Ticket Reopened	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="text"/>	


Preferences

Send Expiration Warnings days in advance

* Required fields

2. Select the events and the appropriate types of users you wish to be notified using the checkboxes in the Send notice to: admin, client, domain user, and e-mail address columns.
3. Enable sending expiration warnings in advance by specifying the necessary value in the appropriate field. Note that expiration warning message is sent once in a specified number of days prior to the domain or client account expiration date.
4. Click OK to submit all changes.

To edit the default notification message text, follow these steps:

1. On the Notification subscription page click on the icon  (Edit notice text), related to the desired system event. Notification editing page appears:

Server > Notifications >
Edit notice Up Level

Notification

Notice text

```
A new client account has been created in Plesk.
Client's contact name: <client_contact_name>
Client's login: <client_login>
Client's password: <password>
Plesk entry point: https://<hostname>:8443
```

* Required fields

Default OK Cancel

2. Click Default, if you wish to use the default notice text. Enter or edit the notice text as desired.
3. Click OK.

When composing a notice you can use several tags that will be replaced with the actual data retrieved from the Plesk database:

Creation of a client account

- <client> or <client_contact_name> - client's contact name
- <client_login> - client's login name
- <password> - user's password
- <hostname> - host name for control panel access

Client account expiration

- <client_login> - client's login name
- <client> or <client_contact_name> - client's contact name
- <expiration_date> - client account expiration date

Client account expiration warning

- <client_login> - client's login name
- <client> or <client_contact_name> - client's contact name
- <expiration_date> - client account expiration date

New domain creation

- <domain_name> or <domain> - domain name
- <client_login> - client's login name
- <client> or <client_contact_name> - client's contact name
- <ip> - ip address pointing to the domain name

Domain expiration

- <domain_name> or <domain> - domain name

- <client_login> - client's login name
- <client_contact_name> or <client> - client's contact name
- <expiration_date> - domain expiration date

Domain expiration warning

- <domain_name> or <domain>- domain name
- <client_login> - client's login name
- <client> or <client_contact_name> - client's contact name
- <expiration_date> - domain expiration date

Account limit notices

- <domain> or <domain_name> - domain name
- <client_login> - client login name
- <client> or <client_contact_name> - client's contact name
- <disk_usage> - information on disk space usage
- <disk_space_limit> - information on the disk space limit set for the account
- <traffic> - information on traffic usage
- <traffic_limit> - the traffic limit

Help Desk system notices

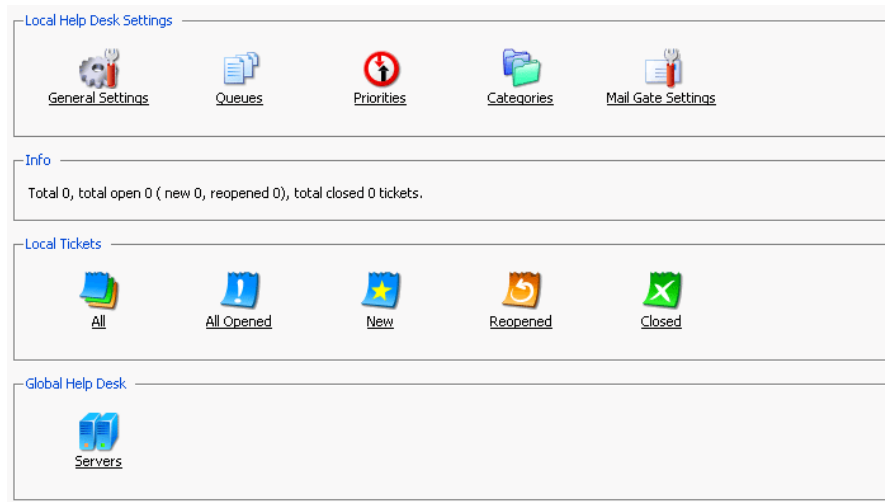
- <ticket_id> - trouble ticket identification number
- <ticket_comment> - trouble ticket comment


Configuring the Help Desk

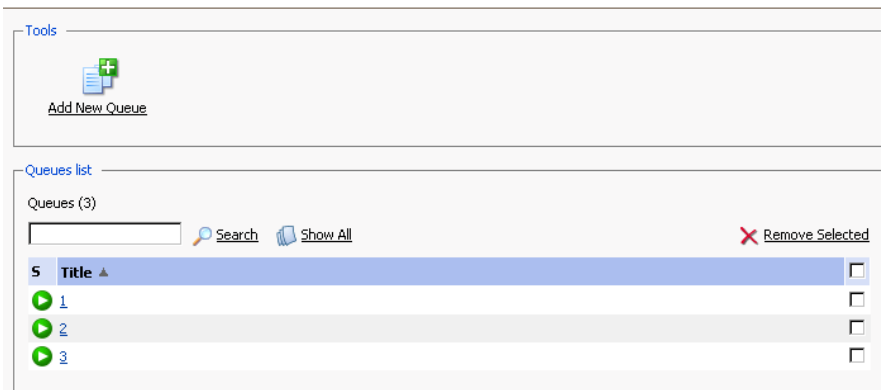
The Help Desk solution integrated with Plesk provides the server administrator with an easy-to-use interface for handling technical assistance requests submitted by the control panel users.


Before users are able to submit the trouble tickets, you should perform an initial configuration of Help Desk. To this effect, you should create at least one instance of Queue, Priority and Category and then activate the Help Desk:

1. Select the Help Desk shortcut in the navigation pane. The Help Desk's main page opens:






- To create a new Queue, select the  Queues icon. The page opens displaying the queues registered in the system:



- Select the  Add New Queue icon. The queue properties page appears:




- Enter a title, select the Enabled checkbox and click OK.
- In the same manner create at least one Priority and one Category using respective  Priorities and  Categories icons on the main Help Desk System's page.
- Once the queue, priority and category are created, return to the main Help

Desk page and click  General Settings. The General Settings page

opens:

Help Desk Settings [Up Level](#)

Tools

 [Enable](#)

Help Desk Settings


Allow customers to submit tickets

Default Priority 2-Normal

Default Queue 1

Default Category General

* Required fields

7. Select the "Allow customers to submit tickets" checkbox, and select the default queue, priority and category, created at the previous steps. Click the  Enable icon. Help Desk is now activated. Click OK.


You can also allow submitting tickets by e-mail. To do this you need to configure the mail gate:

1. On the main Help Desk page, click the  Mail Gate Settings icon.

The mail gate configuration page opens:

Help Desk Mail Gate Settings [Up Level](#)

Tools

 [Enable](#)

Help Desk Mail Gate Settings

Notification Sender's Name * Help Desk

Notification Sender's Return Address * desk@sw-soft.com

POP3 Server * sw-soft.com

POP3 Login * troubleshooter

Old POP3 password None

New POP3 password ••••••


Confirm POP3 Password ••••••

Query mail once in * 30 min

Ticket subject must start with Help Desk -

* Required fields

2. Fill out the following fields:

- Notification Sender's Name - the name that will be set up in the e-mail notification messages
 - Notification Sender's Return Address - the notification sender's return e-mail address
 - POP3 Server - POP3 server, the mail should be fetched from
 - POP3 Login - login name for accessing the POP3 server
 - New POP3 password - POP3 password that will be used for getting mail
 - Confirm POP3 Password - password confirmation
 - Query mail once in - [] min – define the time interval between mail queries.
 - Ticket subject must start with [] – specify the combination of symbols the subject line of mail messages must start with. This can help to filter out spam.
3. Once the required fields are filled out, click  Enable. The mail gate is activated.
4. Click OK to return to the main page.

Chapter 3. Performing Administrative Tasks

This chapter focuses on administrative tasks you perform when administering your Plesk system. The operations described are available only when you are logged on as administrator to your system.

Editing Administrator's Information and Password

To enter or edit Administrator's information, follow these steps:

1. On the Server administration page, click  Edit. The Administrator's

information editing page appears:

Server >
Edit administrator information [Up Level](#)

Administrator information

Company name *	<input type="text" value="SWsoft"/>
Contact name *	<input type="text" value="admin"/>
Phone *	<input type="text" value="112233445"/>
Fax	<input type="text"/>
E-mail *	<input type="text" value="admin@sw-soft.com"/>
Address *	<input type="text" value="your address"/>
City *	<input type="text" value="your city"/>
State/Province *	<input type="text" value="State"/>
Postal/ZIP code *	<input type="text" value="1234567"/>
Country	<input type="text" value="Bermuda"/>

I would like to receive periodic e-mails from SWsoft, Inc. announcing new products, discounts and more.


* Required fields

2. Click in any of the desired fields and type in the necessary data. All required fields are marked with asterisks.
3. Click OK to submit.

NOTE

When you change the administrative email address, be sure to inform your users of the new address.

To change the administrative password follow these steps:

1. On the Server administration page, click  Change Password. The

Administrator's password page appears:

Server >
Administrator's password Up Level

Administrator's password

Old password *

New password *

Confirm Password *

* Required fields OK Cancel








2. Click in the Old password text box and enter your current password.
3. Click in the New password text box and enter the password you wish to change to.
4. Click in the Confirm Password text box and re-enter the new password, exactly as you entered it in the New password text box.
5. Click OK.

If you forget your password

If you forget your password, you can use the password reminder feature available from the control panel login screen, however you should keep in mind that sending administrator's password by e-mail is insecure. You can look up your password in the `/etc/psa/.psa.shadow` file.


Starting and Stopping Plesk Services

To manage Plesk services from the control panel, follow these steps:


1. Click the  Service Management icon on the Server administration page. The Services management page appears. The current state of a service is marked by an icon:  (On) for the service running,  (Off) for the service stopped, and  if service is not installed or its management capabilities are not supported by the license key.
2. To start a service: click  (Start service).
 To stop a service: click  (Stop service).
 To restart a service: click  (Restart service).

Managing Server IP Addresses


If your server has more than one IP address or is on more than one network interface, you can use the IP Addresses function in order to control IP addresses on system network interfaces.


To do this, click the  IP Addresses icon on the Server administration

page. The IP addresses management page appears displaying the list of IP addresses available in the system:

Server > **IP aliasing management**  Up Level




Tools


[Reread IP](#)


[Add IP Address](#)

IP Addresses

IP Addresses (2)

 Search
 Show All
 Remove Selected

S	T	IP Address ▲	Subnet Mask	Interface	Clients	Hosting	<input type="checkbox"/>
✔	👑	10.1.150.1	255.255.0.0	eth0	1	2	<input type="checkbox"/>
✔	🌿	192.168.42.140	255.255.255.0	eth0	0	0	<input type="checkbox"/>

The icons in the S and T columns represent the IP address state and type (👑 exclusive or 🌿 shared) respectively, the numbers shown in the Clients and Hosting columns indicate whether the ip address is used by clients and hosting accounts.

NOTE

You can allocate IPs as either *exclusive*, meaning that a single user obtains the exclusive rights to this IP, or *shared*, meaning that this IP is shared among many clients (i.e. one IP can be used for hosting by many clients).


At this page, you can add and remove ip addresses, refresh the list of ip addresses, access ip properties editing.

To remove an IP from the network interface, select a checkbox corresponding to the IP you wish to remove, and click Remove Selected.

NOTE


You cannot remove the main interface IP from the Plesk control panel; the corresponding checkbox appears as disabled.

! IMPORTANT


When the new IP addresses appear on the interface, but are not displayed in the control panel, you may have to refresh the list of IP addresses manually. To do this, click  Reread IP.

Adding a new IP address

To add an IP to a Plesk managed server, follow these steps:

1. On the IP addresses management page, click the  Add IP Address

icon. The IP address adding page will open:

[Server](#) > [IP Aliasing](#) > **Add IP address**  Up Level

IP Address form

Interface	<input type="text" value="eth0"/>
IP Address *	<input type="text" value="192"/> · <input type="text" value="168"/> · <input type="text" value="42"/> · <input type="text"/>
Subnet Mask *	<input type="text" value="255"/> · <input type="text" value="255"/> · <input type="text" value="255"/> · <input type="text" value="0"/>
IP type	<input checked="" type="radio"/> Shared <input type="radio"/> Exclusive
SSL Certificate	<input type="text" value="default certificate"/>

* Required fields

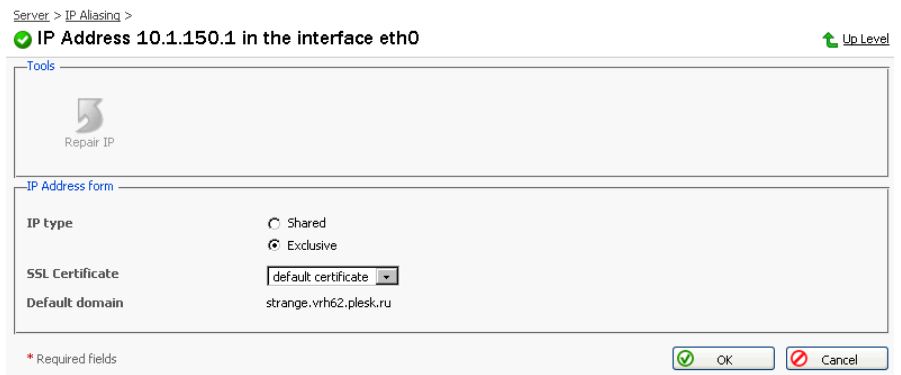
2. Using the Interface drop-down box, select the network interface the IP will be added to. Specify the appropriate IP address and Subnet Mask in the input fields provided. Define the IP address type (Shared or Exclusive) and select the SSL certificate to be used for the hosting accounts created using this IP.
3. Click OK to submit. Once submitted, the new address remains on the screen to facilitate the entry of multiple addresses.


i NOTE

You cannot add random IP addresses; they must be assigned.

Editing the IP address properties: changing the IP type, assigning a SSL certificate to an IP, repairing an IP

1. At the IP addresses management page, select the ip address you wish to edit. The IP editing page will open:



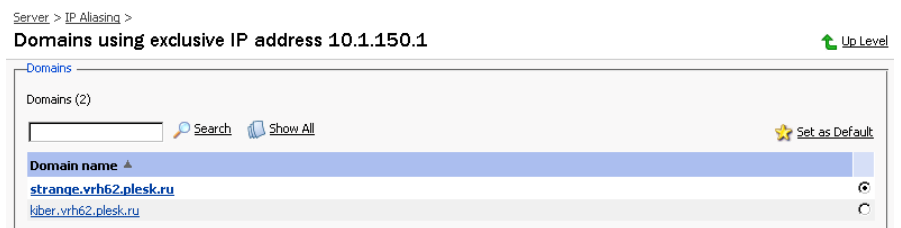
2. To change the IP address type to Shared or Exclusive, select the respective radio button.
3. To assign a SSL certificate to the IP, select the required SSL certificate from the drop-down list of certificates available from the repository.
4. In case if an IP address is missing on the interface, try restoring it using the  Repair IP icon.
5. Click OK to submit your changes.


Selecting a 'default domain'

The default domain seen in the IP properties is the domain, which has the highest priority defined in the web server configuration file over all domains using the given ip address for hosting. This means that all requests coming to the IP address and not recognized by Web server will be directed to the virtual host of the domain selected as default. If the default domain does not have physical hosting configured or the default domain is not assigned to the IP address, the request will be directed to the default virtual host. This feature allows accessing a domain by specifying an IP address in the address bar of the web browser.

To assign the default domain for the given IP address, follow these steps:

1. At the IP addresses management page, click on the number in the Hosting column of the list, corresponding to the necessary IP address. The page will open displaying the list of domains hosted using this IP address:




2. Select the domain using the corresponding radio button.
3. Click  Set as Default. Now the default domain is assigned.

Managing the clients granted a specific IP address


Accessing the list of clients sharing the same IP address

To access the list of clients, follow these steps:

- At the IP addresses management page, click on the number in the Clients column of the list, corresponding to the necessary IP address. The page will open displaying the list of clients who have this IP address in the IP pool:




Server > IP Aliasing >
Clients using Shared IP address 192.168.42.140  Up Level

Tools

 Add Client

Clients


Clients (1)

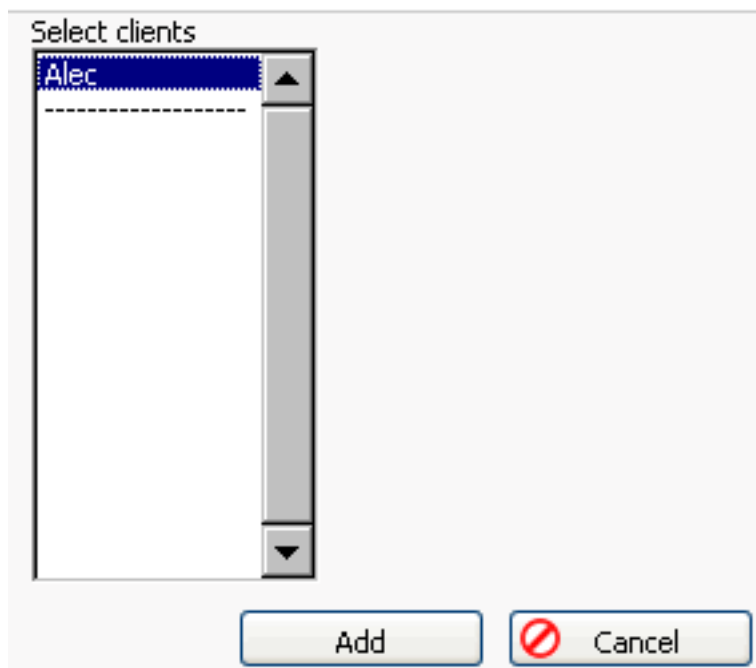
 Search  Show All  Remove Selected

Client name ▲	
client1	<input type="checkbox"/>

Adding IP address to client's IP pool

From this page you can add this ip address to the ip pool of a certain client:

1. Select the  Add Client icon on this page. The clients selection dialog window will open prompting you to select the clients to add the ip address to:



2. Select a client's name from the list.
3. Click Add.

Removing IP address from client's IP pool

From the list of clients who have the IP address in their pools:

1. Select the client you wish to remove an IP from using the checkbox.
2. Click Remove Selected. The confirmation page appears.
3. Select the checkbox to confirm and click OK.

Managing the DNS Zone Template

Plesk allows creation and use of default DNS Zone Template, intended to simplify setting up the DNS records for a freshly created new domain. This feature provides you with a number of DNS records that are more or less standard for a DNS zone.



In order to add a new DNS template record follow these steps:

1. Click the  DNS icon on the Server administration page. The DNS

Zone Template page appears:

Server >
DNS zone template Up Level


Tools

Disable   Default

Add a DNS record

Record type Add DNS record

DNS records

DNS records (8) Search  Show All Remove Selected

Host	Record type	Value	
<domain>.	A	<ip>	<input type="checkbox"/>
<domain>.	MX (10)	mail.<domain>.	<input type="checkbox"/>
<domain>.	NS	ns.<domain>.	<input type="checkbox"/>
<ip> / 24	PTR	<domain>.	<input type="checkbox"/>
ftp.<domain>.	CNAME	<domain>.	<input type="checkbox"/>
mail.<domain>.	A	<ip>	<input type="checkbox"/>
ns.<domain>.	A	<ip>	<input type="checkbox"/>
webmail.<domain>.	A	<ip>	<input type="checkbox"/>

The DNS Zone Status icon at the top of the page indicates whether the DNS is turned on or off.

2. Select the type of record you wish to add from the Record type drop-down box and click Add DNS record. The DNS Zone Template Records Editing page appears:

Server > DNS >
Add A record for zone Up Level

Add a DNS record

Enter domain name * <domain>.

Enter IP address *


* Required fields OK Cancel

3. Fill the required information into the input fields (the type of the information required depends on the type of the DNS record selected).
4. Click OK to submit the entered data and add the new record to the template.

NOTE

The following domain name and host IP templates can be used:
 <domain>, which is then replaced with the domain name, and <ip>, which is replaced by the primary IP address.

In order to remove a DNS record from the template, select a record using the checkbox, and click Remove Selected. The confirmation dialog box will appear. Click OK to confirm. The record will be immediately removed.

- If you wish to turn the DNS on for the template, click  Enable, or click





Disable to turn it off.

- Turning the DNS zone off will refresh the page, so that only a list of nameservers remains:

Server >
DNS zone template Up Level

Tools

 Enable  Default

Add a DNS record

Record type: nameserver Add DNS record

DNS records

Name servers (1)

Search Show All Remove Selected

Name server ▲	<input type="checkbox"/>
ns.<domain>	<input type="checkbox"/>

- If you are running remote DNS, and therefore want to turn DNS off, you should create the appropriate NS entries to be stored in the template. To add a nameserver: click Add DNS record, enter the nameserver in the appropriate input field, and click OK.

To restore the default DNS zone template, click the  Default icon.

Configuring SOA records parameters

The can customize the SOA records parameters via the database. The following SOA records parameters can be adjusted:

- SOA_TTL
- SOA_Refresh
- SOA_Retry
- SOA_Expire
- SOA_Minimum

The values of these parameters are stored in the "misc" table of "psa" database. If some of these parameters do not exist in the "misc" table, the default settings will be used. To set the new SOA records parameters, you

need to insert the above parameters into the "misc" table with the new values.

Example:

```
# mysql -uadmin -p`cat /etc/psa/.psa.shadow` -D psa -e  
"INSERT INTO misc VALUES ('SOA_TTL','86400');"
```

If you have already set the SOA parameters, and need to change the current settings, you can do it using the command like below:

```
# mysql -uadmin -p`cat /etc/psa/.psa.shadow` -D psa -e  
"UPDATE misc SET val='43200' WHERE param='SOA_TTL';"
```

Updated SOA parameters will be set for the newly created domains. If you need to update the SOA for an already existing domain, run the following command from the shell:

```
/usr/local/psa/admin/sbin/dnsmng update domain.name.com.
```

Managing Client Templates

Client template is a predefined set of restrictions and permissions intended to simplify creation of new client accounts with automatic assignment of settings to them. For instance, you can create a client template that will allocate a shared IP address, so that you would not have to manually add the IP address to a client's IP pool each time a new client account is created.


You can use a client template to assign any of the following parameters to a client account:

- Ability to create domains
- Ability to manage physical hosting
- Ability to manage hard disk quota
- Ability to manage subdomains
- Ability to change domain limits
- Ability to manage DNS zone
- Ability to manage log rotation
- Ability to manage crontab
- Ability to manage anonymous FTP
- Ability to manage web applications
- Ability to manage system access
- Ability to manage mailing lists
- Ability to use the backup/restore functions
- Maximum number of domains and subdomains
- Amount of disk space available
- Amount of traffic allowed
- Maximum number of web users
- Maximum number of databases

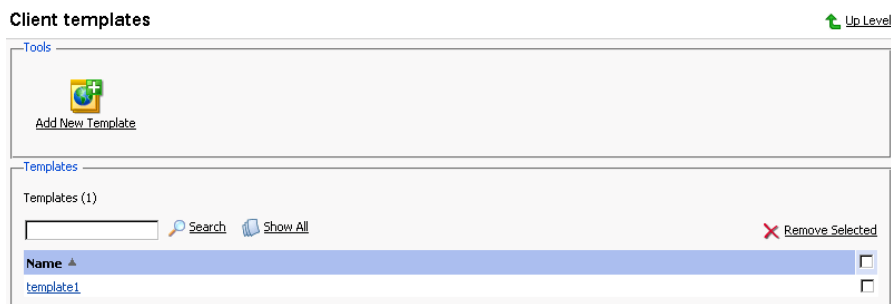
- Maximum number of mailboxes
- Mailbox quota
- Maximum number of mail redirects
- Maximum number of mail groups
- Maximum number of mail autoresponders
- Maximum number of mailing lists
- Maximum number of Tomcat web applications
- Client account validity period
- IP addresses allocation
- Number of lines to be displayed in the interface pages viewed by client


Creating a client template

To create a new client template, follow these steps:

1. Select the Clients shortcut in the navigation pane.
2. Click the  Client Templates icon. The Client templates management

page appears:



3. Click  Add New Template. The Template creation and editing page appears.
4. Enter the name for the client template in the Template name field. In the Permissions group, select the appropriate checkboxes to grant all necessary permissions to the client. In the Limits group specify the limits to be applied: uncheck the "Unlimited" checkboxes and type in the values for the parameters. To limit the client account validity period, uncheck the corresponding "Unlimited" checkbox, select the time unit in the drop-down list (it can be Years, Months, Days) and type in the value.

Select shared ip addresses from the list to be used for the client's hosting accounts, add new ip addresses to the list clicking on the Add button, and remove them by selecting an ip address and clicking Remove.

Check the Allocate exclusive ip addresses to the client checkbox to ensure that the client is provided with exclusive ip addresses. Specify the maximum number of exclusive ip addresses to be allocated.

Enter the number of lines to be displayed on a page.

5. Click OK to submit settings, or click Cancel to discard unsaved settings and return to the Client templates management page.

The template will be added to the list of client templates and become available as option during creation of a new client account.

Editing a client template

To edit a client template:

1. On the Client templates management page, select the template you wish to edit by clicking on its name in the list. The Client Template Editing page will open, allowing you to change the desired options. Settings that can be configured on that page are absolutely the same as on the Client Template Creation page.
2. Click OK after you are done with configuring the template.

Removing a client template

1. On the Client templates management page, select the template you wish to remove by putting a checkmark in the checkbox related.
2. Click Remove Selected. The confirmation page appears.
3. On the confirmation page, check the checkbox to confirm, and click OK.

Managing Domain Templates

Domain template is a predefined set of domain-specific restrictions, options, and hosting parameters, intended to simplify creation of domains with automatic assignment of settings to them.


Use the domain template to assign the following parameters:

- Mail bounce configuration
- Maximum number of subdomains
- Disk space limit

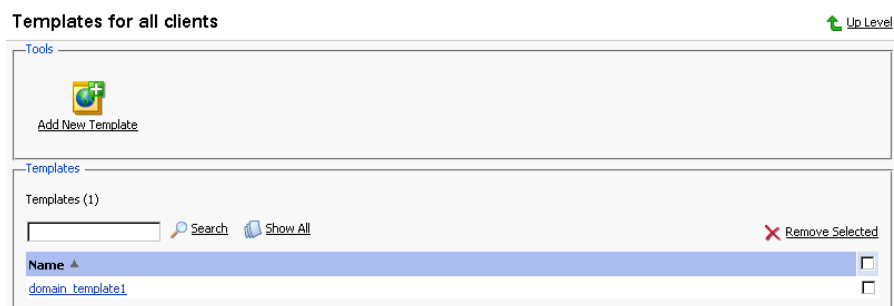
- Maximum amount of traffic allowed
- Maximum number of web users
- Maximum number of databases
- Maximum number of mailboxes
- Mailbox quota
- Maximum number of mail redirects
- Maximum number of mail groups
- Maximum number of mail autoresponders
- Maximum number of mailing lists
- Maximum number of web applications
- Domain validity period
- Log rotation settings
- Scripting capabilities
- Webmail accessibility
- Mailing lists availability
- Traffic statistics retention period
- Domain DNS zone type
- Virtual host type
- Hard disk quota
- SSL support
- Microsoft FrontPage support,
- Microsoft FrontPage over SSL support,
- Microsoft FrontPage Authorization
- Apache ASP support
- SSI support
- PHP support
- CGI support
- mod_perl support
- mod_python support
- ColdFusion support
- Web statistics
- Use of Custom Error Documents


Creating a domain template

To add a new domain template, follow these steps:

1. Select the Domains shortcut in the navigation pane.
2. Click the  Domain Templates icon. The Domain templates

management page appears:



3. Click  Add New Template. The Template creation and editing page appears.
 4. Enter the name for the domain template in the Template name field.
 5. Set the Mail to nonexistent user option to Bounce with phrase or Catch to address, and enable Webmail, if desired.
 6. Use the Limits group to define the resource usage limits for domains. To set the necessary parameters, deselect the Unlimited checkboxes, and type the limit values into the input fields.
 7. To define the domain validity period, deselect the Unlimited checkbox, type the value into Validity period input field, and specify the time measurement unit (years, months, or days).
 8. Select the Enable log rotation checkbox to enable it. Select the log rotation condition: to be based on log file size, or time (select from Daily, Weekly, Monthly). Specify the maximum number of log files, enable log files compression, and specify an e-mail address for the processed log files to be delivered to.
- i NOTE**

It is advisable to set the logrotation options appropriately in order to prevent the log files from growing too large to be handled by the statistics utility.
9. To enable Mailing lists, select the corresponding checkbox.
 10. To retain the traffic statistics for domains, select the corresponding checkbox and specify the retention period in the Retain traffic statistics for ... Months field.
 11. Select the domain DNS zone type using the Master or Slave radio button.
 12. To enable physical hosting for domain, select the Physical hosting

checkbox.

13. Specify the hard disk quota in the appropriate field, if needed.
14. SSL support checkbox enables the maintenance of https protocol.
15. To allow the use of Microsoft FrontPage Server Extensions, check the checkbox for Microsoft FrontPage support and Microsoft FrontPage over SSL support. Authorization will be disabled by default. For security reasons, authorization should only be enabled when Microsoft FrontPage extensions are in use.
16. Use the remaining checkboxes to enable the following hosting features:
 - Allow the web users scripting: enable support for scripting in web users' pages.
 - ASP support: ASP module enabled.
 - SSI support: Server Side Includes scripting enabled.
 - PHP support: supports html documents that contain PHP scripts.
 - CGI support: an individual cgi-bin directory is created and CGI scripting is enabled.
 - mod_perl support: Perl scripting enabled.
 - mod_python support: Python scripting enabled.
 - ColdFusion support: ColdFusion scripting enabled.
 - Web statistics: keeping the hits statistics for the domain.
 - Custom Error Documents: allow the use of custom pages in case of web server errors.
17. Click OK to apply the changes made.

The template will be added to the list of domain templates and become available as option during creation of a new domain.

Editing a domain template

To edit a domain template:

1. On the Domain templates management page, select the template you wish to edit by clicking on its name in the list. The Domain Template Editing page will open, allowing you to change the desired options. Settings that can be configured on that page are absolutely the same as on the Domain Template Creation page.
2. Click OK after you are done with configuring the template.

i NOTE

When altering a template, nothing will change for the domains that were previously created using this template.

Removing a domain template

1. On the Domain templates management page, select the template you wish to remove by putting a checkmark in the checkbox related.
2. Click Remove Selected. The confirmation page appears.
3. On the confirmation page, select the checkbox to confirm, and click OK.

Managing Custom Buttons

You can add to the control panel any number of custom buttons that will be linked to a specific URL, and choose to either make them visible to all of your customers, or only to yourself. The buttons you create from Administrator's repository of custom buttons can be placed in any of the following locations:

- Navigation pane;
- Domain Administration pages of all domains;
- Each Client's (Reseller's) Home page.

You access the administrator's repository of custom buttons clicking the



Custom Buttons icon on the Server administration page.

i NOTE

If you wish to create individual buttons that will be placed only on a specific Client's Home page, you should access the required Client Home page and click Custom Buttons. To create the buttons for a specific Domain Administration page, you should access the required Domain Administration page, and click Custom Buttons.

To create a new custom button, follow these steps:

1. When on the Custom buttons repository page, click



Add New

Button. The Custom button properties page opens.

2. Type the button label in the Button label field.
3. Choose the location for your button.
4. Specify the priority of the button. It will be used by the control panel for defining the button layout order in cases when there are several custom buttons on a page.
5. You can use an image for a button background. To do this, type in the path to its location or click Browse to browse for a file. It is recommended to 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.
6. Type the URL link to be attached to the button into the URL field.
7. Using the checkboxes, specify whether to include the data, such as domain id, domain name, client id, company name, client's contact name, and the client's e-mail to be transferred within the URL. These data can be required for processing by external web applications.
8. In the Context help tip contents input field, type in the help tip that will be displayed when users hover the mouse pointer over the button.
9. Select the Open URL in the Control Panel checkbox if you wish the destination URL to be opened in the control panel's right frame, otherwise leave this checkbox unchecked to open the URL in a separate browser window.
10. If you wish to make this button visible to other users (sub-logins), select the Visible to all sub-logins checkbox.
11. Click OK to complete creation.

Once a new button is created it appears in the list of custom buttons in the repository.

To change the properties of a button, select its label in the list. Note, if you wish to make a button visible/invisible to other users (sub-logins), you can simply click an icon in the A column of the list.


To delete one or several buttons, select the corresponding checkboxes, and click Remove Selected.

Managing Skins

All control panel skins are stored in the Skins repository. This is the location where you can manage the skins: add your custom skin packages and remove the unused ones.

To access the Skins repository, select the Server shortcut in the navigation pane, and click Skins. All available control panel skins and their properties will be presented in a list: skin name, description, author, number of users, who are using a given skin for their control panel environments.

To upload your own skin, click Add New Skin. Specify the skin package file location and click OK.

To download a skin package, click the appropriate  icon in the list, or click on a skin title and then click Download Skin. Select the type of archive you would like to have the skin files packed into, and click OK. Once the skin is prepared for downloading, a file download dialog window appears. Click Save, specify the location and file name for the downloaded skin package file to be saved, and then click Save.

In cases when you need to update the skin contents, click on a skin title and then click Update Skin. Specify the skin package file location and click OK.

To remove one or several skins from the repository, select the corresponding checkboxes and click Remove Selected.

NOTE

When you remove a skin, which is currently used within a certain user's control panel environment, the user's control panel appearance is automatically changed to the default skin. You cannot remove the default control panel skin.

Managing Virtual Host Skeleton

Skeletons are file structure templates, which are used for fast automatic creation of predefined virtual host content when creating a physical hosting.

Skeleton file may contain the following top-level directories only:

- httpdocs
- httpsdocs
- cgi-bin
- anon_ftp
- error_docs

All other directories will be ignored during skeleton deployment.

Allowed skeleton file types are *.tgz and *.zip archives.

Creating a skeleton

Follow these steps to create a skeleton:

1. Create the required directories (available directories are: httpdocs, httpsdocs, cgi-bin, anon_ftp, error_docs)
2. Place the necessary files into the directories. These files will appear in the corresponding directories of each domain that will be created and set-up on physical hosting.
3. Pack those directories and files into an archive file. Make sure that the skeleton directories are located in the root of the archive file and not in a subdirectory.


Now the skeleton file is ready to be uploaded.

Activating a Skeleton

To activate a new custom skeleton, follow these steps:


NOTE

Each new skeleton replaces the previously used one. Now, the new skeleton will be used in the process of creating all new physical hosting instances until it is replaced by another skeleton (new or the default one).

1. Click the  Skeleton button on the Server administration page. The Skeleton management page will open.
2. Select the archive file that contains the skeleton. Use the Browse button to locate the desired file.
3. Click Send File. The new skeleton will be uploaded and activated.

You can always revert to using the default skeleton. To do so, just click the Default button on the Skeleton management page. The default skeleton will replace the currently used one and will be activated.

Scheduling Crontab Tasks


To access the crontab management functions, click the  Crontab

Manager icon on the Server administration page. The Crontab management

page will open:

Crontab tasks [Up Level](#)

Tools

 [Add New Task](#)



Preferences

Show Crontab of:

Send Crontab messages to address:

Tasks

Crontab tasks (2)

S	M	H	DM	M	DW	Command	
	7	4	*	*	*	/usr/local/psa/admin/sbin/statistics_>/dev/null 2>&1	<input type="checkbox"/>
	14	5	*	*	*	/usr/local/psa/bin/mysqldump.sh_>/dev/null 2>&1	<input type="checkbox"/>

On this page, you can view scheduled tasks of various system users, set the e-mail address for the crontab messages to be sent, schedule new tasks and remove them.


The Show Crontab of: drop-down box indicates the system user, whose scheduled tasks are currently displayed. It also allows to select another system user to view and/or manage scheduled tasks that belong to that user.

Each line in the Crontab task list represents a single task. The Status (S) column shows whether the selected task is enabled or disabled (the disabled tasks are not executed). The Command column contains the command that is executed within the selected task and serves as a link to the page that allows editing the selected scheduled task properties.

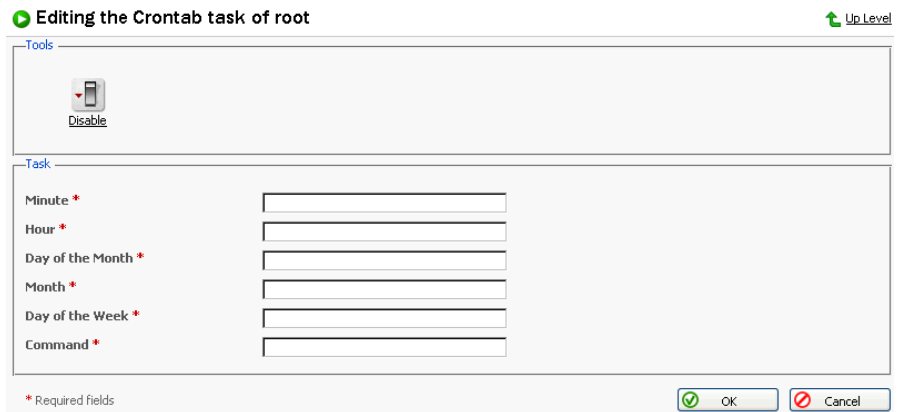
The task list can be sorted by its parameters in ascending or descending order. To sort the task list, click on the name of the sorting parameter. An arrow will show the order of sorting. The sorting criteria are:



- (S)tatus
- (M)inute
- (H)our
- (DM) Day of the Month
- (M)onth
- (DW) Day of the Week
- Command

To add a new task to the list, follow these steps:

1. Click the  Add New Task icon on the Crontab management page.

You will be taken to the crontab record creation/editing page:



2. Choose the status of the scheduled task by clicking the  Enable or  Disable icon. The current status is displayed by the corresponding icon.
3. Specify the date and time for the task to be executed: Minute - enter the value from 0 to 59 or *, Hour - enter the value from 0 to 23 or *, Day of the Month - enter the value from 1 to 31 or *, Month - enter the value from 1 to 12 or *, Day of the Week - enter the value from 0 to 6 (0 is Sunday) or *.
4. Type in the command to be executed in the Command input field.
5. Click OK.

To delete one or several scheduled tasks from the list, select the corresponding checkboxes and click Remove Selected.

To enable crontab to send the messages to a specified e-mail address, enter the e-mail address into the Send crontab messages to address: text input field and click Set. All scheduled tasks from the displayed list that output some information will automatically have their output sent to the specified address. The "" entry in this field specifies that the sending crontab messages option is disabled.

Scheduling Report Deliveries

You can schedule daily, weekly, or monthly deliveries for client and domain reports.

For a client report, you can choose to deliver:

- a report on a specific client to an e-mail address,

- a report on a specific client to administrator's e-mail,
- a report on a specific client to the client's e-mail address,
- the account status report to every client.

For a domain report, you can choose to deliver:

- a report on a specific domain to an e-mail address,
- a report on a specific domain to the administrator's e-mail,
- a report on a specific domain to the client's e-mail address,
- a report on a specific domain to the domain user's e-mail address,
- reports on every domain to the respective clients,
- reports on every domain to the respective domain users.

To manage domain report deliveries, click the Report icon on a domain administration page, and then click Report Delivery.

To manage client report deliveries, click the Report icon on a client home page, and then click Report Delivery.

To schedule the report delivery:

1. Click Add Delivery Schedule.
2. Select the report recipient (or recipients): it can be a registered control panel user or an e-mail address. If the E-mail address option is selected, type the address in the input box.
3. Select the delivery frequency: daily, weekly, or monthly.
4. Click OK to submit.

Once a schedule is created, the corresponding entry is added to the list. To edit a delivery schedule, select a corresponding record in the Frequency column.

To remove a schedule, select a corresponding checkbox and click Remove Selected.


Using Application Vault

Application vault is the location where you store all site application packages that can be easily deployed at any domain hosted on the server.

There are two types of site applications in Plesk:

- free, requiring no license key;
- commercial, requiring a license key;




Plesk goes with a number of free site applications requiring no license key that you can choose to install on your Plesk. All free site applications installed on your Plesk are automatically added to the application pool of each client created in Plesk. However, the commercial applications can be added to the client only upon purchase.

To access the Application Vault, click the  Application Vault icon at the



Server administration page. The Application Vault opens.

All applications stored in the vault are listed in the Site Application Packages area.

The icon in the first left column indicates the type of the site application:

-  - the free site application requiring no license key, included in the default installation of Plesk for free, automatically added to the application pool of each client created in your Plesk control panel.
-  - the commercial site application requiring a license key, purchased from SWsoft, Inc. additionally.
-  - the commercial site application requiring a license key, purchased from SWsoft, Inc. additionally, with no key installed at the moment.

The icon in the second column left to the site application name indicates the site application usage rules defined by the administrator:

-  - free of charge, automatically added to the application pools of all clients;
-  - commercial, added to a client application pool only by the administrator under certain conditions.

You can set usage rules for any site application in the vault. For example, you can make a certain free application a commercial one that will be available to your clients only if you add it to their application pools under your conditions. To make a certain free application a commercial one or vice versa, click the icon in the second column left to the corresponding site application name. When you change a free site application into a commercial one, it is withdrawn from the application pools of all clients. Now only you can add this application to your clients' application pools when needed. When you change a commercial application into a free one, it becomes free of charge for all clients. To revert to

the previous state of the site application, click the icon again.



You can also change the usage rule for an application clicking on the application name. The Site application properties page will open. Select a required value in the Access level drop-down box, and click OK.

The Name column displays the name of the site application. The site application version is presented in the Version column. The Release column shows the site application release number. The Instances column denotes how many times the application package was deployed. The Clients column shows the number of clients using the site application. A brief description of the site application is given in the Description column.

NOTE

You can add an application to a client's application pool right from the Server application vault. To do this, click on the number of clients, then click Add New Client. A dialog window will appear. Select a client and click Add.

Adding an application package to the Vault

1. Click  Add New Application. Select the application package file using the Browse... button and click OK. The selected application package will be uploaded and registered in the database.
2. Refresh the Application Packages list
In order to view all installed packages, please refresh the Application Packages list. Click the  Refresh icon. Refresh the Application Packages list every time you manually install or remove an application package.
3. View info on application
You can view information on available application packages by clicking on the application package name in the list.
The information states the name and the version of the package, a brief description as well as a set of requirements that must be fulfilled in the domain hosting setup in order for the application to function.
4. Removing application packages
In order to remove one or several application packages, select the

corresponding checkboxes and click Remove selected.

If an application from a removed package was installed on a domain it will remain there, but all the information about it will be removed from the Plesk database.

Installing application on domain

1. Select a domain with configured physical hosting and click the




Application Vault icon in the Hosting group.


2. Click the



will open.

3. Select the application package you wish to install on the selected domain. Note: you can also choose to install it on a subdomain – select it in the Target domain drop-down menu.

You can view information on available application packages by clicking on the application package name in the list. If there is a documentation available for the application, it will be accessible through the icon .

4. Click  Install.
5. Some applications require that certain parameters be entered before executing the installation. The required parameters are marked with an asterisk.

You have an option of creating a custom button for accessing this application. The button can be placed on the administration page of a given domain, on the administration pages of all domains, belonging to this client, or all domains hosted on server.

6. Click Finish once you are done editing the required parameters. If you chose to create a custom button for the application, you will be taken to the custom button properties page.

Note: It is not allowed to install one application into a sub-directory of another application. However, most applications allow installing several copies for the same domain but in different directories.

When the installation of the application is complete, the application will appear on the Applications list.





To edit the application settings, click on the corresponding icon .

Use the  icon in the Applications list to access the URL of the application.

To remove one or several applications, in the list of applications select the corresponding checkboxes and click Remove Selected.

Managing User Sessions






You can monitor and manage the currently active control panel and FTP user sessions from the control panel. To access the user sessions management functions, select the Sessions shortcut in the navigation pane. The current control panel user sessions will be presented in a list:

- Type: a control panel user who established the session -  for Administrator's session,  for Client's session,  for Domain User's session, and  indicates that the session was established by the Mail User.
- Login column displays the user's system login,
- IP address: the IP address the control panel is accessed from,
- Logon time: the date and time the session was initiated,
- Idle time: the session idle time.

Click Refresh to refresh the list of user sessions.

To end a control panel user session, select the corresponding checkbox and click Remove Selected.

To manage the FTP sessions, click the FTP Sessions tab. The properties of FTP sessions will be presented in the list:

- Type: the type of user who established the session -  for users not registered in the control panel,  for anonymous FTP users,  for Domain owner's sessions,  for subdomain user's sessions, and  for web user's sessions.
- Status: the current status of FTP connection,
- FTP user login: the user's FTP login,
- 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: speed in Kilobytes,
- %: the file transfer operation progress in percentage,
- IP address: the IP address the FTP account is accessed from,
- Logon time: user logon time,
- Idle time: session idle time.

To refresh the list of FTP sessions, click Refresh.

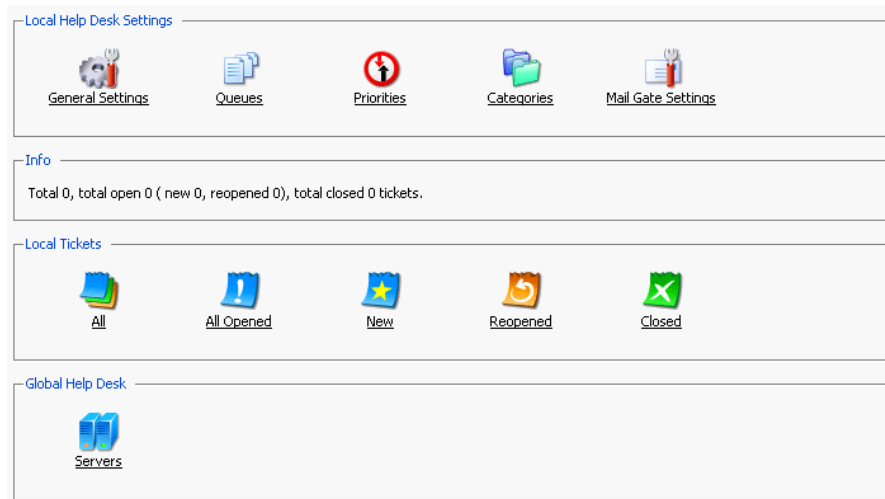
To end a session, select the corresponding checkbox and click Remove Selected.

Operating Help Desk


Being the administrator you cannot submit new tickets to the Help Desk, but only post comments and change the state of submitted tickets: for instance, close the ticket when the issue is resolved or reopen if the problem persists.

To view the submitted tickets, follow these steps:

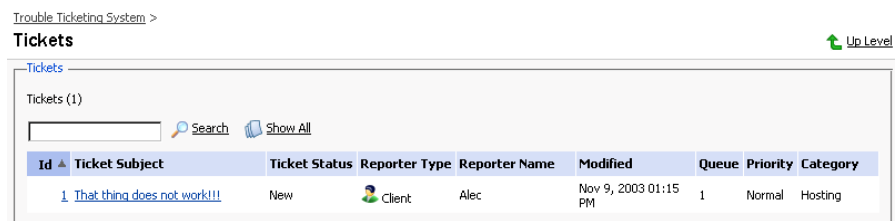
1. Select the Help Desk shortcut in the navigation pane. The Help Desk's main page opens:



2. In the List Local Tickets group, select an appropriate icon in order to list all trouble tickets with the designated status: All, all opened, new, reopened, closed.

3. Click  All to list all existing trouble tickets in any state. The page will

open listing all existing trouble tickets and their properties:



- Id: identification number assigned by the system upon submission,
- Ticket Subject: a summary entered by the problem reporter,
- Ticket Status: new, reopened, closed,
- Reporter Type: a type of Control Panel user that submitted the ticket - client, domain owner, mail name user or e-mail for tickets submitted by e-mail,
- Reporter Name: a name of person who submitted the ticket, or an e-mail address for tickets submitted by e-mail,
- Modified: the date the ticket was modified - a comment appended, or status changed,
- Queue: the queue number assigned,
- Priority: the priority defined,
- Category: the category the trouble ticket is related to.

To change the status of a ticket or add a comment:

1. Click on a ticket id or subject. This page will open displaying all comments made to the ticket, and allowing you to change the ticket properties and

add new comments:

[Trouble Ticketing System](#) > [Tickets](#) >

Ticket 1 [Up Level](#)

Ticket


Ticket Status	New
Client	Alec
Ticket Subject *	<input type="text" value="That thing does not work!!!"/>
Category	<input type="text" value="Hosting"/>
Priority	<input type="text" value="Normal"/>
Queue	<input type="text" value="1"/>

New Event

Ticket Event	<input type="text" value="Comment ticket"/>
Visible to client	<input checked="" type="checkbox"/>
New Comment	<input type="text" value="Please elaborate ..."/>

* Required fields

Ticket History

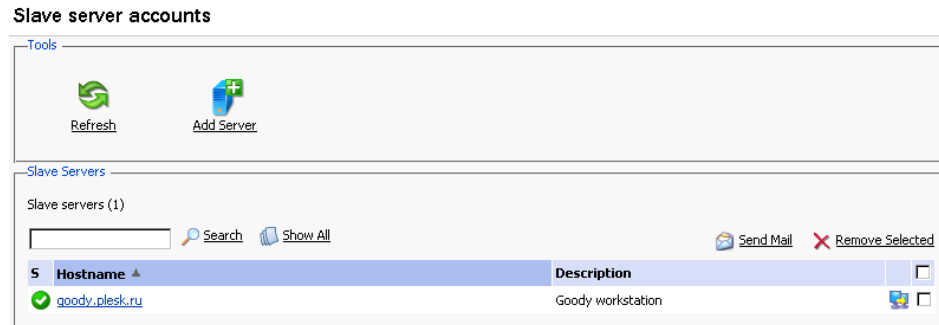
Nov 9, 2003 01:15 PM	 Alec < alec@plesk.ru >
Help! I need some qualified assistance...	

2. To change the ticket subject, edit it in the Ticket Subject field as desired. To assign a new category, priority or queue to the ticket, select the desired values in the corresponding drop-down boxes.
3. To add an event to the ticket, i.e. close, reopen and/or comment it, select a corresponding action in the Ticket Event drop-down box, type a new comment into the New Comment input field if required, select the Visible to users checkbox to inform other users of this event.
4. Click OK to submit all changes.

Master Feature






Provided that there are a number of Plesk servers networked, the Master feature empowers Administrator to log on to other Plesk enabled servers, manage them remotely and monitor their status information from a single point of entry - a Plesk master server control panel.

As an administrator using Plesk, you can perform a variety of slave server management tasks in a few clicks. When you are logged on as an administrator, select the Master shortcut in the navigation pane to access the slave servers management functions: registering a new slave server, editing a slave server account, and logging on to a slave server.



The slave servers management page also lists all slave server accounts registered with the system. Each list item representing a slave server is accompanied by the following icons:


Table 3.1. The slave server status icons.

Icon	Meaning
	means that the slave server is functioning normally
	means that some system service at the slave server is experiencing problems
	means that on the slave server some client has exceeded allocated disk space or traffic limitations in at least one of the client's domains. The Plesk system evaluates disk space and traffic every 24 hours
	means that the slave server is currently down, disabled or inaccessible
	means that the slave server information is not requested

You can send an e-mail message to administrator of a slave server. To do that put a check mark in the corresponding checkbox, and click Send Mail.

Registering a Slave Server Account

To add a new slave server account, follow these steps:

1. Access the slave servers management function by clicking on the Master shortcut in the navigation pane. The Slave Servers Administration page appears.
2. Click  Add Server. The Slave server account page will open:

[Slave server accounts >](#)

Slave server account [Up Level](#)

Preferences

Hostname *	<input type="text"/>	:	<input type="text" value="8443"/>
Login *	<input type="text" value="admin"/>		
Password *	<input type="password"/>		
Description	<input type="text"/>		
Do not request information from the server	<input type="checkbox"/>		

Info

Slave server information is not currently available.

3. Enter the hostname and port number in the appropriate fields, enter login name, and password for Plesk to be able to log on to the given slave server. You may also wish to type in a description for the slave server. Select the Do not request information from the server checkbox, if you do not wish the detailed slave server information to be retrieved.
4. Click Set. The Slave server account page will be updated with server details and statistics:

[Slave server accounts >](#)

Slave server account [Up Level](#)

Preferences

Hostname * :
 Login *
 Password *
 Description
 Do not request information from the server

Info [Refresh](#) [Login](#)

Key number	plsk000000000000
OS	Linux 2.4.18-17.7.x
Version	psa v7.0.0_build031125.15 os_RedHat 7.3
CPU	
System Uptime:	9:02
CPU usage	
Last 1 minute	0%
Last 5 minutes	0%
Last 15 minutes	0%
Clients	14
Problem clients	0
Domains	13
Active domains	11
Domains with hosting	8
Problem domains	0
Databases	2
Database users	2
Web users	3
Mail autoresponders	1
Mail groups	1
Mail redirects	4
Mailboxes	3
WEB Server status	✔
FTP Server status	✘
SMTP server status	✔
POP3 Server status	✔
IMAP Server status	✔
DNS Server status	✔

- To manage certificate for the server use the Certificate button. You will be taken to Slave server certificate management page:

Slave server accounts > Slave server information >
Slave server kan.plesk.ru certificate setup Up Level

File

Upload certificate file

Text

Enter certificate text

You can copy and paste the certificate content into appropriate field or simply browse to its location by clicking the Browse... button. After that, click on Send File or Send Text buttons respectively to submit the certificate, or use the Up Level button to discard any changes and return to the Slave server account page.

To refresh information on the slave server, click Refresh.

To log on to the slave server, click Login. The Plesk control panel of the remote slave server will open in a new browser window.



Editing a Slave Server Account

Occasionally, you may need to change the information in a slave server account. This may occur if the slave server login information was changed.

1. In the list of slave server accounts, click on the host name of the slave server whose account you wish to edit. The Slave server account page appears, displaying detailed slave server account information.
2. Click in any text box to edit the information.
3. When you are done editing, click Set to save the changes made. The changes will take effect immediately.

Logging on to a Slave Server

There are two ways you can log on to a slave server:

- On the Slave Servers Administration page, select the slave server you wish to log on to and click the corresponding  icon.
- You can also use the  icon located on the Slave server account page.

Removing a Slave Server Account

You can remove one or several slave server accounts at once. To remove a server (servers):

1. Select the checkboxes corresponding to the servers you wish to remove.
2. Click Remove Selected. The Slave Server Removal page appears.
3. Select the checkbox to confirm removal, and click OK.

Viewing Server Statistics

Plesk compiles statistics on server usage. You can access this information at any time. The report is especially helpful if the server is slow or is experiencing performance problems, it may help you diagnose and correct such problems.

The report lists several informative statistics:

CPU: This gives a description of the CPU of your server.

Version: This provides with the version of Plesk you are running.

OS: Displays operating system version.

Key Number: This will report the key number for your Plesk license.

System Uptime: How long the server has been available without interruptions such as those from rebooting or shutting down the operating system.

CPU usage (load averages for the last minute, 5 minutes, and 15 minutes): The average number of processes waiting in the scheduler queue for execution in the last time frame.

Memory Usage: displays the amount of memory used

Swap Usage: displays the amount of swap space used

Hard Disk Usage:



- *Filesystem* - the hard disk drive partitions used.

•

Domains:


- *Active* - How many domains are currently turned on
- *Problem* - How many domains exceed disk space and traffic limitations but are still available
- *Passive* - How many domains are turned off (either by the administrator or the client) and not working

To access the System Statistics page, follow these steps:

1. Click the  Statistics icon on the Server administration page. The system statistics report appears.
2. Click  Refresh to update the server statistics with the latest data.


To print out a copy of the statistics, use your browser's File/Print command.

Viewing Information on Plesk Components

To access information on the components controllable under Plesk, select the  Component Info icon on the Server Administration page. The

component information is presented in a table:

[Server](#) >


Information on Plesk components  [Up Level](#)

[Info](#)

Component name	Component version
apache	1.3.23-10
bind	9.2.1-1.7x:2
courier-imap	1.7.3-40psa.rh2.1AS
frontpage	5.0.2.2634
mailman	Component was not installed
mysql	3.23.41-1
postgresql	Component was not installed
stunnel	3.22-1
webalizer	2.01_09-0.72
php	4.0.6-16
mod_python	2.7.8-1
coldfusion	Component was not installed
psa-qmail	1.03-rh2.1AS.build040124.14
psa-proftpd	1.2.9-rh2.1AS.build040124.14
psa-logrotate	3.6.6-10.rh2.1AS
psa-spamassassin	7.0.0-rh2.1AS.build040124.14
tomcat4	4.1.24-full.2jpp
mod_perl	1.26-2
perl-Apache-ASP	2.49-30psa

Submitting a Request for Online Server Support

You can request online server support service directly from the Plesk control panel.

To do that, click the  Support icon on the Server administration page.

You will be taken to the Online Server Support form at the SWsoft's web site. Fill out the form and enter all the information required. Click Submit Request. Your request will be encrypted and delivered to the technical support staff.

i NOTE

It is highly important to make sure that you provided all the information required, otherwise the form will not be accepted. The request will be assigned a unique request identification number that is generated for your request to be addressed and will be valid until your issue is solved.

Updating Plesk

Using the Plesk Updater feature you can easily install the necessary updates, control panel add-ons, and even upgrade your control panel to the latest available release in a few steps:

1. At the Server Administration page click Updater. The control panel connects to the Plesk Update server, retrieves information on the available releases, then analyses the components installed in the system, and displays the lists of available releases and component updates. For each release a brief description of available operations is displayed.
2. Select the release version that you want to update, or upgrade to. A list of available components appears.
3. Select the checkboxes corresponding to the components you wish to install and click Install. A confirmation page appears.
4. Specify the e-mail address. You will be sent a notice by e-mail once update is completed. To confirm installation of the selected components, select the checkbox and click OK. The components/updates you selected will be downloaded and automatically installed in the background mode.

Notes on updating procedures

- When upgrading to a new control panel version, you will be notified by e-mail of upgrade procedure start and end. The notification message will include the event log and a list of installed packages, if upgrade is successful. However, you may not receive any error notice if your mail server fails. In this case you can check for errors in the `autoinstaller.log` file located in the `/tmp` directory on the server hard drive.
- All control panel operations are suspended during installation of the so-called “base” packages that affect the control panel’s core functionality.
- After upgrading your control panel to a new version you will need to install a new license key. To obtain an appropriate license key, use the License Manager function in the control panel. If you experience any problems,

please contact sales@sw-soft.com

Changing Updater Settings

By default updates are downloaded from the Plesk Update server. If you prefer updating from a local network storage, you should change the default settings. To do this:

1. Click Settings.
2. Select the Local network storage option and specify the URL to the directory where updates reside.
3. Click OK to apply settings.

License Management

Using the License Manager feature you can

- Order add-ons or upgrades for your Plesk version.
- Order key upgrades, and purchase new license keys.
- Retrieve the ordered keys from the SWsoft server. Plesk retrieves the license key and automatically installs it to your control panel.
- Upload the necessary license key from your local machine to your Plesk server.
- Roll back the installed licensed key.

The license manager is available to the administrator even if a license key is expired.

Upgrading Default Key

When you download Plesk from the SWsoft website, it goes with the default key. This key has limited functionality. To upgrade the default key to the license key with basic Plesk functionality, do the following:

1. Select the Server shortcut in the navigation pane.
2. Click the License Management icon on the Server administration page.
3. On the License Management page, click the Order Control Panel Upgrades icon.
4. This will take you to the SWsoft online store that will open in a separate

browser window. When there, please select the desired features for your license, provide the purchase details and billing address, specify the payment method, and place your order. Once you placed it, your order will be sent to the online store operator. The new key will be sent to your e-mail when your order is processed.

Note

Here you will only be able to order Domains upgrade. By ordering upgrade to a certain number of domains, you buy thus the new license key with the basic Plesk functionality and the ordered number of domains included. The Master upgrade will be unavailable until your default key is changed to the ordinary one.

5. After you received the new key, save the license key file on your local machine.
6. When the file is saved, get back to the License Management page in your Plesk control panel and select the Upload Key icon. This will take you to the License Installation page.
7. On this page, specify the path to the license key file location: enter the path into the input field provided, or click Browse to browse for the desired location.
8. Click OK to submit the settings, or Cancel to return to the previous page without submitting any changes.

Ordering Control Panel Add-Ons

Plesk allows you to order add-ons (additional features) for your control panel directly from your control panel. To order add-ons for your control panel, follow these steps:

1. Select the Server shortcut in the navigation pane.
2. On the Server administration page, click the License Management icon.
3. On the License Management page, click the Order Control Panel Add-Ons icon.
4. This will take you to the SWsoft online store that will open in a separate browser window. When there, please select the desired features for your license, provide the purchase details and billing address, specify the payment method, and place your order. Once you placed it, your order will be sent to the online store operator. You will be notified by e-mail when your order is processed.

5. After you received the e-mail notification on a successful processing of your order, get back to the License Management page in your Plesk control panel and select the Retrieve Keys icon to retrieve the ordered license key. Plesk will retrieve the purchased license key from the license keys management system and automatically upload it to your control panel.

Ordering Control Panel Upgrades

Plesk allows you to order upgrades for your control panel directly from your control panel. To order upgrades for your control panel, follow these steps:

1. Select the Server shortcut in the navigation pane.
2. Click the License Management icon on the Server administration page.
3. On the License Management page, click the Order Control Panel Upgrades icon.
4. This will take you to the SWsoft online store that will open in a separate browser window. When there, please select the desired features for your license, provide the purchase details and billing address, specify the payment method, and place your order. Once you placed it, your order will be sent to the online store operator. You will be notified on your e-mail when your order is processed.

Note

If you have a default license key installed on your Plesk, you will only be able to have Domains upgrade. By ordering upgrade to a certain number of domains, you buy thus the new license key with the basic Plesk functionality and the ordered number of domains included. The Master upgrade will be unavailable until your default key is changed to the ordinary one.

5. After you received the e-mail notification on a successful processing of your order, get back to the License Management page in your Plesk control panel and select the Retrieve Keys icon to retrieve the ordered license key. Plesk will retrieve the purchased license key from the license keys management system and automatically upload it to your control panel.

Uploading License Key

You can manually upload any desired license key file from your local machine to your Plesk control panel. To do that, follow these steps:

1. Select the Server shortcut in the navigation pane.

2. Click the License Management icon on the Server administration page.
3. On the License Management page, click the Upload Key icon. This will take you to the License Installation page.
4. On this page, specify the path to the license key file location: enter the path into the input field provided, or click Browse to browse for the desired location.
5. Click OK to submit the settings, or Cancel to return to the previous page without submitting any changes.

Rolling Back License Key

To roll back a license key installation, click Roll Back Key. A page will open displaying the properties of the previously used license key, the control panel will revert to. Click OK.

Expired License Key

If your license key has expired, you will be able to log in to your Plesk control panel. However, you will only be able to use License Manager while all other functionality will be unavailable. Your customers, however, will not be able to log in to Plesk at all. At the same time, all your services and services of your clients will remain activated, meaning that you and your clients will be able to use your domains, subdomains, etc.

Managing Additional License Keys

Additional keys are license keys for add-ons (additional features for your Plesk), such as site applications and Dr.Web antivirus program which are not included in the basic Plesk license key.

To access the additional license keys management functions, on the License management page, click the Additional License Keys tab.

To retrieve the ordered additional key, click the Retrieve Keys icon. Plesk will retrieve the license key and automatically upload it to your control panel.

To manually upload the desired additional license key file from your local machine to your Plesk control panel, click the Upload Key icon. You will be taken to the page where you will be asked to specify the path to the license key file location.


To download the desired additional key to your local machine, click the diskette icon of the corresponding additional key. The File Download dialog window will

open. Click Save, specify the file location and then click Save again. The file will be saved on your local machine.

To remove one or several additional keys from Plesk, select the corresponding checkboxes and click Remove Selected.

Rebooting the System

Rebooting simply means restarting the server. If users are logged on to the system, you should not reboot the server until you have informed all the users that the server must be shut down temporarily; however, sometimes an emergency necessitates immediate rebooting of a server to correct a problem that cannot be fixed any other way. To reboot your system, follow these steps:


1. Click the  Reboot icon on the Server administration page.
2. Plesk warns you that the system will be restarted and asks you to confirm your choice, for safety purposes. Click OK to reboot, or Cancel to keep the server up.

IMPORTANT

Rebooting the server via the Plesk interface also reboots the operating system and anything else running on the server.

Shutting Down the System

When you need to completely shut down the server, you should do it through the Plesk software rather than simply turning off the hardware. Shutting down with Plesk closes all open files and gracefully ends all current services. To shut down your system, follow these steps:

1. Click the  Shut Down icon on the Server administration page.
2. Plesk warns you that the system will be shut down and asks you to confirm your choice, for safety purposes. Click OK to turn the server off or Cancel to keep it running.

IMPORTANT

Shutting down the server via the Plesk interface will also shut down the operating system and anything else running on the server. After having done this, there is no way to remotely bring the server back up; it must be done manually.

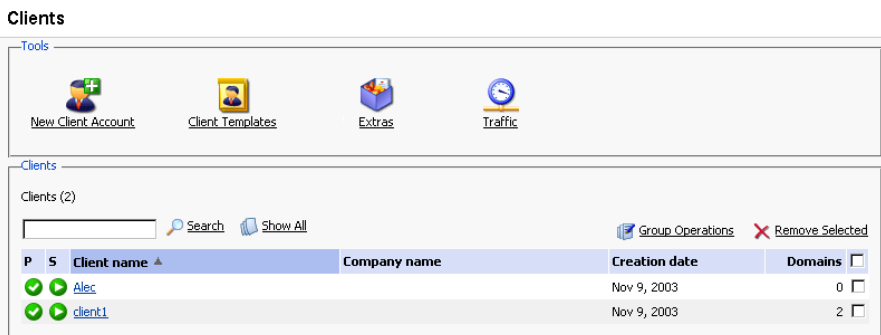
Chapter 4. Managing User Accounts

This chapter focuses on administrative tasks you perform when delivering customer services. Follow the instructions provided in this chapter to learn how to create and manage client accounts, and configure all required restrictions and limits.

Creating a New Client Account




Follow these instructions to create a new client account:


1. Select the Clients shortcut in the navigation pane to access the client management functions. The Clients management page opens displaying the list of registered client accounts:




The client's status is represented by two icons:


Table 4.1. The client state/status icons.

Icon	Meaning
The state icon indicates the system state of the client:	
	means that the client's account is operating within defined disk space and traffic parameters
	means that the client has exceeded allocated disk space or traffic limitations in at least one of the client's domains. The Plesk system evaluates disk space and traffic every 24 hours
The status icon indicates if the system administrator has activated this client account:	
	means that the client account is activated

Icon	Meaning
The state icon indicates the system state of the client:	
	means that this client account is presently deactivated. When the client account is deactivated, all of the client's domains are deactivated and inaccessible.

2. Click  New Client Account. The Client form appears prompting you

to enter all the information required:

[Clients >](#)  [Up Level](#)

Enter the information on new client

Client form

Company name	<input type="text"/>
Contact name *	<input type="text"/>
Login *	<input type="text"/>
Password *	<input type="password"/>
Confirm Password *	<input type="password"/>
Phone	<input type="text"/>
Fax	<input type="text"/>
E-mail	<input type="text"/>
Address	<input type="text"/>
City	<input type="text"/>
State/Province	<input type="text"/>
Postal/ZIP code	<input type="text"/>
Country	<input type="text" value="United States"/>
Interface language	<input type="text" value="English"/>
Select template	<input type="text" value="Create client without template"/>

Proceed to client's IP pool configuring

* Required fields

3. Enter the necessary data. Click in a specific text box to enter data, or use the Tab key to move from one text box to the next. The following data fields are required:

- Contact name. The contact name must be unique in order to work with it in the Plesk system.
- Login - By assigning a control panel login name to a client, you grant that user access to Plesk for independent account administration. Each client's login name must be unique in the system.

 NOTE

Use only alphanumeric symbols in the login name.

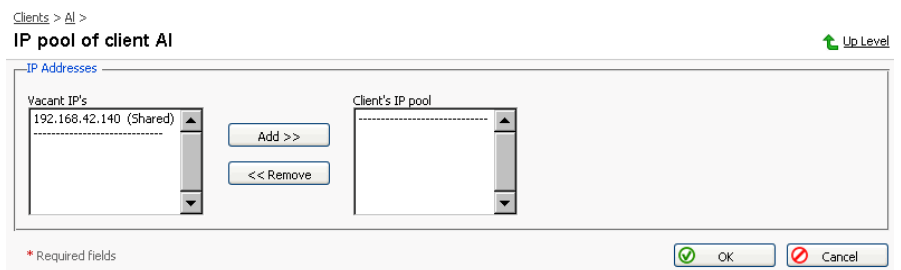
- Password - You must assign a password to each client for security purposes. When entering the password, the symbols will be replaced by the asterisks so that nobody can accidentally see your password on the

screen.

i NOTE

Do not use quotes, space and national alphabet characters in the password. The password should be between 5 and 14 characters long and must not be the same as the login name.

- Confirm password. In order to make sure that you have entered the password you wanted, re-enter it in this field.
4. Review the entered information. Edit data in any text box by clicking and editing the specific word or phrase.
 5. Select a template from the drop-down box to create the client account by the template. This option may be unavailable if not supported by your license key.
 6. To proceed directly to configuring the IP pool for the new client account, leave the Proceed to client's IP pool configuring checkbox selected.
 7. When you are satisfied that the information is complete and correct, click OK. The client's IP pool opens:



8. Select a desired IP address in the list of Vacant IPs, and click Add>> to add it to the pool.
9. Click OK. Now the client account is created, and the client is provided with the IP addresses necessary for creating domains. The Client Home page appears, providing you with client account management functions:

The screenshot displays a web management interface with three main sections:

- Tools:** A grid of icons for various functions: Disable, Edit, Report, Preferences, Permissions, Limits, IP Pool, Application Pool, Skeleton, Logo Setup, and Custom Buttons.
- Info:** A summary box showing "1 domains, 1 active domains, 284 KB disk space used, 0 B traffic used".
- Domains:** A table listing domains with columns for P, S, H, Domain name, Creation date, Subdomains, Disk usage, and Traffic. A search bar and "Show All" button are present above the table.

P	S	H	Domain name	Creation date	Subdomains	Disk usage	Traffic
			domain.com	Oct 4, 2003	0	0.28 MB	0.00 MB/Month

You can now proceed to configuring the necessary permissions for the client account.

Note that if you skipped the IP allocation procedure during account creation, you can do this later using the Client's IP pool function, which is described in the following section. You should keep in mind that the client will not be able to create domains unless he or she is granted an IP address.

Managing IP Pool

The IP pool is the location within which the client's IP addresses are managed. Clients are given IPs and then are able to utilize them within their own domains. IPs are able to be granted as either *exclusive*, meaning that the target client becomes the user with exclusive rights to this IP, or *shared*, meaning that this IP is shared among many clients (i.e. one IP can be used for hosting by many clients).

The IP Pool also provides the mechanism by which IP usage can be tracked. The client immediately sees his/her complete list of allocated IPs and can identify the locations on which each IP is currently being used within their environment.

Click the  IP Pool icon on the Client Home page to access the Client IP

pool. It displays the list of IP addresses that were granted (exclusively or as shared) to this client:

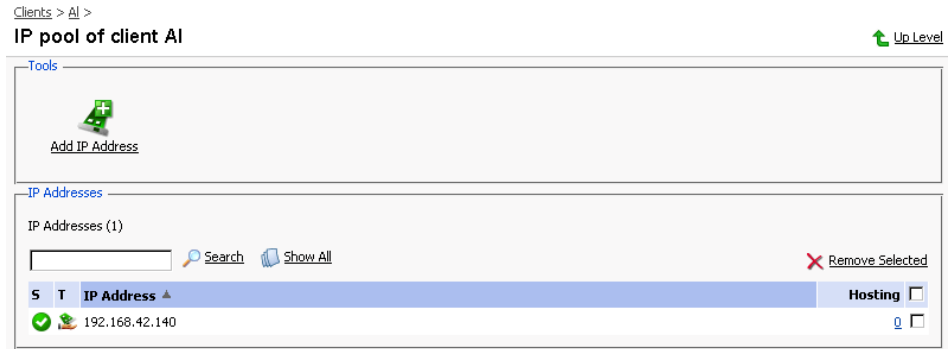


Table 4.2. The IP state/type icons.

Icon	Meaning
The state icon indicates the system state of the IP address:	
	means that the IP address functions properly
	means that the IP address is malfunctioning. Plesk experiences problems when trying to work with this IP address.
The type icon indicates how the IP address was granted:	
	means that the IP address was granted exclusively
	means that the IP address was granted as shared

The Hosting column displays the number of client's domains that use (have hosting configured) the corresponding IP address.

Adding IP address to the client's IP pool

The admin grants available IP addresses to a particular client so that they can be used for setting up hosting at client's domains.

1. At the Client IP pool page, click Add IP Address icon. IP selection

dialog will open:

Clients > All > IP_addresses >

Select ip addresses Up Level

IP Addresses

Vacant IP's

192.168.42.240 (Exclusive)

* Required fields

OK Cancel

2. Select an IP address from the List of vacant IP's.

i NOTE

You can select several IP addresses at a time.

3. Click OK to add the selected IP address(-es) to the client's IP pool.

Viewing the hosting configured for an IP and setting a default domain

You can view the domains that have hosting set up using a particular IP address. Here you can also set a *default domain* for the exclusive IP address - the domain that will be addressed if a user specifies this IP address in the browser or a domain that cannot be resolved.

1. At the Client IP pool page, select the IP address you wish to inspect and click on the number of domains displayed in the Hosting column. The page that contains the list of domains using the specified IP address will appear:

Clients > client1 > IP_addresses >


The domains of client client1 that use exclusive ip address 10.1.150.1 Up Level

Domains

Domains (2)

Search Show All Set as Default

Domain name	
kiber.vrh62.plesk.ru	<input type="radio"/>
strange2.vrh62.plesk.ru	<input checked="" type="radio"/>

2. To jump to a Domain administration page, simply click on the name of the domain.
3. To set a domain as default for the exclusive IP address, select the domain using the corresponding radio button and click  Set as Default. The default domain name will be displayed in bold.
4. Click Up Level to return to the Client IP pool page.

Assigning an SSL certificate for an exclusively granted IP address

The administrator can assign SSL certificates to the exclusively granted IP addresses in the client's IP pool.

IMPORTANT

The admin can only choose the new SSL certificate from those that are available in the certificate repositories of the domains that belong to the corresponding client.

1. At the Client IP pool page, select the exclusively granted IP address you wish to assign a new SSL certificate to and click on it.
2. Select the new certificate in the SSL Certificate drop-down box.
3. Click OK.

Removing an IP address from the client's IP pool

You can remove one or several IPs at the same time.

IMPORTANT


IP addresses that are in use for hosting cannot be removed from the IP pool.

To remove an IP address(-es):

1. Check the corresponding checkboxes of the IPs list.
2. Click Remove Selected. Select the checkbox to confirm and click OK.

Setting the Permissions for Operations

You can decide what operations the client can perform and what operations he/she should not be able to perform. To edit the client's permissions for operations:

1. Click the  Permissions icon on the Client Home page. The Client permissions page will appear displaying the list of permissions for all available operations:

Clients > AI >

Client AI's permissions Up Level

Permissions

Domain creation	<input type="checkbox"/>
Physical hosting management	<input type="checkbox"/>
Hard disk quota assignment	<input type="checkbox"/>
Subdomains management	<input type="checkbox"/>
Domain limits adjustment	<input type="checkbox"/>
DNS zone management	<input type="checkbox"/>
Log rotation management	<input type="checkbox"/>
Crontab management	<input type="checkbox"/>
Anonymous FTP management	<input type="checkbox"/>
Web applications management	<input type="checkbox"/>
System access management	<input type="checkbox"/>
Mailing lists management	<input type="checkbox"/>
Backup/restore functions	<input type="checkbox"/>

* Required fields

- In order to allow (forbid) the client to perform a specific operation, check (uncheck) the corresponding checkbox.

IMPORTANT

Allow performing operations of managing crontab and system access only to trusted clients as these operations must be performed with great care and can have most serious effects on the system.


- When you are done editing, click OK.

NOTE

When you revoke certain permissions granted to the client, these permissions are also revoked from his/her customers.

Setting the Resource Usage Limits

While performing various tasks in Plesk clients use resources. For each client you can limit each specific resource usage. To edit the client's resource limits:

- Click the  Limits icon on the Client Home page. The Client limits

page will appear containing the list of resource limit types:

Clients > AI >
Client AI's limits Up Level

Limits

Maximum number of domains	<input type="text" value="100"/>	<input type="checkbox"/> Unlimited
Maximum number of subdomains	<input type="text" value="100"/>	<input type="checkbox"/> Unlimited
Disk space	<input type="text" value="1024"/> MB	<input type="checkbox"/> Unlimited
Maximum amount of traffic	<input type="text" value="500"/> MB/month	<input type="checkbox"/> Unlimited
Maximum number of web users	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Maximum number of databases	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Maximum number of mailboxes	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Mailbox quota	<input type="text"/> KB	<input checked="" type="checkbox"/> Unlimited
Maximum number of mail redirects	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Maximum number of mail groups	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Maximum number of mail autoresponders	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Maximum number of mailing lists	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Maximum number of web applications	<input type="text"/>	<input checked="" type="checkbox"/> Unlimited
Validity period	<input type="text" value="10"/> <input type="text" value="Dec"/> <input type="text" value="2005"/>	<input type="checkbox"/> Unlimited

* Required fields OK Cancel

- To set a limit value for a specific resource, uncheck the corresponding "Unlimited" checkbox and enter the value into the corresponding input field.

i NOTE


The total limit on resources for the client must be more or equal to the total sum of the domain limits defined for the client.

- At this page you can also set the period of validity for the given client account. To this effect, deselect the corresponding "Unlimited" checkbox, and define the desired date of account expiration in the Validity period input fields.
- When you are done editing, click OK.

Setting the Interface Preferences

You can choose to set such properties of the Plesk user interface as the interface language, skin, set a number of entries shown per page when displaying various lists (e.g. the list of Domains), set the limit on button label length, and allow multiple sessions under the same client's login.

To change the interface preferences, follow these steps:

- Click the  Preferences icon at the Client home page. The client preferences page will open.
- To define the number of list entries that will be shown per page, click into

the Display ... lines per page input box and type in the desired number.

3. To limit the size of interface buttons, type the desired value into the Button label length box.
4. If you have several language packs installed for Plesk, you can select the client's interface language. Select the desired language from the Interface language drop-down box.
5. To set a skin to be used for client's sessions, select one from the Interface skin drop-down box.
6. To allow multiple simultaneous sessions under client's login name, select the Allow multiple sessions checkbox.
7. When you are done editing, click OK.

Managing Client Application Pool

Each client in Plesk has an application pool - the location where all site application packages provided to this client are stored. This feature was designed specially for administrators and is available only to them. Clients do not have application pools in their control panel environments. With this feature administrator can now manage site applications provided to the client and add new application packages to the client.

NOTE

Application pools of all clients will be disabled if the Application Vault is disabled in your Plesk. The Application Vault may be disabled if not supported by your license key. You should order a new license key if you wish to use this feature.

There are two types of site applications in Plesk:



- free, requiring no license key;
- commercial, requiring a license key;

Plesk goes with a number of free site applications requiring no license key that you can choose to install on your Plesk. All free site applications installed on your Plesk are automatically added to the application pool of each client created in Plesk. However, the commercial applications can be added to the client only upon purchase.



To access the application pool of a client, on a Client Home page click the Application Pool icon.

All site applications provided to the client are presented in the list. Each site application is accompanied by two types of icons.

The icon in the first left column indicates the type of the site application:

-  - the free site application requiring no license key, included in the default installation of Plesk for free. It is automatically added to the application pool of each client created in your Plesk control panel.
-  - the commercial site application that requires a license key. This application is purchased from SWsoft, Inc. additionally.

The icon in the second left column indicates the site application usage rules defined by the administrator:

-  - free of charge, automatically added to the application pools of all clients;
-  - commercial, customers have to buy this application to be able to use it.

NOTE


You may set rules for each site application and choose whether to make it free of charge or commercial. Site application usage rules can be set in the Application Vault.

To add a new application package to the client application pool, follow these steps:

1. Click the Add New Application Package icon on the Client Application Pool page. The Add New Application Package will open. All available commercial applications, not included in the client application pool will be shown in the list.
2. Select the desired application and click OK. The selected site application will be added to the client application pool.

Note: If there are no commercial applications available, the Add New Application Package icon will be disabled.

To view information on a site application package and the resources required for the application to run, select its title in the list.

To view help on a certain site application, click the icon . The Help page containing the general information on this site application will open in a separate browser window.


To remove one or several site applications from the client application pool, select the corresponding checkboxes and click Remove Selected.

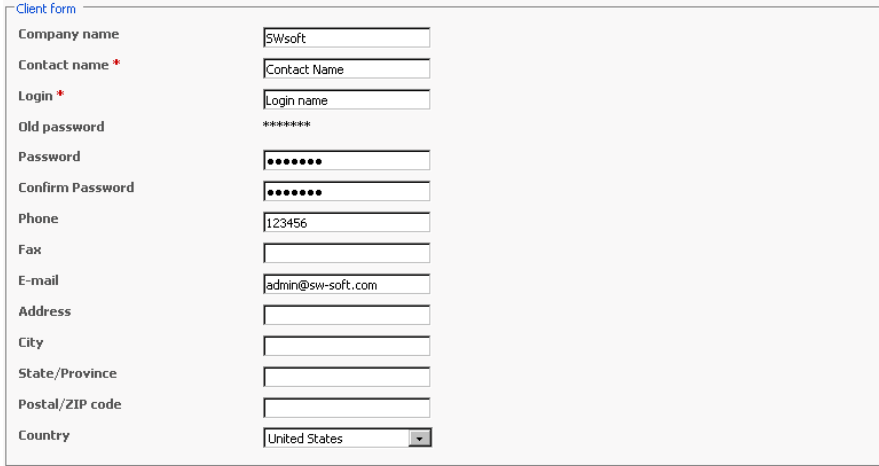
NOTE

You can remove only commercial applications. Free applications cannot be removed from the client application pool, so the corresponding checkboxes will be disabled. Free site applications can be removed only in the Application Vault.

Editing Client Information

Occasionally, you may need to change the information in a client's record. To do it, follow these steps:

1. Click the  Edit icon on the Client Home page. The Client information page will appear:



The screenshot shows a 'Client form' with the following fields:

Company name	SWsoft
Contact name *	Contact Name
Login *	Login name
Old password	*****
Password	*****
Confirm Password	*****
Phone	123456
Fax	
E-mail	admin@sw-soft.com
Address	
City	
State/Province	
Postal/ZIP code	
Country	United States

* Required fields

OK Cancel

2. To modify an item in the client's data, click in a specific text box to enter data, or use the Tab key to move from one text box to the next. The following data fields are required:
 - Contact Name - This is the name that appears in the Clients list. The contact name must be unique in order to work with it in the Plesk system.
 - Login - By assigning a login name to a client, you grant that user access to Plesk for independent account administration. Each client's Plesk Control Panel login name must be unique in the system.

i NOTE

Use only alphanumeric symbols in the login name.

- Password - You must assign a password to each client for security purposes. When entering the password, the symbols will be replaced by the asterisks so that nobody can accidentally see your password on the screen.

i NOTE

Do not use quotes, space and national alphabet characters in the password. The password should be between 5 and 14 characters long and must not be the same as the login name.

- Confirm password. In order to make sure that you have entered the password you wanted, re-enter it in this field.
3. Review the entered information. Edit data in any text box by clicking and editing the specific word or phrase.
 4. When you are satisfied that the information is complete and correct, click OK.

! IMPORTANT


Changes to client's email address will not be reflected in Start of Authority (SOA) records of client's DNS zones until you rebuild them by switching zone off and back on, or by modifying the zone.

Viewing the Client Report and Statistics

Plesk keeps a summary of important data for every client in the system. The client report is a brief overview of the client-related system information.


To view the report, click the  Report icon on a Client Home Page.

To get a printer-friendly version of report, use the  icon.


To send the report by e-mail, enter the email address into the input field and click the  icon.

Viewing traffic history


Traffic history is a record of amounts of traffic registered for the selected client's domains over a period of time.

1. Click the  Traffic History icon at the Client report page.
2. The client's traffic history is displayed in the form of a table. Each line entry in the table contains the following data:
 - Year - the reported year
 - Month - the reported month
 - Traffic usage - the amount of traffic registered for the client's domains over the reported month
3. To return to the Client report page, click Up Level.

Customizing a report layout

You can define which sections of the client report will be displayed. To this effect, on the client report page, click the  Customize icon. The Custom report layouts page will open displaying the list of currently existing report layouts.

To add a new custom layout, follow these steps:


1. Click the  Add New Report icon.
2. Enter the report layout name in the Report name field.
3. In the General field, define the amount of data that will be presented in the General section of the report.
4. In the Domains field, define the amount of data that will be presented in the Domains section of the report.
5. To use this layout by default, select the corresponding checkbox.
6. Click OK.

To remove a custom report layout from the Custom report layouts page, select it using the corresponding checkbox, and click Remove Selected.

To edit a custom layout, select its title in the list.

Viewing Traffic Statistics by Clients

To view the information on total amount of server traffic used by all clients, follow these steps:

1. Select the Clients shortcut in the navigation pane.
2. Click  Traffic. The page will open, providing the detailed traffic

statistics:

[Clients](#) >
Server traffic [Up Level](#)

[Traffic by client](#)

Clients (2)

[Search](#) [Show All](#) Nov 2003 (0 B)


Server Total		0.00 MB			
Client name ▲	Used	Limit	Available	Used (in %)	
Alec	0.00 MB	Unlimited	-	-	
client1	0.00 MB	Unlimited	-	-	

Presented in the table are the data on amounts of traffic used by clients.

To view the traffic statistics for a certain month, select the required month from the drop-down box.

To view the information on traffic used by domains of a certain client, click on the client's name.

Viewing Traffic Statistics by Client's Domains

To view the statistical information on traffic used by domains of a client, on the Home Page of the selected client, click  Traffic. The page will open,

providing the detailed traffic statistics:

[Alec](#) >
Traffic at the domains of client Alec [Up Level](#)

[Traffic by domain](#)

Domains (1)

[Search](#) [Show All](#) Oct 2003 (0 B)

Client Total	Used	Limit	Available	Used (in %)	
Alec	0.00 MB	Unlimited	-	-	
Domain name ▲	Used	Limit	Available	Used (in %)	
domain.com	0.00 MB	Unlimited	-	-	

Presented in the table are the data on amount of traffic used by the client, and his/her domains.

To view the traffic statistics for a certain month, select the required month from the drop-down box.


To view the traffic statistics at the domain and the data on traffic used by

domain services, click on a domain name.

Deactivating/Activating a Client Account

To restrict client's access to system and suspend operation of client's domains, you can deactivate the client's account.


To deactivate a client's account:

1. On the Client Home page of the selected client, click  Disable. The

confirmation will appear querying whether you actually wish to change the status of the selected client's account.

2. Click OK.

To activate an account, follow these steps:

1. On the Client Home page of the selected client, whose account is deactivated, click  Enable. The confirmation will appear querying

whether you actually wish to change the status of the selected client's account.

2. Click OK.

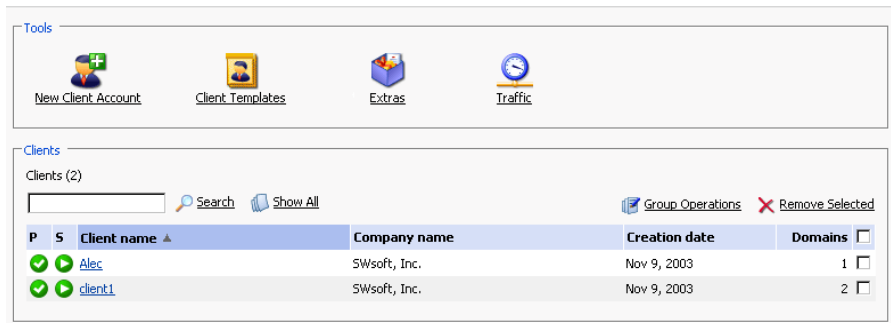
Performing Group Operations on Accounts


In cases when you need to introduce certain similar changes to several client accounts, you can use the Group Operations function, made available to simplify administration of multiple accounts. Using this feature you can, for instance, select a number of clients, enable all of them to create domains and limit the maximum number of domains to a specific number - all that within a single operation, without having to select each client independently and edit his/her settings.

To perform group operations on client accounts, follow these steps:

1. Select the Clients shortcut in the navigation pane. The page will open displaying the list of registered client accounts:

Clients



2. Select the clients, whose accounts you wish to modify by checking the corresponding checkboxes.
3. Click the  Group Operations icon. The Group Operations page will appear, divided into three groups:
 - The Permissions group is used for setting permissions for various operations
 - The Limits group is used for modifying limits for granted resources
 - The Modified accounts area lists the client accounts selected for modification.
4. To set permissions, select the **Do not change**, **Enable** or **Disable** radio button for the corresponding type of operation.
5. To edit limit settings for a particular resource type:
 - 5.1. First, select the desired action from the drop-down box:
 - Leave the **Do not change** option selected, if you do not wish to make a change
 - Select **Unlimited** if you wish not to limit the resource usage
 - Select the **value** option in order to specify a new value for the resource limit
 - Select **Increase (+)**, to specify the value by which to increment the presently set resource limit value
 - Select **Decrease (-)**, to specify the value by which to decrement the presently set resource limit value
 - 5.2. Then, specify the value of the new resource limit in the corresponding input field.
 - 5.3. If you chose to increase/decrease the presently set limit value, use the drop-down box to select **units** if you wish to modify the limit value by a quantity of commonly used units or % if you wish to modify the limit value by a particular percentage.
6. Click OK to apply the new settings to the selected client accounts.

Removing Client Accounts

You can remove one or several client accounts at the same time. To remove client accounts:

1. Select the Clients shortcut in the navigation pane. The page will open displaying the list of registered client accounts:

Clients

Tools

[New Client Account](#) [Client Templates](#) [Extras](#) [Traffic](#)

Clients

Clients (2)

[Search](#) [Show All](#) [Group Operations](#) [Remove Selected](#)

P	5	Client name ▲	Company name	Creation date	Domains
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alec	SWsoft, Inc.	Nov 9, 2003	1 <input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	client1	SWsoft, Inc.	Nov 9, 2003	2 <input type="checkbox"/>

2. Select the clients, whose accounts you wish to remove by checking the corresponding checkboxes.
3. Click Remove Selected. The Removal confirmation page appears:

Removal confirmation [Up Level](#)

Remove

The following client accounts and their domains will be removed:

- Alec
 - domain.com

Confirm removal.

* Required fields

4. Select the "Confirm removal" checkbox to confirm removing, and click OK. If you decide to not delete these client accounts or wish to modify the list of accounts selected for deletion, click the Cancel button.

Chapter 5. Administering Domains

This chapter focuses on administrative tasks you perform when administering domains for your customers. Follow the instructions provided in this chapter to learn how to create new domain names, configure all required restrictions and limits, set up hosting, mail, and other services.

Creating a Domain

A domain is a virtual address on the Internet for any organization or entity. Technically, a domain is defined as a group of networked computers (servers) that represent an organization and provide network services; however, several domains could reside on one server, in dedicated space provided by a Web hosting service. To the Internet user, a domain appears as space on one server, regardless of its implementation.

Domains are identified by their familiar Internet URL (uniform resource locator) addresses. Syntactically, a domain name is a string of names or words separated by periods. For example, `www.sw-soft.com` is the name of the domain where SWsoft's information resides on its servers. A domain must belong to one client. For example, John Doe may be a programmer whose domain is `aceprogrammer.com`; the ABCDE, Inc. company may own a domain by the name of `abcde.com`. All domains are assigned to clients.

NOTE

You must officially register a domain and Internet address before you create it in Plesk. You can do this using the Register option available within Plesk or through any of the Internet registration services.

To create a new domain, follow these steps:

1. Select the Domains shortcut in the navigation pane. The list of domains will open:

Domains

Tools

[Add New Domain](#) [Domain Templates](#) [Summary Report](#) [Traffic](#)

Domains










Domains (3)


[Search](#) [Show All](#) [Show Subdomains](#) [Group Operations](#) [Remove Selected](#)

P	S	H	Domain name ▲	Creation date	Subdomains	Disk usage	Traffic	
✓	✓	✓	domain.com	Oct 4, 2003	0	0.28 MB 0.00 MB/Month		<input type="checkbox"/>
✓	✓	✓	myadmin.vrh9c.plesk.ru	Oct 4, 2003	0	0.17 MB 0.00 MB/Month		<input type="checkbox"/>
✓	✓	✓	test.vrh9c.plesk.ru	Oct 4, 2003	0	0.16 MB 0.00 MB/Month		<input type="checkbox"/>


Each domain name is accompanied by the following icons:

Table 5.1.

Icon	Meaning
The state icon indicates the system state of the domain:	
	means that the domain is operating within defined disk space and traffic parameters
	means that the client has exceeded allocated disk space or traffic limitations at this particular domain. The Plesk system evaluates disk space and traffic every 24 hours
The status icon indicates if the client or system administrator has activated/deactivated this domain:	
	means that the domain is activated
	means that this domain is presently deactivated and inaccessible
The hosting type icon indicates the type of hosting set-up for the domain:	
	indicates Physical Hosting
	indicates Standard Forwarding
	indicates Frame Forwarding
	indicates that no hosting was configured for the domain
Additional:	
	used for accessing the domain URL in browser



2. Click  Add New Domain. The client selection page will open:







Domains >



Select the client to create the domain for  Up Level

Clients

Clients (2)

 Search  Show All

P	S	Client name ▲	Company name	Creation date	Domains
		Alec	SWsoft, Inc.	Nov 9, 2003	0 
		client1	SWsoft, Inc.	Nov 9, 2003	2 

 OK  Cancel

- Using a radio button, select the client, you wish to create the domain for, and click OK. The domain creation page will open:

Domains >

Create new domain for Alec Up Level

Domain form

Domain name * WWW

Select template

Select an IP address

Proceed to hosting setup

Client card

Personal name	Alec
Company name	SWsoft, Inc.
Phone	111111
Fax	
E-mail	
Address	Nsk
City	Nsk
State/Province	Nsk
Postal/ZIP code	1111111
Country	Vanuatu

* Required fields

i NOTE

You can also access the domain creation page directly from the Home page of a certain client.

- In the Domain name field - enter a valid domain name (e.g. mycompany.com) that is unique to the system. If you enter a domain name that already exists, Plesk will ask you to change it. The Domain Name field also has a prompt for the WWW tag. The WWW checkbox, when checked, indicates that the WWW prefix can be used when addressing the domain as well as the domain name by itself. If the box is unchecked, then the domain can only be referenced by its name without the WWW prefix.
- Select a template to be applied from the drop-down list, if you wish this domain to be created by a template.
- Select the IP address to be used for hosting from the drop-down list.
- Check (or leave checked) the Proceed to hosting setup checkbox if you wish to set up hosting for the domain after it is created.

i NOTE

If you are creating a domain by a template that allows physical hosting creation, you will proceed to the Physical Hosting Setup page for this domain. Otherwise, you will be taken to the Hosting Type Selection page.

8. When you are satisfied that the information is complete and correct, click OK.

IMPORTANT

- If you have chosen to set up hosting for the domain after it is created (leaving the Proceed to hosting setup checkbox selected), you will be taken to the hosting setup wizard. Please, refer to the following section of this manual to learn how to set up hosting for the domain.
- If you decided to set up hosting later and deselected the Proceed to hosting setup checkbox, you will be taken to the Domain Administration page, which provides you with domain management functions.

Managing Hosting

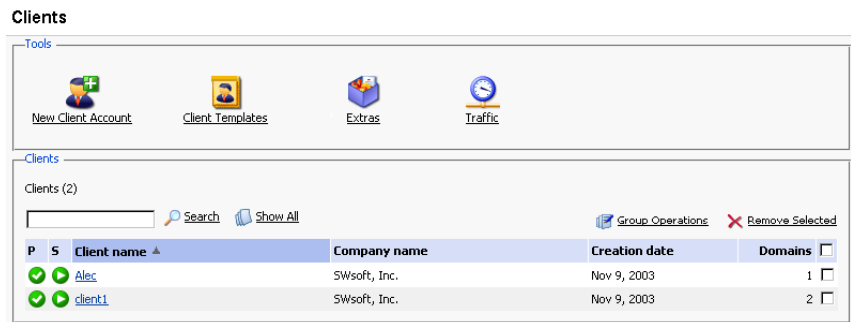
Using Plesk you can select any of three different types of hosting services, as listed below:

- **Physical hosting:** the most common type of hosting service, creating a virtual host (disk space on the local server) for the client. The client controls and publishes his own web site without having to purchase a server and dedicated communication lines.
- **Standard forwarding:** with this type of forwarding, all requests to the domain are forwarded by your server to another Internet address (no virtual server is created). When an end user searches the Internet for the client's domain, he is routed to another URL, and the address in his browser window changes to the new URL.
- **Frame forwarding:** all requests to this domain are forwarded to another Internet address (no virtual server is created). But with this type of forwarding, the end user sees the client's domain name in his browser, not the forwarding address. Plesk uses frames to 'trick' the browser into displaying the correct domain name. The problem with this type of forwarding is that some search engines do not index these frame pages and some browsers do not support frames.

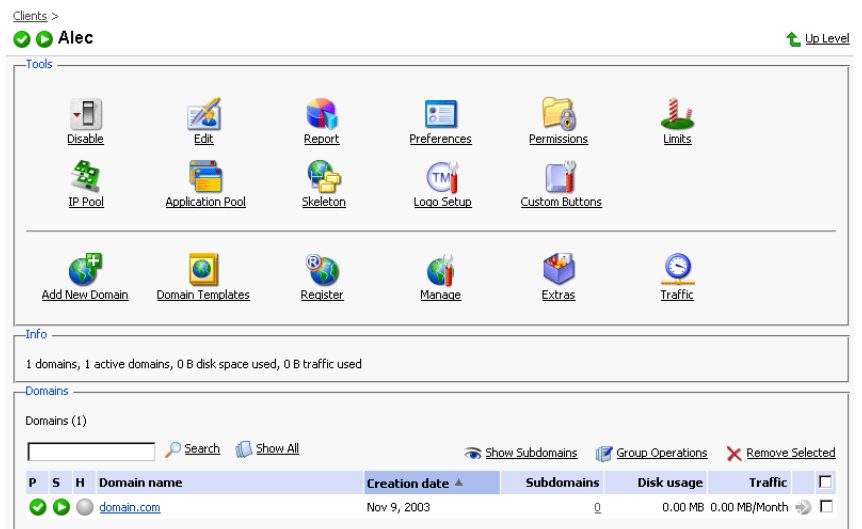
Accessing the Hosting Setup Wizard


To access the hosting setup wizard for the domain, which is created but does not have hosting configured yet, use any of the following ways:

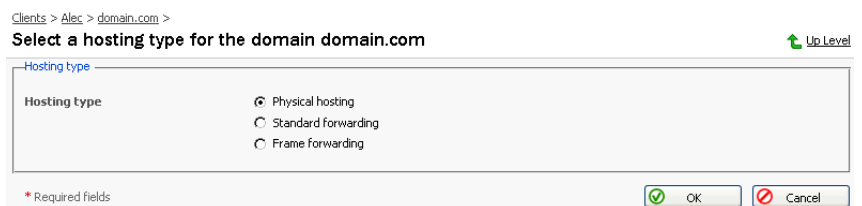
1. Select the Clients shortcut in the navigation pane. The Clients list page opens:



2. Click on a client's name. The Client Home page opens:







3. Click on the  icon to the left of the domain name. The hosting type selection page opens:



1. Select the Domains shortcut in the navigation pane. The Domains list page will open:

Domains


Tools

 [Add New Domain](#)  [Domain Templates](#)  [Summary Report](#)  [Traffic](#)

Domains (3)

[Search](#) [Show All](#) [Show Subdomains](#) [Group Operations](#) [Remove Selected](#)

P	S	H	Domain name	Creation date	Subdomains	Disk usage	Traffic	
			chappa2.vrh62.plesk.ru	Nov 9, 2003	1	13.9 MB 0.65 MB/Month		<input type="checkbox"/>
			domain.com	Nov 9, 2003	0	0.00 MB 0.00 MB/Month		<input type="checkbox"/>
			quick.vrh62.plesk.ru	Nov 9, 2003	0	4.23 MB 0.49 MB/Month		<input type="checkbox"/>

- Click on the  icon to the left of the domain name. The hosting type selection page opens:

Clients > Alec > domain.com >


Select a hosting type for the domain domain.com [Up Level](#)

Hosting type

Hosting type

Physical hosting
 Standard forwarding
 Frame forwarding

* Required fields

- When on the Domain Administration page click the  Setup icon. The

Hosting Type Selection page appears:

Clients > Alec > domain.com >

Select a hosting type for the domain domain.com [Up Level](#)

Hosting type

Hosting type

Physical hosting
 Standard forwarding
 Frame forwarding

* Required fields

Configuring Physical Hosting

To set up physical hosting, follow these steps:

- On the Hosting Type Selection page, select the **Physical hosting** radio button. Click OK. The Physical hosting setup page appears.
- Select the SSL support checkbox. SSL certificates provide additional security for Web sessions. SSL certificates are often used for e-commerce and other private or confidential applications. Enabling SSL creates an httpsdocs directory in the FTP account, and provides https protocol; as a result, users access the domain with the command `https://newdomain.com`. If you want to grant permission to your client to implement an SSL certificate, make sure a check mark appears in the SSL support box.

3. You must set an FTP login name and password. FTP allows end users to upload and download files from the Internet site to remote PC's. If you want to provide FTP services, click in the FTP Login box. Then, enter or edit a login name to be used for accessing FTP file transfer services on the domain.

 NOTE

The maximum FTP user name length should not exceed 16 symbols, which is required for compatibility purposes. As the FreeBSD operating system does not support user names longer than 16 symbols, the clients who are running RedHat Linux and having users registered in the system with names longer than 16 symbols (as allowed by RedHat Linux OS) and willing to migrate to FreeBSD would encounter certain problems during restoring of data backed up on RedHat Linux.

You cannot use the reserved system words, such as "mailman" for user names.

4. Click in the FTP Password text box and enter or edit the password.
5. Tab to the Confirm Password text box and re-enter the password for confirmation.

 NOTE

You should specify the FTP password, otherwise the FTP user will not be able to login to the FTP account that will be created.

6. Hard disk quota field allows you to set the limit for the maximum disk space amount available for use by this domain.
7. In the Access to system drop-down list, select the system access availability.

i NOTE

"Forbidden" option - prohibits access, which is more preferable as it helps to alleviate security concerns. Note that allowing system access is highly dangerous for the system security. Allow access to the system only if you clearly understand what you are doing, and only to trusted users.

You can choose to allow customers to log in to a chrooted environment, in order to prevent users from accessing the information they are not allowed to possess, such as the list of domains hosted on server, or the information on installed software. However, the use of chrooted environment will not protect your data in case of kernel exploits, which can be used for gaining root privileges or organizing a DoS attack. Even in a chrooted environment a user with root privileges can cause a server failure, or gain access to confidential data.

8. To allow the use of Microsoft FrontPage Server Extensions, check the checkbox for Microsoft FrontPage support and Microsoft FrontPage over SSL support. Authorization will be disabled by default. For security reasons, authorization should only be enabled when Microsoft FrontPage extensions are in use. Microsoft FrontPage is Microsoft's Web publishing tool. It is one of the most commonly used tools for creating a client's web site. Microsoft FrontPage includes several extensions that provide special functionality. If you want this domain to support these extensions, be sure that a check mark appears in the FrontPage support box.
9. Tab to the Authoring enabled option. You can authorize or disable remote editing of the web site using Microsoft FrontPage. This setting is changeable by the Admin, Client, and Domain User logins to the control panel. For security purposes the main server administrator should notify their Clients and Domain Users that Microsoft FrontPage authoring should be disabled whenever not in use. To activate Microsoft FrontPage authoring, make sure this option is selected. If you want to turn off Microsoft FrontPage authoring, select the Authoring disabled option.
10. If FrontPage authoring is selected, then the FrontPage Admin Login, FrontPage Admin Password, and Confirm Password fields must be filled out. This login and password will be used to login to the domain when Microsoft FrontPage is being used. Click in each box and enter the desired Login and Password.
11. Tab to the Apache ASP support checkbox. It enables the development of dynamic web applications with embedded code.
12. Tab to the SSI support check box. SSI stands for 'server-side includes', a type of HTML comment that directs the web server to dynamically generate

data for the Web page whenever information is requested. SSI can also be used to execute programs and insert the results; therefore they represent a powerful tool for web developers. If your client wants to support SSI, make sure a check mark appears in the SSI box.

13. Tab to the PHP support check box. PHP is a server-based HTML embedded scripting language used to create dynamic Web pages. If your client wants to support PHP scripting in HTML documents, make sure a check mark appears in the PHP box.
14. Tab to the CGI support check box. CGI is a set of rules describing how a web server communicates with another piece of software on the same machine, and how the other piece of software (based on the CGI program) communicates back to the web server. If your client wants to support CGI, make sure a check mark appears in the CGI box.
15. Tab to the mod_perl support check box. Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use it for a vast number of automation tasks. Many CGI programs are written in Perl. If your client wants to support Perl, make sure a check mark appears in the Perl support checkbox.
16. Tab to the mod_python support checkbox. Python is an interpreted, interactive, object-oriented, high-level programming language. Python is good for many system administration type tasks and for CGI programming and is also extensively used as a graphical user interface development aide. If your client wants to support Python, make sure a check mark appears in the Python support checkbox.
17. Tab to the ColdFusion support checkbox. This enables the ColdFusion scripting.
18. Tab to the Web statistic check box. Activation of web statistics will result in the installation of a graphical statistics package for the domain.

 NOTE

When enabling web statistics, it is recommended that you also select the checkbox for creating a password protected directory plesk-stat to restrict access to statistics. You will be able to access the statistics via URLs like `https://domain.tld/plesk-stat/` using your FTP login and password. The password for accessing the directory may be changed in the password protected directory properties. For web statistics, you will need to access `https://domain.tld/plesk-stat/webstat`, for secure web server statistics - `https://domain.tld/plesk-stat/webstat-ssl`, for FTP statistics - `https://domain.tld/plesk-stat/ftpstat`, and for Anonymous FTP - `https://domain.tld/plesk-stat/anon_ftpstat`.

19. Tab to the Custom Error Documents checkbox. Selecting this option will place the domain's error documents into a location that is accessible via FTP allowing users to customize their own web server error documents.
20. When you are satisfied that you have fully defined the hosting services for this domain, click OK.

Configuring Forwarding Hosting

Configuring Standard Forwarding

To set up standard forwarding, follow these steps:

1. On the Hosting Type Selection page, select the **Standard Forwarding** radio button. Click OK. The standard forwarding assignment page appears.
2. Click in the Destination URL text box and enter or edit a URL address. Users will be redirected to this address when they access your client's domain on the web. The URL change will be visible in the browser.
3. Click OK to save your changes and return to the Domain administration page. Clicking Up Level will discard all changes you made and return you to the Domain Administration page.

Configuring Frame Forwarding

Follow these steps to configure frame forwarding:

1. On the Hosting Type Selection page, select the **Frame Forwarding** radio button. Click OK. The frame forwarding assignment page appears.
2. Click in the Destination URL text box and enter or edit a URL address. Users will be redirected to this address when they access your client's domain on the web. The URL change will not be visible in the browser.
3. Click OK.

Deleting Hosting Configuration


You can change hosting type for a domain only after you delete the hosting configuration. To delete the current hosting configuration, use the



Delete icon, located at the Domain administration page, Hosting group.

Setting Domain Level Limits

For each domain you can limit the domain-specific resource usage and the domain validity period. To edit the domain limits:

1. Click the  Limits icon on the Domain administration page. The

Domain limits page will appear containing the list of resource limits. At this page you can set the limits on the following resources:

- Number of subdomains
 - Amount of disk space
 - Amount of traffic
 - Number of web users
 - Number of databases
 - Number of mailboxes
 - The mailbox quota
 - Number of mail redirects
 - Number of mail groups
 - Number of mail autoresponders
 - Number of mailing lists
 - Number of web applications
 - The domain validity period.
2. To set a limit value for a specific resource, uncheck the Unlimited checkbox, and enter the value into the corresponding input field.
 3. To set the validity period for the domain, define the required domain expiration date in the Validity period field.
 4. When you are done with editing, click OK.

Editing Domain Preferences

To change the domain name, requirement for www prefix, and adjust the traffic statistics retention setting, follow these steps:

- 1.



Preferences icon at the Domain administration page. The Domain

preferences page will open.

2. Check or uncheck the WWW prefix checkbox to determine whether the given domain will allow the www prefix to be used to access the domain. If the box is checked, Internet users will be able to access a domain (i.e. domain.com) by specifying either the domain name itself or the domain with the "www" prefix. If the box is unchecked it will not be accessible with the "www" prefix (i.e. www.domain.com).
3. To change the domain name, click in the Domain name field, displaying the given domain name and edit it as desired.

IMPORTANT

- Use this feature with caution, as renaming a domain may result in problems with software running on this domain.
- After you have changed a domain name, you should update the SSL certificate correspondingly.
- Make sure that you inform a domain owner and domain users of the domain name change.

4. To set the traffic statistics retention period, select the Retain traffic statistics for Months checkbox, and type the number in the input field provided.
5. Click OK to submit the changes and return to the Domain administration page.

Customizing DNS Settings

Through Plesk, a user can customize DNS settings for each domain created. The Plesk administrator can also enable the client to customize his/her own DNS settings; however, it is very important that the client possesses a strong understanding of DNS prior to making any modifications to the DNS settings.

NOTE

Improper setup of DNS results in improper functioning of web, mail and FTP services.

Types of DNS Records

There are five types of accessible DNS records:

A = Address - This record is used to translate host names to IP addresses.

CNAME = Canonical Name - Used to create additional host names, or aliases, for hosts in a domain.


NS = Name Server - Defines an association between a given domain name and the name servers that store information for that domain. One domain can be associated with any number of name servers.

MX = Mail Exchange - Defines the location of where mail should be delivered for the domain.

PTR = Pointer - Defines the IP address and host name of individual hosts in the domain. Translates IP addresses into host names.

Changing DNS Settings

Plesk retrieves the default DNS settings from Server DNS configuration. In order to change the DNS settings, follow these steps:

1. At the Domain Administration page click the  DNS icon to access the DNS Settings page.
2. The DNS Zone Status icon indicates whether DNS is turned on or off.

- If you wish to turn DNS on or off for the domain, click the



Enable or



Disable icon respectively.


- Turning the DNS zone off will refresh the page, so that only a list of nameservers remains.
 - If you are running remote DNS, and therefore want to turn DNS off for the domain, you should first create the appropriate NS entries for the domain and remove any inappropriate NS entries possibly created by the default DNS template created in the Server DNS section. At that point, turn DNS off. You see that the name server(s) for the domain remains listed as a link.
 - You can perform a test on these name servers by selecting any of them. Selecting any name server will perform an NSLookup to check for the DNS records for your specific domain on that specific name server. NSLookup is used to verify the A record for the domain, the CNAME record for www, and the MX record to ensure that these basic records are resolved properly on the remote name server. The results are interpreted and presented through the user interface.
3. In order to add a DNS entry, select the type of record you wish to create and click Add. Each record type has its own different setup. When creating DNS entries within a specific DNS zone the name of the zone must be present for all entries. Plesk sets the screen up with certain unchangeable fields in order to prevent possible errors within the zone.
- For an A record you will need to enter the domain name for which you wish to create an A record. If you are simply defining an A record for your main domain, then you should leave the available field empty. If you are defining an A record for a name server then you will need to input the appropriate entry for the given name server (ie. ns1). Then, you need to enter the appropriate IP address to which to associate the domain name. Then select OK to submit your entry.
 - For a NS record, you will need to enter the domain name for which you wish to create the NS record. If you are defining an NS record for your main domain, then you will leave the available field blank. Then enter the appropriate name server name in the field provided. You will need to enter the complete name (i.e. ns1.mynameserver.com). Then select OK to submit your entry.
 - For a MX record, you will need to enter the domain for which you are creating the MX record. For the main domain, you would simply leave


the available field blank. You will then need to enter your mail exchanger, this is the name of the mail server. If you are running a remote mail server named 'mail.myhostname.com' then you would simply enter 'mail.myhostname.com' into the field provided. You will then need to set the priority for the mail exchanger. Select the priority using the drop-down box: 0 being the highest and 50 being the lowest. Keep in mind you would also need to add the appropriate A record, and/or CNAME if applicable for the remote mail server. Select OK to submit your entry.

- For a CNAME record, you will need to first enter the alias domain name for which you wish to create the CNAME record. You then need to enter the domain name within which you want the alias to reside. Any domain name can be entered. It does not need to reside on the same server. Select OK to submit your entry.
 - For a PTR record you will first enter the IP address/mask for which you wish to define the pointer. Then enter the appropriate domain name for this IP to be translated to. Select OK to submit your entry.
4. To remove a DNS record, select it using a corresponding checkbox, and click Remove Selected. Before anything is processed you will be asked to confirm the deletion.

From the DNS Settings page, you can switch the DNS zone type from master to slave.

To switch the DNS zone, follow these steps:

1. Click on the  Switch icon. The DNS Zone Properties page will open and the DNS zone type will change to slave.
2. Enter the DNS master server IP in the field provided, and click Add. The new DNS master server record will be added immediately to the list of DNS master servers.
3. To remove a DNS master server record, select it by clicking in the appropriate checkbox, and click Remove Selected.

To switch the DNS zone type back to master, click the  Switch icon

again. You will return to the DNS Settings page.


To restore the DNS zone by the DNS template, you can select the IP address from the drop-down list to be set up in the template, add the www prefix if required, and click on the Default button to restore it.

Managing Mail

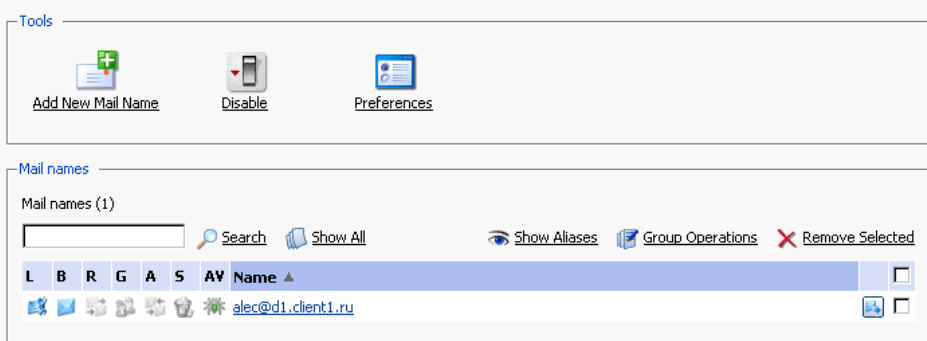
Using Plesk, you can create and manage e-mail boxes for individuals within a domain, or your client can manage the e-mail accounts via domain self-administration. As an administrator, you can use the following e-mail administration functions:

- Create, edit or delete e-mail boxes and set individual mailbox quotas.
- Allow mail user access to the control panel.
- Use several mail aliases for a single mail name.
- Set up redirection of mail addressed to the mail name to another e-mail address.
- Enable the mail name to function as a mail group used for forwarding mail to a number of e-mail addresses at once.
- Manage mail group membership for the mail name
- Set up autoresponders: automatic replies to e-mail sent to the mail name.
- Configure the integrated anti-spam software for filtering incoming mail.
- Configure the antivirus filter.



Managing Mail Names

When you create e-mail accounts for domain users, you are creating e-mail boxes, which will be accessible via POP3 or IMAP protocols. Mailbox creation is as easy as typing in a name and password. Click the  Mail icon at the


Domain administration page to access the Mail Names Management functions:




The screenshot displays the Plesk Mail Names Management interface. It is divided into two main sections: 'Tools' and 'Mail names'. The 'Tools' section contains three buttons: 'Add New Mail Name' (with a plus icon), 'Disable' (with a mobile phone icon), and 'Preferences' (with a gear icon). The 'Mail names' section shows a list of mail names. At the top, there is a search bar and several action links: 'Search', 'Show All', 'Show Aliases', 'Group Operations', and 'Remove Selected'. Below this, a table lists mail names. The first entry is 'alec@d1.client1.ru', which is highlighted in blue. The table has columns for 'L', 'B', 'R', 'G', 'A', 'S', and 'AV Name'. There are also icons for adding, deleting, and refreshing the list.

From this page, you can enable/disable the mail service for the domain. To this effect, click the  Enable or  Disable icon respectively.

You can allow the use of web-based e-mail for the domain through webmail.'domain name' and set up a mail bounce message or a catch-all e-mail address for invalid (nonexistent) user names. These items are used to handle mail that is received for this domain for a mail account that has not been created within the domain:

1. Click  Preferences
2. To utilize a mail bounce message select the radio button for Bounce with phrase and enter the appropriate text.
3. To utilize a catch-all e-mail address, select the radio button for Catch to address and enter the appropriate e-mail address.
4. Check or uncheck the WebMail checkbox to allow or disallow the use of web-based e-mail for the given domain through webmail.'domain name'.
5. Click OK to submit the changes.

To create a new mail name, follow these steps:

1. Click  Add New Mail Name. The mail name creation page will open:

Mail name form

Mail name * @ d1.client1.ru

Old password None

New password

Confirm Password

Control panel access

Display lines per page

Button label length

Interface language

Interface skin

Allow multiple sessions

Mailbox

Mailbox quota Default for the domain (Unlimited)
 Enter size KBytes

Enable spam filtering (Administrator has disabled spam filtering)








* Required fields

2. Enter the desired name into the Mail name field and type a password that will also be used by the mail user to access the control panel.
3. To allow the mail user access to the control panel, check the Control panel access checkbox and select the interface language and skin for the mail

user's sessions. Check the Allow multiple sessions checkbox to allow multiple sessions under the same mail user's login. For the mail user's interface, you can also set a number of list items per page, and set the limit on size of interface buttons.

4. To create a mailbox, select the Mailbox checkbox, specify the mailbox quota if desired, and enable the mail filtering using the Enable spam filtering checkbox if you want the mail to be filtered by server.
5. Click OK to submit all changes.

After the mail name is created, it appears on the Mail Names list, accompanied by seven icons:

-  indicates the mail user access,
-  represents a mailbox,
-  represents a mail redirect
-  represents a mail group
-  represents a mail autoresponder
-  represents spam filtering
-  represents antivirus filtering


These icons are displayed in gray when the corresponding services are not active, and appear in color when active. To edit mail name account settings select a mail name or click on an icon corresponding to the service you wish to configure.

To switch to displaying the mail aliases for the mail names in the list, click the Show Aliases button, to hide them use the Hide Aliases button.

To remove one or several mail names, check the checkboxes in the mail names list, corresponding to the mail names you wish to remove and click Remove Selected.











Enabling Mail Services

When you click on a mail name, you access the mail name properties page, which allows setting up any combination of services for a mail name: mail alias, mailbox, redirect, mail group, autoresponder, spam filter, and antivirus filtering.

1. Click the  Mail icon at the Domain administration page. The Mail Names page appears.

2. Click on the mail name you wish to edit. This takes you to the Mail Name Properties page:

Tools

 Add New Mail Alias	 Preferences	 Mailbox	 Redirect	 Mail Group	 Groups
 Autoresponders	 Spam Filter	 Dr.Web	 WebMail		

Info

Control panel access	<input checked="" type="checkbox"/> On	Mailbox	<input checked="" type="checkbox"/> On
Redirect	<input type="checkbox"/> Off	Autoresponders	<input type="checkbox"/> Off
Mail group	<input type="checkbox"/> Off	SpamAssassin	<input checked="" type="checkbox"/> On
Antivirus mail checking	<input checked="" type="checkbox"/> Incoming and outgoing mail		

Mail aliases

No items.

3. To set up or configure a mail service for the mail name, click on a corresponding icon (button) in the Tools group or select a shortcut in the Info group.


The Mail Aliases area lists the aliases created for the mail name. To add new mail alias, click the





Add New Mail Alias icon.

To edit an alias, click on its title. To remove an alias, select it using a corresponding checkbox, and click Remove Selected.

4. To edit the mail name preferences, click  Preferences.

5. To edit mailbox quota and enable spam filtering, click  Mailbox.

6. To set up mail forwarding - a redirect, click  Redirect.

7. To enable a mail group service for the mail name and add new members to the mail group, click  Mail Group.

- 8.



Groups.

9. To manage autoresponders and autoresponder attachment files, click Autoresponders.



10. To manage personal spam filtering settings, click Spam Filter.



11. To manage antivirus settings, click Dr.Web.



12. To manage your mail box via Webmail interface, click Webmail.



Mailbox

Using this function, you can set up mailbox quota and enable spam filtering:

1. When on the mail name properties page, click on the Mailbox icon
2. To enable the mailbox, select the Mailbox checkbox.
3. To set up the mailbox quota, select the Default for domain radio button to set the limit to the maximum available for the given domain, or select Enter size and enter the quota you wish to set, in Kilobytes, for the given mailbox. Note that this limit may not exceed the default set for the domain.
4. Select the Enable spam filtering checkbox, to enable mail filtering based on your personal settings.
5. Click OK to submit your changes.

Once enabled, the mailbox icon on the Mail Names page appears in color.

Managing Mail Redirects

You can forward or redirect email from one mailbox to another email address. By creating an email redirect or alias, messages are sent to a different email box without requiring the sender to know the new address. Email can be redirected to an address outside the domain. Use this redirect feature to:

- Temporarily forward mail when the person who owns the mailbox is unavailable.

- Send mail to a new mailbox if a mailbox user is leaving the company.
- Forward mail to a new account, which will eventually replace an old mailbox. (e.g. someone is changing their name but hasn't had time to inform all correspondents of the change yet).

In order to enable and set a redirect for the mail name, follow these steps:

1. On the mail name properties page, click the Redirect icon.
2. Select the Redirect checkbox, and in the text box to the right, enter the appropriate address that you wish mail for this mail name to be forwarded to.
3. Click OK.

Once enabled, the Redirects icon on the Mail Names page appears in color.

Managing Mail Groups

A mail group is a list of several email accounts that are grouped together under one email address. This feature enables sending one message to multiple recipients at once. For example, if you want to send the same message to five people in the technical support department, you can create a "Support" email group that includes the individual email addresses for all five staff members. When someone sends a message to mail group "Support", he/she only types and sends one message, but copies of the message go to all five individuals. The sender does not need to know the addresses for all five individuals, just the group name. Essentially, mail groups help save time and effort.

In order to enable and set up a mail group for the mail name, follow these steps:

1. On the mail name properties page, click the Mail Group icon.
2. Before enabling the mail group, you need to add at least one mail group member. Click Add New Member.
3. Enter the desired external e-mail address into the E-mail input field and/or select one or more of the listed mail name accounts using checkboxes, and click OK.

NOTE

Group members can consist of either external mail addresses (those not belonging to this domain) or accounts, which exist within the domain.

4. The selected addresses will appear in the list of Mail group members on the Mail Name Properties page.
5. To delete one or several group members, select the corresponding checkbox and click Remove Selected.

Once enabled, the mail group icon on the Mail Names page appears in color.

Clicking on the Groups button you will access the Mail Groups Management page.

All mail groups created for the domain are displayed on that page and two lists are presented: the list of mail groups you are currently subscribed to is located on the right side, and the list of available mail groups is on the left.

NOTE

If you are removing a mail name from a mail group, and this is the last member in this group, then this group is deactivated. The name of the group is no longer listed in the list of groups available for adding.

- If you wish to subscribe to a new mail group, select the desired group from the list of available mail groups, and click Add>>.
- If you wish to unsubscribe from a mail group, select it in the right side list, and click <<Remove.
- Click Up Level to return to the Mail Name properties page.

Managing Mail Autoresponders

A mail autoresponder is an automatic reply that is sent out from a given mail name when incoming mail is received at that address. Autoresponders can include both a text message and attached files. This mail function is often used on mail accounts for individuals who need an automated response because they are away, or are unable to check their mail for any number of reasons. In the autoresponders management section you can upload and include attachment files for your autoresponders, enable the autoresponder function for a given mail name, and access the list of autoresponders.

Attachment files repository

For the autoresponder feature you have the option to include file attachments. To include a file to be selectable within the set up of autoresponders for the given mail name, use the Attachment Files icon available from the Autoresponders management page. The Attachment files repository page opens. It allows you to upload files and remove them.

To upload a file, specify the path and filename in the File name field, and click Send File. The attachment will then appear in the Repository.

These files will be available for any autoresponders that are set up for the given mail name. To delete one or more files, select the checkboxes related to the files you wish to remove, and click Remove Selected button.

In order to enable and set up a mail autoresponder for the given mail name, follow these steps:

1. On the mail name properties page, click the Autoresponders icon. Autoresponders management page will open.
2. Click Add New Autoresponder. The autoresponder creation/editing page will open.
3. Enter the name into the Autoresponder name field.
4. Below the Request text input box, you can determine whether an autoresponder responds to specific text or set of characters found within either the subject line or body of the incoming email, or if it responds to ALL incoming requests. Type the phrase or a set of characters in the Request text input box, and select the appropriate radio button to enable checking **in the subject** or **in the body**.
5. To set up the autoresponder to always respond, regardless of the contained text, click the bottom radio button for always respond.
6. You can select a specific subject to appear in your automatic reply using the Answer with subject option. To simply respond with the same subject as was received from the incoming request select the radio button for the default setting. To specify a certain subject line select the radio button beside the text box and enter the desired text.
7. In the Return address field, you can specify the return address that will be set up in the autoresponder message. This is done for the messages not to be directed to the autoresponder itself, when users use the "Reply to the message" function in their mail client software.
8. You can enter text to be included into the autoresponder in the Reply with text field.
9. Using the Add New Attachment button, you can attach files to be included in the autoresponder. These files must be uploaded into the Repository on the Mail Names Properties page. Select the uploaded file from the Attach files list, and use the Add New Attachment button to attach the file to the autoresponder. To remove an attached file, select the corresponding checkbox, and click Remove Selected.

10. You can limit the frequency at which the autoresponder responds to the same unique address, after receiving multiple emails from it. In the Reply to the unique email address not more than [] times a day input field, you can set the autoresponder to respond no more than a specified number of times per day. The default setting is to respond not more than 10 times in one day to unique mail addresses.
11. You can define the number of unique addresses that the autoresponder will remember. Enter the desired number in the Store up to: field. This memory enables the system to control response frequency. In the event of extremely high mail volume, to protect server performance, you can limit the address memory of the system database.
12. To specify an email address to which incoming requests are forwarded, enter the new e-mail in the Forward request to e-mail field. Email requests meeting the requirements established on this page will be forwarded to this alternate e-mail address.
13. Click OK to submit all changes.
14. Click the Enable button to enable the autoresponder service.

Managing the spam mail filter settings

Plesk allows for setting up and using black lists and white lists for filtering mail at the server level as well as at the user level.

The user level spam filter functionality is available for each specific mail name configured as a mailbox. That means that the Mailbox functionality should be activated for the selected mail name.

If the spam filtering functionality is enabled for users by the Administrator, it should first be activated. To do that:

1. Go to the selected Mailbox management page (select the mail name and click the Mailbox icon, Tools group);
2. Check the Enable spam filtering checkbox;
3. Click OK to save changes.

You will see the Spam Filter icon become active (displayed in color), meaning that the spam filtering functionality is now available for this mail name. If the spam filtering functionality was not enabled for the users by the Administrator, the Enable spam filtering checkbox at the Mailbox management page will be inactive and the Spam Filter icon will also be inactive (displayed in gray).

Click on the Spam Filter icon to access the Spam filter configuration page, where you can set the filtering rules for the selected mail name.

If the Administrator has set up and activated mail filter at the server level, all the incoming mail will be processed with it before it reaches the users' mailboxes. You can choose to use or, on the contrary, not use the server wide settings for your mail. If you decide not to use the server wide settings, those will be disregarded and your mail will be processed only according to the configuration you set at the user level.

1. To use (not use) the server wide mail filtering settings, check (uncheck) the Use server wide settings checkbox;
2. Click Set to save the changes.

In order to recognize a mail message as spam it needs to score a certain amount of hits. The hits are scored according to the internal SpamAssassin settings and based on the contents of the mail messages and its subject. You can change the sensitivity of the spam filter by varying the amount of hits required for marking a message as spam. The more hits are required the less sensitive the filter is, and vice versa – the less hits are required the more sensitive the filter is.

1. The default amount of hits is set to 7. If you wish to change this value, click into the Hits required for spam input box and type in the new value.
2. Click Set to save the changes.

You can choose what to do with the mail recognized as spam: you can choose to either delete it, or to mark it as spam and leave it in the mailbox.

1. Select the Delete radio-button to delete mail recognized as spam, or the Mark as spam and store in mailbox radio-button to leave the mail marked as spam in your mailbox;
2. Click Set to save the changes.

If you decide to leave the mail recognized as spam in your mailbox such messages will be marked correspondingly so that they can be easily visually identified. In particular, a special string is added to the subject of the message (e.g., by default the string *****SPAM***** will be added to the spam messages subjects). You can change this string (or tag) to whatever you like, or even to disable this option.

1. In order to activate/deactivate the option of modifying the spam messages subject, check the Modify spam mail subject;
2. To change the text of the string, click into the input field and enter the new text;
3. Click Set to save the changes.

Black list is a list of E-mail addresses, which are automatically considered as

sending unsolicited mail – spam. Therefore, all messages coming from the E-mail addresses that match those specified in the black list will automatically be marked as spam.

You can add to the black list either exact E-mail addresses or patterns, using wildcards (*, e.g.: entry *@spammers.online.com will cause all messages coming from the domain spammers.online.com be marked as spam, regardless of what the exact mail name is).

1. Enter the E-mail address or pattern into the Email pattern input field;
2. Click Add to add the new entry to the black list, the new entry will appear in the user's black list section.

The Administrator's black list section contains the server wide black list entries that were added by the Administrator. If you chose to use the server wide filtering settings (the Use server wide settings checkbox checked) you may wish to edit this section by removing unnecessary entries. To do that, just select the Administrator's black list entry and click Remove.

White list contains E-mail addresses, which are automatically considered as trustworthy. Therefore, all messages coming from the E-mail addresses that match those specified in the white list will never be marked as spam.

You can add to the white list either exact E-mail addresses or patterns, using wildcards (*, e.g.: entry *@your-company.com will cause all messages coming from the domain your-company.com not be marked as spam, regardless of the content of a message).

1. Enter the E-mail address or pattern into the Email pattern input field;
2. Click Add to add the new entry to the white list, the new entry will appear in the user's white list section.

The Administrator's white list section contains the server wide white list entries that were added by the Administrator. If you chose to use the server wide filtering settings (the Use server wide settings checkbox checked) you may wish to edit this section by removing unnecessary entries. To do that, just select the Administrator's white list entry and click Remove.

You can train your mail filters on actual messages you receive. Click the Training icon in the Tools group to access the Spam filter training page. The headers for all mail that comes to your mailbox will be listed here. Each such header you can select to mark as spam, ham (good mail) or forget.

- Marking a header as spam will result in recognition of same or similar mail as spam;
- Marking a header as ham will result in recognition of same or similar mail as not spam;

- Option forget clears the database of any rules (spam or ham) previously set for this header.

Once you select one of the options, appropriate rules will be added to the spam filter database, which will allow in the future to recognize messages similar to the ones it was trained on, and make decisions regarding whether a message should be considered spam or not based on that.

Use the Clear button if you want to clear the spam filter's database.

Click OK to save the changes and return to the Spam Filter page.

This concludes setting up the user level spam mail filter. All the incoming mail for the selected mail name will be processed according to these settings.

Enabling Antivirus Checking For Mailboxes

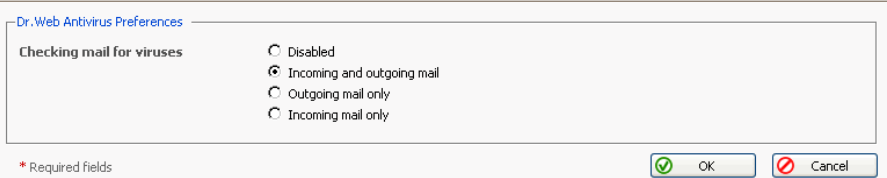
For a user's mailbox you can enable the antivirus scanner to work in one of the following modes: checking incoming and outgoing mail, checking outgoing mail only, and checking only incoming mail.

When antivirus scanning is enabled, all e-mail messages containing viruses are intercepted and placed to the directory `/var/drweb/infected`. You should clean this directory from time to time.

To enable antivirus scanning for a mailbox, follow these steps:

1. On the mail name properties page click  Dr.Web. The antivirus

preferences page will appear:




2. Select a required scanning mode and click OK.

Performing Group Operations on Mail Names

In cases when you need to introduce certain similar changes to several mail name accounts, you can use the Group Operations function, made available to simplify administration of multiple accounts. Using this feature you can, for instance, select a number of mail names, and enable antivirus protection for all of them - all that within a single operation, without having to select each mail name independently and edit its settings.

To perform group operations on mail names, follow these steps:

1. In the list of mail names, select the mail names, whose accounts you wish to modify by checking the corresponding checkboxes.
2. Click the  Group Operations icon. The Group Operations page will appear.
3. To enable a specific mail service, select an appropriate radio-button in the Enable column.

To Disable a service, select the radio button in the Disable column.

Use the Do not change option to leave as is.

4. Click OK to apply the changes to the selected mail names.






Managing Mailing Lists

You can create and manage mailing lists via Plesk. Click the  Mailing

lists icon on the Domain administration page to access the Mailing Lists Management functions: activating/deactivating the Mailing List service, adding, administering and removing mailing lists, enabling/disabling the selected mailing lists.

The status of Mailing list service and status of a Mailing list are represented by the following icons:



Table 5.2. The Mailing lists service/mailling lists status icons

Icon	Meaning
The Mailing lists service status	
	means that the Mailing lists service is activated
	means that this mailing list is presently deactivated.
The mailing list status	
	means that the mailing list is activated
	means that this mailing list is presently deactivated and inaccessible.
	the mailing list is disabled as the mailing lists service is disabled for the domain.

Activating/deactivating the Mailing lists service


In order to disable the support of mailing lists the Mailing lists service can be deactivated. When the mailing list service is deactivated, all mailing lists also change their status to 'deactivated' and therefore cannot be accessed.

NOTE



When the mailing list service is deactivated, the status icon will change to , and the status icons of the mailing lists at this domain will change to .

Activation of the mailing list service enables access to active mailing lists.

NOTE


When the mailing list service is activated, the status icon will change to , and so will the status icons of the mailing lists at this domain that were active before deactivating the mailing list service.

To activate/deactivate the mailing list service:

1. Click the  Enable or  Disable icon respectively. The confirmation will appear querying whether you actually wish to change the status of the mailing list service.
2. Click OK to proceed with changing the status.

Creating a new mailing list

To create a new mailing list, follow these steps:

1. On the mailing lists management page, click the  Add New Mailing List.
2. Specify the mailing list name.
3. Specify the mailing list administrator's e-mail address to notify the administrator of the mailing list creation, and check the corresponding checkbox to enable the notification.
4. Click OK to create a new mailing list.


After the mailing list is created, you are taken to the page where you can add to

and remove users from the mailing list.

To add a subscriber, click Add New Subscriber. Enter the user's e-mail address, and click OK.

The e-mail addresses of mailing list users are displayed in the list. To remove a user, select a corresponding checkbox and click Remove Selected.

Accessing the mailing list administration

The mailing list administration can be accessed by clicking on the icon  corresponding to the necessary mailing list. The mailing list administration software interface will open in a new browser window.

Removing mailing lists

You can remove one or several mailing lists at the same time. To remove a mailing list(s):

1. At the Mailing lists management page, select the checkboxes corresponding to the mailing lists you wish to remove.
2. Click Remove Selected. The Mailing lists removal page appears.
3. Confirm removal, and click OK.

Enabling/disabling mailing lists

You can enable/disable one or several mailing lists at the same time. To change the current state of a mailing list(s):

1. At the Mailing lists management page, check the checkboxes corresponding to the mailing lists you wish to change state.
2. Click the On/Off icon. The confirmation page appears.
3. Click OK. The state of the selected mailing lists will be changed.

Setting Up a Domain User Account

If you wish to allow a domain owner to use Plesk control panel for managing his/her domain, you should create a domain user account in Plesk. When a user is logged in to a domain user account, his/her control panel environment comprises the specific Domain's administration page, and access to the domain management capabilities is limited in accordance with the permissions you define.

For accessing the domain user account, a user should specify his/her domain name as the control panel login name.


To set up the Domain User account:

1. Click the  Domain User icon at the Domain administration page.

The Domain User Properties page appears.


2. To allow domain level entry, select the Allow domain user access checkbox, enter and confirm the password.
3. Set the visual preferences for the domain user's environment: select the domain user's language, skin, limit the number of entries displayed in various control panel object listings per page, and limit the button label length for domain user's custom buttons, if desired.
4. Select the Allow multiple sessions checkbox to allow several simultaneous sessions under the same domain user's login name and password.
5. Use the Permission section to define a set of management capabilities granted to the user.
6. In the Personal information section, fill in the domain user information.
7. To submit the changes made, click OK.

Registering a Domain with MPC

You must officially register a domain and Internet address before you create it in Plesk. Plesk allows accessing the domain registration facilities provided through My.Plesk.com. To register a domain, click the  Register icon on

the Domain administration page. You will be taken to the MPC (My.Plesk.com) interface.

Accessing Additional Services (Extras)


From the Plesk control panel, you can access external services, such as third party solutions provided through My.Plesk.com. To do that, click the 

Extras icon on the Domain Administration page. You will be taken to the MyPlesk.com login page, where you will need to enter your login and password. You will then be taken to the Domain Tools area.

Managing Databases

With Plesk you can create multiple databases and multiple users within each database, and make use of DB WebAdmin - a web-based administration tool, allowing you to sort, edit, and create tables within a given database.

Creating a New Database


1. At the Domain administration page, click the  Databases icon. The

Databases Management page appears:

Clients > Alec > domain.com >

Databases for domain domain.com [Up Level](#)


Tools

 [Add New Database](#)

Databases

Databases (1)

[Search](#) [Show All](#) [Remove Selected](#)

T	Name ▲	
	base1	<input type="checkbox"/>

2. Click  Add New Database. The page appears:

Clients > Alec > domain.com > Databases >

Add New Database [Up Level](#)

Add new database

Database name

Type

* Required fields

3. Enter the desired name for the database, select the database type and click OK. The Database Users page appears:

Clients > Alec > domain.com > Databases >

Users for database database2 on domain domain.com [Up Level](#)

Tools

[DB WebAdmin](#) [Add New Database User](#)

Database users

No Database users.

4. To add database users to the newly created database, click  Add

New Database User. The Database user addition page appears:

Clients > Alec > domain.com > Databases > database2 >

The database user addition for database2 database [Up Level](#)

Database user

Database user name	<input type="text"/>
Old password	NONE
New password	<input type="password"/>
Confirm Password	<input type="password"/>

* Required fields

5. Enter the user name into Database user name text box, specify a password in the New Password text box, and then enter it again in the Confirm Password text box. Select OK to complete the creation of new user.
6. Once you have completed the creation of the new database and its users click Up Level to return to the Databases Management page.
7. To add further databases, follow the steps outlined above.


Editing a Database

1. On the Databases Management page, click on the database name that you wish to edit. The Database Editing page appears:


Clients > Alec > domain.com > Databases >

Users for database database2 on domain domain.com [Up Level](#)

Tools



DB WebAdmin




Add New Database User

Database users


Database users (1)

Search
Show All
X Remove Selected

Name ▲	□
user2	□

2. To add database users to the selected database, click  Add New Database User. The Database user addition page appears:


Clients > Alec > domain.com > Databases > database2 >

The database user addition for database2 database  Up Level

Database user

Database user name	<input type="text"/>
Old password	NONE
New password	<input type="text"/>
Confirm Password	<input type="text"/>

* Required fields

3. Specify user name, enter new password in the New Password text box, and then re-enter it into the Confirm Password text box. Select OK to complete creation of the new user. Selecting Up Level will ignore all entries and return to the Database Editing page making no changes.
4. To edit the password of an existing database user, select the user from the database user list.
5. To delete existing database users select the users that you wish to delete using the corresponding checkboxes, and click Remove Selected.
6. To access and/or edit database content use the  DB WebAdmin function.
7. Once you are finished with editing the database and its users, click Up Level to return to the Database Management page.
8. To delete databases from the system, select the databases that you wish to delete using the checkboxes and click Remove Selected.
9. To edit further databases, follow the steps outlined above. To return to the Domain Administration page, click Up Level.

Domain SSL Certificates Repository Management

Plesk enables you to upload a Secure Socket Layer (SSL) Certificate, generate a Certificate Signing Request (CSR), and/or generate a Self-signed Certificate. Each certificate represents a set of rules used when exchanging encrypted information between two computers. Certificates ensure secure communications; this is especially important when handling e-commerce transactions and other private transmittals. Only authorized users can access and read an encrypted data stream. If your client intends to implement SSL support for a virtual host domain, you can grant permission for SSL capabilities to the domain. Or, your client can implement the SSL certificate by self-administering his/her domain.

i Notes on Certificates:


- You can acquire SSL certificates from various sources. We recommend using the CSR option within Plesk. You can also purchase the certificate through the My.Plesk.com (MPC) web site.
- If using a SSL certificate issued by a certificate authority other than Thawte or Verisign, a rootchain certificate is required to appropriately identify and authenticate the certificate authority that has issued your SSL certificate.
- Once you have obtained a SSL certificate or a certificate part, you can upload it through Plesk using the instructions, which follow in this section.

! IMPORTANT

When you add a certificate, it is not installed automatically onto the domain or assigned to an IP address, but only added to the Certificate repository.

You can assign a certificate to an IP address at the Client's IP pool, at the server IP addresses management page, and during hosting creation on an exclusively granted IP.

Accessing the Domain SSL Certificates Repository



To access the Domain certificates repository page, click the  Certificates

icon at the Domain administration page. The certificates repository page will open displaying the list of available certificates:

Clients > Alec > domain.com >

Certificates Up Level

Tools

 Add Certificate  View Certs

Find the appropriate private key to the certificate

Certificate

Certificates

SSL certificates (1)

Remove Selected

R	K	C	A	Certificate Name	Used
				cert1	<input type="checkbox"/>

The four icons, preceding the certificate name in the list, indicate the present parts of a certificate. The icon displayed in the R column indicates that the Certificate Signing request part is present in the certificate, the icon in the K column indicates that the private key is contained within the certificate, the icon in the C column indicates that the SSL certificate text part is present and the icon in the A column indicates that CA certificate part is present. The number in the Used column indicates the number of IP addresses the certificate is assigned to.

Uploading a certificate file with finding the appropriate private key


After you have received your signed SSL certificate from the certificate authority you can upload it from the Certificate repository page. First make sure that the certificate file has been saved on your local machine or network. Use the Browse button to locate the certificate. Click Send File. The existing certificate with appropriate private key will be found and the certificate part will be added to the repository.

Changing a certificate name


To change a certificate name follow these steps:

1. At the certificate repository page, select a certificate from the list. You will be taken to the SSL certificate properties page.
2. Click in the Certificate name field and edit the name as desired.
3. Click Set.

Viewing purchased certificates

After you have purchased your certificates through the control panel you can utilize the  View Certs function to view the information about your SSL certificate(s).


Downloading a certificate to the local machine

To download the certificate to the local machine, click on the  icon, corresponding to the required certificate. Select the location when prompted, specify the file name and click Save to save it.

Removing a certificate from repository

To delete one or several certificates from the repository, at the certificate repository page, select the corresponding checkboxes, and click Remove Selected.

Adding a certificate to the repository

To add a certificate to repository, click the  Add Certificate icon at the

Domain certificate repository page. The SSL certificate creation page will open. On this page you can generate a self-signed certificate, certificate-signing request, purchase a SSL certificate, and add the certificate parts to an existing certificate.

Generating a self-signed certificate

To generate a self-signed certificate follow these steps:

1. Specify the certificate name.
2. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop-down list.
3. Select a country from the drop-down list.
4. Specify the state or province, location (city).
5. Enter the appropriate organization name and department/division in the field provided.
6. Enter the Domain Name for which you wish to generate the self-signed certificate.
7. Specify the E-mail address.
8. Click the Self-Signed button. Your self-signed certificate will be immediately generated and added to the repository.

Generating a Certificate Signing Request

To generate a certificate signing request (CSR) follow these steps:

1. Specify the certificate name.
2. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop-down list.
3. Select a country from the drop-down list.

4. Specify the state or province, location (city).
5. Enter the appropriate organization name and department/division in the field provided.
6. Enter the Domain Name for which you wish to generate the certificate signing request.
7. Specify the E-mail address.
8. Click the Request button. A certificate signing request will be generated and added to the repository. You will be able to add the other certificate parts later on.

Purchasing a Certificate


To purchase a new certificate follow these steps:

1. Specify the certificate name.
2. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop-down list.
3. Select your country from the drop-down list.
4. Enter your State or Province, your Location (City), Organization Name (Company), organization department (division name)
5. Enter the Domain Name for which you wish to purchase a SSL certificate.
6. Enter the domain owner's e-mail address in the appropriate field.
7. Select the Buy Cert button. You will be taken step by step through the purchase procedure. It is important to note that you must make sure that all the provided information is correct and accurate, as it will be used to generate the private key.

When using Plesk to purchase your SSL certificate you will receive the certificate file via e-mail from the certificate signing authority. Follow the instructions in the Uploading a certificate file with finding the appropriate private key section to upload the certificate to the repository.

Uploading certificate parts

If you have already obtained a certificate containing private key and certificate part (and may be a CA certificate), follow these steps to upload it:

1. At the certificate repository page, click the  Add Certificate icon. You will be taken to the SSL certificate creation page.
2. In the Upload certificate files section of the page, use the Browse button to locate the appropriate certificate file or a required certificate part.

NOTE

Your certificate can be contained within one or several files, so you may upload the certificate by parts or as a single file, selecting it in several fields (Plesk will recognize the appropriate certificate parts and upload them correspondingly).

3. Click Send File. This will upload your certificate parts to the repository.

You can upload an existing certificate in two ways:

1. Choose a file from the local network and click the Send File button (.TXT files only).
2. Type in or paste the certificate text and private key into the text fields and click the Send Text button.

Uploading a CA certificate

For the certificates purchased through certificate signing authorities other than Verisign or Thawte you will receive what is typically called a CA Certificate, or rootchain certificate. The CA Certificate is used to appropriately identify and authenticate the certificate authority, which has issued your SSL certificate. To upload your CA Certificate, follow these steps:

1. At the certificate repository page, select a certificate from the list. You will be taken to the SSL certificate properties page.
2. Use the Browse button, within the section related to the certificate uploading, to locate the appropriate CA Certificate file.
3. Click Send File. This will upload your CA Certificate to the repository.

You can upload an existing certificate in two ways:

1. Choose a file from the local network and click the Send File button (.TXT files only).
2. Type in or paste the CA certificate text into the text field and click the Send Text button.

Generating a CSR using an existing private key

A situation may occur in some cases, that you have a certificate in the repository, which has only the private key part and the other parts are missing due to some reasons. To generate a new Certificate Signing Request using the existing private key, follow these steps:


1. At the certificate repository page, select from the list a certificate, which has the private key part only. You will be taken to the SSL certificate properties page.
2. Click Request.

Removing a certificate part

After you have uploaded a CA certificate part (rootchain certificate), you are able to remove it. To do so, follow these steps:


1. At the certificate repository page, select a certificate from the list. You will be taken to the SSL certificate properties page.
2. Click on the Remove button located next to the CA certificate field.

Managing Tomcat Web Applications




Plesk supports deploying and managing Tomcat web application in order to enable users to set up hosting with JSP support. Click the  Tomcat icon

on the Domain Administration page, to access the Tomcat Web Applications Management functions:

Clients > Alec > domain.com >

 **Tomcat web applications for domain domain.com** [Up Level](#)

Tools

 Add New Web Application	 Enable	 Refresh
---	--	---

Tomcat web applications

No Tomcat web applications.






At this page you can activate/deactivate the Tomcat service, upload the Tomcat web application archive files (.WAR files) and remove them, start/stop/restart web applications, and access them.

IMPORTANT

Users can only manage the Tomcat web application through Plesk interface. Managing the web application through the Tomcat manager was disabled in order to maintain coherence of Plesk Tomcat configuration.

The status of Tomcat service and the status of Tomcat web application are represented by the following icons:

Table 5.3. The Tomcat service/web applications status icons


Icon	Meaning
The Tomcat service status	
	means that the Tomcat service is activated
	means that the Tomcat service for the domain is presently deactivated.
The Tomcat web application status	
	means that the web application is activated
	means that this web application is presently deactivated and inaccessible.
	means that web application is inaccessible.

Activating/deactivating the Tomcat service



In order to disable the support of Tomcat web applications the Tomcat service can be deactivated. When the Tomcat service is deactivated, all active Tomcat web applications also change their status to 'inaccessible' while all inactive web applications remain unchanged.

Activation of the Tomcat service enables access to active web applications.

NOTE


When the Tomcat service is activated, the status icon will change to , and so will the status icons of the Tomcat web applications at this domain that were active before deactivating the Tomcat service.

To activate/deactivate the Tomcat service:

- Click the  Enable or  Disable icon respectively. The confirmation will appear querying whether you actually wish to change the status of the Tomcat service.
- Click OK to proceed with changing the status. Clicking Cancel will leave the Tomcat service status unchanged.

Uploading Tomcat web application archive files

To upload a new Tomcat web application archive file, follow these steps:

1. Click  Add New Web Application.
2. Select the web application archive file. Use the Browse button to locate the desired file.

i NOTE


Only .war format (Web-application archive) files can be uploaded. The application file cannot be named as manager.war


3. Click OK. The new web application will be uploaded and added to the Tomcat web applications list.


Restarting the web applications



You can restart the Tomcat web applications directly from the control panel. In order to stop, start or restart a web application follow these steps:

1. Select the web application at the Tomcat web applications list on the Tomcat Web Applications Management page.

2. To start the web application: click on the  icon (Start the web application).

To stop the web application: click on the  icon (Stop the web application).

To restart the web application: click on the  icon (Restart the web application).

The current web application state will be marked by an icon:  (ON) for the web application running, and  (OFF) for the web application stopped.

Accessing the Tomcat web applications

A Tomcat web application can be accessed simply by clicking on its name in the Tomcat web applications list. The selected application will be opened in a new browser window.

i NOTE

If a web application is disabled, it cannot be accessed, and therefore, the link to it is also disabled.

Removing web applications

You can remove one or several web applications at the same time. To remove a web application(s):


1. Check the checkboxes in the Tomcat web applications list corresponding to the web applications you wish to remove.
2. Click Remove Selected. The Web Application Removal page appears.
3. Confirm the removal, and click OK.

Managing Web Users

A web user is a user account within web server. It is used to define locations for personalized web pages with individual FTP access. The result of creating a web user is a subdirectory within your domain (e.g. domain.com/~webuser).

Creating a web user account

To create a new web user account:



1. Click the  Web Users icon on the Domain administration page. The

Web Users page appears:

[Clients](#) > [Alec](#) > [domain.com](#) >

Web users of domain domain.com [Up Level](#)

Tools

 [Add Web User](#)  [Preferences](#)

Web users

No Web users.

2. Click the  Preferences icon to configure web user access format

and enable scripting capabilities. The Preferences page opens:

[Clients](#) > [Alec](#) > [domain.com](#) > [Web users](#) >

Preferences [Up Level](#)

Additional Features

Enable [webuser@domain.com](#) access format

Allow the web users scripting

* Required fields

3. To allow accessing web user pages via URLs like webuser@domain.com select the corresponding checkbox.

Select the Allow the web users scripting checkbox to enable scripting for web users' pages.

Click OK to submit your changes.

- To add a web user, click  Add Web User. You will be taken to the

Web User Configuration page:

Clients > Alec > domain.com > Web users >

Add new web user of domain domain.com [Up Level](#)

Web user

Web user name	<input type="text" value="Alec"/>	
Old password	NONE	
New password	<input type="password" value="*****"/>	
Confirm Password	<input type="password" value="*****"/>	
Hard disk quota	<input type="text" value="200"/> MB	<input type="checkbox"/> Unlimited
Apache ASP support	<input checked="" type="checkbox"/>	
SSI support	<input checked="" type="checkbox"/>	
PHP support	<input checked="" type="checkbox"/>	
CGI support	<input checked="" type="checkbox"/>	
mod_perl support	<input checked="" type="checkbox"/>	
mod_python support	<input checked="" type="checkbox"/>	

* Required fields

- Specify the name of the new web user, enter and confirm the password for web user, specify the hard disk quota, and select the available scripting options for the given domain (if enabled in Preferences).

i NOTE

Each web user creates a system account within web server; therefore, you cannot have two web users with identical names on the same server.

You cannot use the reserved system words, such as "mailman" for user names.

i NOTE

Do not use quotes, space and national alphabet characters in the password. The password length should be between 5 and 14 characters and password must not be the same as the login name.

- Once you have completed all entries click OK.

As you create web users, the user names appear listed on the Web Users page.

i NOTE

New web users can access the directory using FTP software by entering the domain name under which the web user account was created and using the appropriate web user name and password.


Editing the web user account properties

To change web user passwords or edit scripting options, click on the user name in the web user list. This takes you to the Web User Configuration page. Follow the same procedure as described above.

Deleting a web user account

To delete existing web users select the users that you wish to delete using the checkboxes, and click Remove Selected. You will be asked for confirmation prior to deleting the selected web users.

Managing Subdomains


You can create and manage subdomains from the control panel. Access the subdomains management functions, selecting the  Subdomains icon on

the Domain Administration page. The subdomains management page opens, listing the subdomains existing under the domain and corresponding FTP account names used for managing them:

[Clients](#) > [Alec](#) > [domain.com](#) >

Subdomains of domain domain.com [Up Level](#)

Tools

 [Add New Subdomain](#)


Subdomains

Subdomains (1)

[Search](#) [Show All](#) [Remove Selected](#)

Subdomain name ▲	Login	
dominio.domain.com	ftlogin	<input type="checkbox"/>

To create a subdomain, follow these steps:

1. Click  Add New Subdomain. The Subdomain creation page will open:

Clients > Alec > domain.com > Subdomains >

Create a subdomain domain.com Up Level

Subdomain

Subdomain .domain.com

FTP user Use the same FTP user as that of the main domain
 Create a separate FTP user account for this subdomain

Old password None

FTP Login *

Password

Confirm Password

Hard disk quota MB Unlimited

Apache ASP support

SSI support

PHP support

CGI support


mod_perl support

mod_python support

ColdFusion support

* Required fields

2. Enter the subdomain name in the appropriate field.
3. Select the FTP account user the subdomain is created for: the owner of a parent domain or another individual.
4. Define FTP login, password, and specify hard disk quota if needed.
5. Enable required scripting capabilities to be supported on the subdomain.
6. Click OK.

To open the subdomain URL in browser, click 

To edit hosting account of a subdomain, select the required subdomain name in the list.

To remove one or several subdomains, select them using the corresponding checkboxes, and click Remove Selected.

Managing Protected Directories

This feature is active if virtual hosting has been configured for the domain. It creates and provides password-protected access to the directories where the secure documents reside in the virtual domain. It is possible to create directories under either the standard virtual host accessible via http protocol, or if applicable for the given domain, under the SSL virtual host accessible via https protocol.


To access the protected directories management functions, use the 

Directories icon on the Domain Administration page. The page will open listing all protected directories of this domain:

Clients > Alec > domain.com >

Protected directories for domain domain.com [Up Level](#)



Tools



 [Add New Directory](#)

Protected directories

Protected directories (1)

[Search](#) [Show All](#) [Remove Selected](#)

S	N	Name	
		  /directory1	<input type="checkbox"/>


Each directory name is accompanied by icons, identifying which virtual host type (SSL or non-SSL) the directory resides within:  depicts non-SSL;  depicts SSL.

NOTE

We strongly recommend that you create and change the protected directories through Plesk and not within the FTP program. Plesk may not recognize manual changes.

Creating a protected directory

Follow these steps to create secure directories for the domain:

1. Click  Add New Directory. This takes you to the Protected Directory

Creation page:

Clients > Alec > domain.com > Protected directories >

Create new protected directory on domain domain.com [Up Level](#)

Preferences

Directory name

Directory location Non-SSL SSL

Header Text

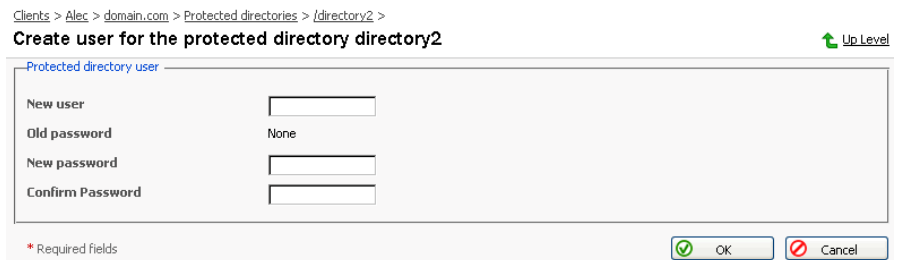
* Required fields

2. Enter the name of the protected directory you wish to create in the Directory name field.
3. For Directory Location you can choose a non-SSL, SSL secure directory, or both. Use the appropriate checkboxes to select.
4. Click in the Header Text input box, and enter the header for this directory. When a user tries to access the protected directory, the text in this box displays as the realm they are entering.

- Click OK to complete creation. You will be taken to the list of protected directory users:



- To add a new user, click the  Add New User icon. You are taken to the new directory user creation page:



- Specify the user name, password and confirm password.
- Click OK to submit. You will return to the Protected Directory Management page. The new user record will appear in the list of users.
- To remove existing directory users select the users that you wish to remove using the corresponding checkboxes and click Remove Selected. You will be asked for confirmation prior to deletion of the directory users.
- To access a directory user record in order to edit the user password, click on the user name in the list.
- Once you have completed everything within your new protected directory, click OK to submit all changes to the system and to return to the Protected Directory page.

i NOTE

An SSL protected directory can be created even if SSL support has been disabled for the domain, however this protected directory will be inaccessible until you enable the SSL support.

Editing the protected directory properties

Follow these steps to edit protected directory properties:

1. On the Protected directories page, click on a title of the directory that you wish to edit. You will be taken to the Protected Directory Management page.
2. Edit the directory properties by following the same steps outlined above, in the Creating a protected directory section.
3. Click OK to submit all changes to the system and to return to the Protected Directories page.

Removing a Protected Directory

To remove one or more directories, follow these steps:

1. Select the checkboxes in the list of protected directories.
2. Click Remove Selected. The Protected Directory Removal page appears.
3. Confirm removal, and click OK.

NOTE

Removing a protected directory in Plesk does not delete the directory off the server, it simply removes the protection. Meaning that the directory and its contents will now be reachable via the Internet without the need for login and password.



Managing Anonymous FTP Access

Within Plesk the Administrator, or Client given domain creation capabilities, can set up Anonymous FTP capabilities for a given virtual host. Anonymous FTP is used to allow an open, yet controlled, environment for visitors to the domain to download and/or upload files to and from the domain account. Users will be able to log into ftp.'domain name' with the standard anonymous user name and any password. Plesk allows the setup and limitation of incoming file space, number of connected users, and bandwidth usage throttling. Administrators should take care when allowing the use of anonymous FTP and be sure to use all the limitation capabilities within the interface wisely. If set up with excessive limits, it could lead to problems with server resources as well as excessive bandwidth usage.


NOTE

You can set up anonymous FTP only for domains that have physical hosting configured on exclusive IP.

To set up Anonymous FTP:

1. Click the  Anonymous FTP icon on the Domain Administration page. The Anonymous FTP Account Management page will appear.
2. By default anonymous FTP capabilities are disabled. To activate anonymous FTP select the  Enable icon.
3. 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.
4. Select the checkbox beside Allow uploading to incoming directory to allow visitors to access the anonymous FTP site to upload files into the /incoming directory.
5. To allow users to create nested directories in the /incoming directory, select the Allow creation of directories in the incoming directory checkbox.
6. To allow downloading from the /incoming directory, select the Allow downloading from the incoming directory checkbox.
7. Deselect the Unlimited checkbox in the Limit disk space in the incoming directory field to set the disk space quota (i.e. hard limit) on the /incoming directory. Then enter the amount of disk space, in Kilobytes, you wish to allow for the /incoming directory.
8. Deselect the Unlimited checkbox in the Limit number of simultaneous connections field to set limits on the number of users who can be simultaneously connected to the anonymous FTP site. Then enter the number of connections allowed.
9. Deselect the Unlimited checkbox in the Limit download bandwidth for this virtual FTP domain field to set throttling up for the anonymous FTP site. Then enter the maximum average bandwidth, in Kilobytes per second, allowed.
10. Once you have completed all changes, click OK to submit.

Managing Log Files and Log Rotation


Plesk allows managing log files and log rotation settings from the control panel. To access these functions, click the  Log Manager icon on the Domain

Administration page. The Log Manager page will open:

Clients > Alec > domain.com >

Log files management for domain domain.com [Up Level](#)

Tools

 Log Rotation

Preferences

Lines of log file to be displayed (from the end of the file)


Log files

Log files (6) [Search](#) [Show All](#) [Remove Selected](#)

Modification date	Name ▲	Size	<input type="checkbox"/>
Jan 30, 2004 04:07 AM	access_log	0 B	<input type="checkbox"/>
Jan 30, 2004 04:07 AM	access_log.processed	294 B	<input type="checkbox"/>
Jan 30, 2004 04:07 AM	access_ssl_log	0 B	<input type="checkbox"/>
Jan 29, 2004 04:07 AM	access_ssl_log.processed	0 B	<input type="checkbox"/>
Jan 29, 2004 07:46 AM	error_log	1.08 KB	<input type="checkbox"/>
Jan 30, 2004 05:03 AM	error_ssl_log	4.10 KB	<input type="checkbox"/>

Log files total size: 5.47 KB

At this page, you can perform the following operations:

- Define the number of log file's lines to be displayed at once. To do that, type in the number of lines in the Lines of log file to be displayed input field prior to selecting a log file for viewing.
- View a log file. To this effect, click on a log file's name in the list. The log file contents will be displayed in a separate Log File Viewer window.
- Save a log file on your local machine. To do that, click on the appropriate  icon. After that you will need to specify the location on your local machine and the file name for the downloaded log file to be saved, and then click Save.
- Delete log files. To this effect, select the corresponding checkboxes, and click Remove Selected.

To configure the log rotation preferences, follow these steps:


1. Click the  Log Rotation icon on the Log Files Management page.

The Log Rotation Preferences page will open:

Clients > Alec > domain.com > Log files >

Log rotation preferences for domain domain.com Up Level

Tools

 Enable

Preferences



Log rotation condition * by size KB
 by time Daily

Maximum number of log files

Compress log files

Send processed log files to e-mail

* Required fields

2. Click the  Enable or  Disable icon respectively to enable/disable log rotation.
3. Select the log rotation condition:
 - log file size - enter the size in kilobytes in the appropriate field
 - time - select from the drop-down list. It can be set to **Daily**, **Weekly**, and **Monthly**.
4. Specify the maximum number of log files in the appropriate input field, if desired. The maximum number is the number of processed files to be kept for each log file.
5. Select the Compress log files checkbox to enable compression.
6. If desired, in the Send processed log files to e-mail input field, enter the e-mail address, for the processed log files to be delivered to.
7. Click OK to submit changes.

Using File Manager

Once you have configured hosting for a domain, you can use a file manager to operate domain files and directories.

To access the file manager functions, click the  File Manager icon on the

Domain Administration page. The file manager page will open displaying a root directory structure and contents:










File Manager

[Up Level](#)

root (12)

Search Show All Create file Create directory Copy/Move Touch Remove Selected


T	Name ▲	Size	Change date	User	Group	Permissions	
	anon_ftp	4.00 KB	Jan 28, 2004	ftplugin	psaserv	750	
	bin	4.00 KB	Jan 28, 2004	root	psaserv	755	
	cgi-bin	4.00 KB	Jan 28, 2004	ftplugin	psach	755	
	conf	4.00 KB	Jan 30, 2004	root	psaserv	750	
	error_docs	4.00 KB	Jan 28, 2004	ftplugin	psaserv	755	
	httpdocs	4.00 KB	Jan 30, 2004	ftplugin	psach	751	
	httpsdocs	4.00 KB	Jan 30, 2004	ftplugin	psach	751	
	pd	4.00 KB	Jan 30, 2004	root	psaserv	750	
	private	4.00 KB	Jan 28, 2004	ftplugin	root	700	
	statistics	4.00 KB	Jan 28, 2004	root	psaserv	550	
	subdomains	4.00 KB	Jan 30, 2004	root	psaserv	755	
	web_users	4.00 KB	Jan 29, 2004	root	psaserv	755	


- To browse a directory, click the  icon or directory name.
- To change permissions for a directory or a file: click on the corresponding permission set in the Permissions column. The permissions settings page will open, allowing you to set the required permissions for all users. Select the desired settings using the checkboxes, then click OK to submit.
- To rename a directory or file, click on the corresponding  icon. A new page will open allowing you to rename the selected file or directory. Type in a new name and click OK.
- To copy or move a file or directory to another location, select the required file or directory using the corresponding checkbox, and click  Copy/Move. You will then need to specify the destination for the file or directory to be copied or renamed to. Then click Copy to copy, or Move to move it.
- To change a timestamp of a directory or file, click on the  Touch icon. The time stamp will be updated with the current local time.
- To remove a file or directory, select the corresponding checkbox, and click Remove Selected.
- To upload a file to the current directory, click  Create File, then specify its location. Click OK.
- To create a file, click  Create File, then type in a file name in the corresponding field, check (uncheck) the "html template" box, and click OK.
- To create a subdirectory that will be nested in the current directory, click  Create Directory, then type in the directory name in the Directory name field, and click OK.
- To edit a file, click the corresponding  icon. The File Manager's editor window will open, allowing you to edit the file source. After you are done with editing, click Save to save the file, Save and Exit to save the file and quit the file editing mode, Cancel to cancel editing mode and return to the FileManager panel, or Reset to discard the alterations made.
- To edit a file in the WYSIWYG editor, click the corresponding  icon.




Using the Domain Application Vault

The domain application vault function enables you to install various applications on domain and view the properties of the already installed applications.



Installing application on domain


1. Select a domain with configured physical hosting and click the  Application Vault icon on the Domain Administration page.


2. Click the  Add Application icon. The application installation wizard will open, displaying the available application packages and their properties. The icons in the first left column indicate the type of the site application:

-  - the free site application requiring no license key, included in the default installation of Plesk for free, automatically added to the application pool of each client registered in the control panel.
-  - the commercial site application requiring a license key, obtained at SWsoft company additionally.
-  - the commercial site application requiring a license key, obtained at SWsoft company additionally, with no key installed at the moment.

The icons in the second column left to the site application name indicate the site application usage rules defined by the administrator:

-  - free of charge, automatically added to the application pools of all clients;
 -  - commercial, added to a client application pool only by the administrator under certain conditions.
3. Select the application package you wish to install on the selected domain. Note: you can also choose to install it on a subdomain – select it in the Target domain drop-down menu.

You can view information on available application packages by clicking on the application package name in the list. If there is a documentation available for the application, it will be accessible through the icon .


4. Click  Install.
5. Some applications require that certain parameters be entered before executing the installation. The required parameters are marked with an asterisk.


You have an option of creating a custom button for accessing this application. The button can be placed on the administration page of a given domain, on the administration pages of all domains, belonging to this client, or all domains hosted on server.

6. Click OK once you are done editing the required parameters. If you chose to create a custom button for the application, you will be taken to the custom button properties page.

Note: It is not allowed to install one application into a sub-directory of another application. However, most applications allow installing several copies for the same domain but in different directories.


When the installation of the application is complete, the application will appear on the Applications list.

To edit the parameters of an application, click on the corresponding icon .

Use the  icon in the Applications list to access the URL of the application.

To remove one or several applications, in the list of applications select the corresponding checkboxes and click Remove Selected.

Accessing Site Builder

Plesk is shipped with Mambo site builder software intended to simplify the process of creating and deploying web sites. In order to use the site builder, you need to have the PHP support enabled for the domain set-up on physical hosting. You can set it up to work via HTTP or HTTPS protocol. The application can be installed on the domain and configured either via Domain Application Vault or using the installation procedure invoked when you click on the Site Builder icon for the first time. After the application is installed and configured, use the  Site Builder icon on the Domain administration page to access

it.

Accessing Microsoft FrontPage Web Administrator


You can access the Microsoft FrontPage Web Administrator directly from the

Control Panel, using the  FP Webadmin icon, or  FP-SSL

Webadmin if you wish to access it over secure SSL connection. These icons are located at the bottom of the Domain Administration page, provided that hosting is set up for the domain, and Microsoft FrontPage is available. Note, that the FrontPage Web Admin software should be installed and configured properly for this function to work, and the FrontPage and FrontPage over SSL support should be enabled within Plesk.

Backing Up and Restoring Domains

You can back up and restore domain data by the control panel means, provided that the backup utilities are installed on your server, and the backup/restore functions are supported by the product license key.

To access the backup/restore functions, on the Domain administration page of the selected domain, click the  Backup icon. The Backup files repository

page opens displaying the stored domain backup files and their properties.

To be able to use a directory on your FTP server as an integral part of backup files repository, you need to specify the FTP connection properties in the control panel. To do this, follow these steps:

1. Click the FTP Account Properties icon.
2. Enter the FTP server name in the FTP server text input field.
3. Type the name of the FTP server directory where the domain backups are stored in the Base directory on FTP server text input field.
4. Enter the FTP server login in the FTP Login text input field.
5. Enter and confirm the FTP password.
6. Click OK to submit.

To schedule automated backing up, follow these steps:

1. Click the Scheduled Backup Settings icon.
2. Select the period of backups creation - should they be created daily, weekly or monthly,
3. Select the location where the backup files should be placed,
4. Specify the maximum number of backup files that can be stored in the selected location,

Note: When the specified number is exceeded, the oldest backups are removed from the repository.

5. Enter the name the backup files should begin with,
6. Click OK to submit.

To view the properties of backed up domain click the backup file's name.

To save a backup file on your local machine, click the corresponding  icon.

After that you will need to specify the location on your machine and the file name for the downloaded backup file to be saved, and then click Save.

To delete one or several backup files from the repository, select the corresponding checkboxes and click Remove Selected.

To upload a backup file to the server, specify file location using the Browse button, then click Upload.

To upload a backup file from the remote FTP server to the Plesk server, click the FTP Upload icon. You will be taken to the FTP server directory where you can select which files you want to upload to your Plesk server.

Note: To be able to use this option, you should first specify the FTP connection properties in the control panel.

To back up the domain data, follow these steps:

1. Click the  Create Backup icon on the Backup files repository page.

The Backup file creation page appears.

2. Specify the backup file name.

Select the create backup file and store in repository option, and type in your comments in the Comments text field.


To download a backup file to your local machine without storing it in the backup repository, select the "do not store the backup file in repository, only download it" option.

To create the backup file and store it on FTP server, select the corresponding option.

If you wish Plesk to notify you of the backup progress, enter your e-mail into the "Notify by e-mail" field, and select the checkbox for activating this function.

3. Click Back Up.

To restore a domain, follow these steps:

1. Click the  Backup icon at the Domain administration page. The Backup files repository page appears.
2. Select the desired backup file from the list clicking on its file name. The backup file information page will open displaying the domain configuration to be restored.
3. If desired, enter an e-mail and select the checkbox to enable the notification.

Select the IP address to be used for restoring the domain data.
4. Click Restore.


NOTE

During backup/restore processes, the domain is automatically switched off and all of its services are unavailable.


Deactivating/Activating a Domain

You can disable the domain operations by deactivating it. When a domain is deactivated, it cannot be accessed.

To deactivate a domain:

1. On the Domain administration page of the selected domain, click  Disable. The confirmation will appear querying whether you actually wish to change the status of the selected domain.
2. Click OK.


To activate a domain, follow these steps:

1. On the Domain administration page of the selected domain, whose operation is disabled, click  Enable. The confirmation will appear querying whether you actually wish to change the status of the selected domain.
2. Click OK.

i NOTE

When a domain is deactivated, the domain status icon will change to



When a domain is activated, the domain status icon will change to 

















Performing Group Operations on Domains


In cases when you need to introduce certain similar changes to several domains, you can use the Group Operations function, made available to simplify administration of multiple domains. Using this feature you can, for instance, select a number of domains, enable all of them to support SSL and limit the total amount of available traffic to a specific figure - all that within a single operation, without having to select each domain independently and edit its settings.

To perform group operations on domains, follow these steps:

1. Select the Domains shortcut in the navigation pane. The page will open displaying the list of registered domains:

Domains

Tools								
								
Add New Domain	Domain Templates	Summary Report	Traffic					
Domains								
Domains (3)								
<input type="text"/>		Search	Show All	Show Subdomains	Group Operations	Remove Selected		
P	S	H	Domain name	Creation date ▲	Subdomains	Disk usage	Traffic	<input type="checkbox"/>
			chappa2.vrh62.plesk.ru	Nov 9, 2003	1	13.9 MB 0.65 MB/Month		<input type="checkbox"/>
			domain.com	Nov 9, 2003	0	0.00 MB 0.00 MB/Month		<input type="checkbox"/>
			quick.vrh62.plesk.ru	Nov 9, 2003	0	4.23 MB 0.49 MB/Month		<input type="checkbox"/>

2. Select the domains, whose settings or limits you wish to modify by checking the corresponding checkboxes.
3. Click the  Group Operations icon. The Group Operations page will appear, divided into five sections:
 - The Limits group is used for modifying the limits for various resources
 - The Hosting group is used for editing various hosting-related settings
 - The Preferences group contains miscellaneous editable options for domains
 - The Services group is used for enabling/disabling the use of domain services
 - The Modified domains area lists the domains, whose settings you are

going to modify.

4. To edit limit settings for a particular resource type:
 - 4.1. First, select the appropriate action from the drop-down box:
 - Leave the **Do not change** option selected, if you do not wish to make any changes
 - Select **unlimited**, if you wish not to limit the resource usage
 - Select the **value** option in order to specify a new value for the resource limit
 - Select **Increase (+)**, to specify the value by which to increment the presently set resource limit value
 - Select **Decrease (-)**, to specify the value by which to decrement the presently set resource limit value
 - 4.2. Then specify the value of the new resource limit in the corresponding input field.
 - 4.3. If you chose to increase/decrease the presently set limit value, use the drop-down box to select **units** if you wish to modify the limit value by a quantity of commonly used units or **%** if you wish to modify the limit value by a particular percentage.
5. To change the hosting-related settings, select **Do not change**, **Enable** or **Disable** radio button for the corresponding type of setting. You can manage the following:
 - SSL support
 - Web statistics
 - Password protection of access to Web statistics
 - Custom Error Documents
 - Apache ASP support
 - SSI support
 - PHP support
 - CGI support
 - mod_perl support
 - mod_python support
 - ColdFusion support

You can also choose to manage (or not) log rotation. Here you can:

- Activate/deactivate log rotation
- Choose the condition of rotating the log files: **by size** - specify the maximum size of the log files, or **by time** - select **Daily**, **Weekly** or **Monthly**.
- Choose the maximum number of log file instances allowed
- Choose whether to use the log files compression or not
- Choose whether to send the log files to a specific e-mail

i NOTE

It is advisable to set the log rotation options for all domains appropriately in order to prevent the log files from growing too large to be handled by the statistics utility.

6. To change preferences, select **Do not change**, **Enable** or **Disable** radio button for the corresponding item. You can edit the following:
 - WWW prefix requirement
 - Web Mail
 - Support for web users' scripting
 - Traffic statistics retention settings
 - Mail to nonexistent user; if enabled, you can choose to either **Bounce with phrase** or **Catch to address**.
7. To enable/disable services, select **Do not change**, **Enable** or **Disable** radio button for the corresponding service. You can edit the following:
 - DNS Zone
 - Mail
 - Mailing lists
 - Tomcat
 - Anonymous FTP
8. Click OK to apply the new settings to the selected domains.

Removing Domains

You can remove one or several domains at the same time. To remove domains:

1. Select the Domains shortcut in the navigation pane. The page will open displaying the list of registered domains:

Domains

Tools

[Add New Domain](#) [Domain Templates](#) [Summary Report](#) [Traffic](#)

Domains (3)

Search [Show All](#) [Show Subdomains](#) [Group Operations](#) [Remove Selected](#)

P	S	H	Domain name	Creation date	Subdomains	Disk usage	Traffic	
✓	✓	✓	chappa2.vrb62.plesk.ru	Nov 9, 2003	1	13.9 MB 0.65 MB/Month	→	<input type="checkbox"/>
✓	✓	✓	domain.com	Nov 9, 2003	0	0.00 MB 0.00 MB/Month	→	<input type="checkbox"/>
✓	✓	✓	quick.vrb62.plesk.ru	Nov 9, 2003	0	4.23 MB 0.49 MB/Month	→	<input type="checkbox"/>

2. Select the domains that you wish to remove by checking the corresponding checkboxes.
3. Click Remove Selected. The Removal confirmation page appears:

Removal confirmation [Up Level](#)

[Remove](#)

The following domains will be removed:

- domain.com

Confirm removal.

* Required fields

4. Select the checkbox to confirm removing, and click OK. If you decide to not delete these domains or wish to modify the list of domains selected for deletion, click Cancel.

Chapter 6. Using Plesk Migration Manager

This chapter provides you information on how to migrate from competitive control panels to Plesk control panel.

Overview

Plesk Migration Manager is created for easy and fast migration from other, competitive control panels to Plesk, and also for migration from older releases of Plesk and from different platforms of Plesk. At the present moment you can migrate the following platforms to Plesk:

- Confixx2;
- older releases of Plesk and other platforms of Plesk - FreeBSD or Linux;
- Cobalt Raq;
- cPanel 9.

The Plesk Migration Manager can be accessed by selecting the Server shortcut and clicking the Migration Manager icon on the Server administration page. The Migration Agent Upload page will open. The Migration Manager will guide you through the migration process.

Note: The Migration Manager icon will be disabled, if this feature is not supported by your license key.

Uploading Migration Agent To Remote Host

First, you need to upload the migration agent to the remote host you wish to migrate to Plesk. This can be done on the Migration Agent Upload page. On this page, please, specify the remote control panel parameters:

- select the platform from which you would like to migrate to Plesk from the Source Platform drop-down box.
- specify the source host. You can use either the IP address or the domain name of the server you wish to migrate.
- enter the login. You need to log in as "root".
- enter the password, used for logging in to the remote host you are

migrating.

- click Next.

The agent will upload to the specified remote host and acquire its status. You will proceed to the progress page where you can view the migration progress and to stop it.

Viewing Information on Source Host

When the migration agent uploads to the remote host, it sends information on this host to your Plesk control panel. This information is displayed on the Information on source host page. On this page, please, select the option you need:

- clear the Select objects for migration checkbox, if you wish to migrate all objects from the remote host to Plesk.
- select the Select objects for migration checkbox, if you wish to select certain objects to be migrated from the remote host to Plesk.
- click Cancel to cancel the migration.

Migrating All Objects

After you cleared the Select objects for migration checkbox, you will proceed to the Downloading remote host content page, where you can view and stop the downloading if desired.

Once the downloading is complete, you will be taken to the IP Mapping page.

IP Mapping

The IP Mapping page displays all IP addresses of the host you are migrating to Plesk and all IP addresses of Plesk you are migrating this host to.

On this page,

- select the Plesk IP address you want to map the remote host IP addresses to.

Note: You can map all IP addresses of the remote host only to one Plesk IP address.

- click Migrate to continue migration or Cancel to cancel the migration.

Viewing Migration Result

When the remote host objects are migrated, you will proceed to the Migration Result page where you can view the migration result. This can be either the message on the successful migration or error messages, if any errors occurred during the migration process, and the list of objects that could not be migrated due to the errors occurred.

Click Finish to finish the migration.

Selecting Objects For Migration

After you selected the Select objects for migration checkbox, you will proceed to the Migration Progress page, where you can view migration progress and stop the migration if desired.

After that you will be taken to the Select objects for migration page. On this page, select which objects you wish to be migrated to Plesk:

- select the Accounts tab and specify which accounts should be migrated by clicking the corresponding checkboxes, then click Migrate.
- select the Domains tab and specify which domains should be migrated by clicking the corresponding checkboxes, then click Migrate.
- click Cancel to cancel migration.

Migrating Accounts

After you chose accounts for migration, you will proceed to the Downloading remote host content page, where you can view and stop the downloading if desired.

Once the downloading is complete, you will be taken to the IP Mapping page.

Migrating Domains

After you chose domains for migration, you will be taken to the Select client account for domains migration page.

On this page,

- select the Plesk client account on which you wish to migrate the selected domains of the remote host.
- click Migrate to continue migration or Cancel to cancel the migration.

If you decided to continue migration, you will be taken to the IP Mapping page.

IP Mapping

The IP Mapping page displays all IP addresses of the host you are migrating to Plesk and all IP addresses of Plesk you are migrating this host to.

On this page,

- select the Plesk IP address you want to map the remote host IP addresses to.

Note: You can map all IP addresses of the remote host only to one Plesk IP address.

- click Migrate to continue migration or Cancel to cancel the migration.

Viewing Migration Result

When the remote host objects are migrated, you will proceed to the Migration Result page where you can view the migration result. This can be either the message on the successful migration or error messages, if any errors occurred during the migration process, and the list of objects that could not be migrated due to the errors occurred.

Click Finish to finish the migration.

Stopping Migration

You can stop migration by clicking Cancel on the Migration Progress, Downloading remote host content or IP Mapping pages. This will take you to the Stop migration process page.

To stop the migration, you need to remove the migration agent from the remote host. Thus, on the Stop migration process page, select the Remove agent checkbox and click OK. You will get back to the Migration Agent Upload page.

If you do not select this checkbox, the migration will not stop and you will return to the previous page.

Appendix A. Plesk Advanced Features

In addition to operations available via control panel, the Plesk software provides several advanced management capabilities, available to the administrator from the command line. The administrator can:

- Use the Creation Utilities for creating and managing client accounts, domains, hosting accounts, various settings and services,
- Include domain-specific Apache configuration directives into `httpd.include` for domains,
- Install the Sun Chili!Soft ASP support and configure it for working with Plesk,
- Use the global access control list in `named.conf` for allowing dns transfers,
- Configure the ports to be used by Tomcat connectors,
- Restore the mail configuration by Plesk database.

Creation Utilities

The creation utilities allow to create and manage client accounts, domains, hosting accounts, and manage domain preferences and services from the command line.

To manage client accounts, use the `client.sh` utility located in `/usr/local/psa/bin/`. The following commands and options can be used:

Table A.1.

Command	Parameter	Action
<code>--create</code> or <code>-c</code>	<login_name>	creates a new client account
<code>--update</code> or <code>-u</code>	<login_name>	updates client account
<code>--remove</code> or <code>-r</code>	<login_name>	removes client account
<code>--info</code> or <code>-i</code>	<login_name>	retrieves client information
<code>--on</code>	<login_name>	enables client account
<code>--off</code>	<login_name>	disables client account
<code>--help</code> or <code>-h</code>		displays the help on utility usage
Option	Parameter	Note
<code>-status</code>	<true false>	enables/disables client account (default: true)

Command	Parameter	Action
-company	<string>	company name
-name	<string>	contact name (required for creation)
-login	<login_name>	control panel login name (may be used only with update command)
-passwd	<passwd>	control panel password (required for creation)
-phone	<number>	phone number
-fax	<number>	fax
-email	<string>	e-mail address
-addr	<string>	street
-city	<string>	city
-state	<string>	state/province
-pcode	<string>	postal/zip code
-country	<string>	country
-notify	<true false>	enables/disables notifying of client account creation

To edit client accounts, use the `client_pref.sh` utility located in `/usr/local/psa/bin/`. The following commands and options can be used:

Table A.2.

Command	Parameter	Action
--update or -u	login_name	updates an existing client account
--info or -i	login_name	retrieves client information
--help or -h		displays the help on utility usage
Option	Parameter	Note
-create_domains	<true false>	allows client to create domains

Command	Parameter	Action
-manage_phosting	<true false>	allows managing physical hosting
-change_limits	<true false>	allows changing domain limits
-manage_dns	<true false>	allows managing DNS
-manage_log	<true false>	allows managing log rotation
-manage_crontab	<true false>	allows managing Crontab (Scheduler)
-manage_anonftp	<true false>	allows managing Anonymous FTP
-manage_webapps	<true false>	allows managing Tomcat web applications
-manage_maillists	<true false>	allows managing mailing lists
-manage_sh_access	<true false>	allows managing system access
-manage_subdomains	<true false>	allows managing subdomains
-manage_quota	<true false>	allows changing hard disk quota
-make_dumps	<true false>	allows the use of backup/restore functions
-max_dom	<number>	limits number of available domains (-1 is unlimited)
-disk_space	<number>	limits amount of available disk space to the specified value (in Megabytes)
-max_traffic	<number>	limits the amount of available traffic to the specified value (in Megabytes)
-max_box	<number>	limits the allowed number of mailboxes to the specified value
-mbox_quota	<number>	limits the mailbox quota to the specified size (in Kilobytes)
-max_redir	<number>	limits the number of mail redirects
-max_mg	<number>	limits the number of mail groups

Command	Parameter	Action
-max_resp	<number>	limits the number of mail autoresponders
-max_wu	<number>	limits the number of web users
-max_db	<number>	limits the number of databases
-max_maillists	<number>	limits the number of mailing lists
-max_webapps	<number>	limits the number of Tomcat web applications allowed
-max_subdom	<number>	limits the number of subdomains
-expiration	<date>	limits the validity period of client account
-ip_pool	<add del>:<ip1>,<ip2>,...,<ipN>	adds/deletes ip addresses to/from client's IP pool.

i NOTE

The <number> tag means any positive (or zero) integer value. The <date> tag implies date in the following format: 'YYYY-MM-DD'.

You may use the '-1' value for "unlimited" when defining any limit applicable to a client account.

You may specify any number of -ip_pool options to achieve the desired results, for example: `client_pref.sh -u 'c1' -ip_pool add:127.0.0.1,127.0.0.2 -ip_pool del:127.0.0.3`

To manage domains, use the domain.sh utility located in `/usr/local/psa/bin/`. The following commands and options can be used:

Table A.3.

Command	Parameter	Action
--create or -c	<domain_name>	creates a new domain
--update or -u	<domain_name>	updates an existing domain
--remove or -r	<domain_name>	removes an existing domain
--info or -i	<domain_name>	retrieves domain information

Command	Parameter	Action
--on	<domain_name>	enables domain
--off	<domain_name>	disables domain
--shells or -s		lists available shells
--help or -h		displays help on utility usage
Option	Parameter	Note
-status	<true false>	turns domain on/off (default: true)
-dom_user	<true false>	turns the domain level user account on/off (default: false)
-du_passwd	<passwd>	sets up password for domain level user
-dns	<true false>	turns DNS zone for the domain on/off (by default DNS template status)
-www	<true false>	adds www prefix (default: true)
-hosting	<true false>	enables/disables hosting for the domain (default: false)
-hst_type	<phys std frm>	sets up the specified hosting type (default: physical)
-target_url	<URL>	sets up target URL (required if hst_type is "std" or "frm")
-ip	<ip_address>	ip address
-login	<login>	FTP user login name (required if hosting is physical)
-passwd_type	<plain crypt>	FTP user password type (default: plain)
-passwd	<password>	FTP password (no password is set by default)
-shell	<shell_name help>	system shell (you can use the --shells command to list available shells)
-hard_quota	<MB>	hard disk quota (0 is unlimited)

Command	Parameter	Action
-fp	<true false>	turns on/off FrontPage support on domain (default: false)
-fp_ssl	<true false>	turns on/off frontpage over ssl support on domain (default: false)
-fpauth	<true false>	FrontPage authoring (default: false)
-fplogin	<login>	FrontPage login name
-fppasswd	<password>	FrontPage password
-ssi	<true false>	SSI support on domain (default: false)
-php	<true false>	PHP support on domain (default: false)
-cgi	<true false>	CGI support on domain (default: false)
-perl	<true false>	Perl support on domain (default: false)
-asp	<true false>	ASP support on domain (default: false)
-python	<true false>	Python support on domain (default: false)
-coldfusion	<true false>	ColdFusion support on domain (default: false)
-ssl	<true false>	SSL support on domain (default: false)
-webstat	<true false>	Webalizer support on domain (default: false)
-err_docs	<true false>	custom error documents support on domain (default: false)
-log_rotate	<true false>	log rotation status (default: true)
-log_bysize	<KB>	enables log rotation by size
-log_bytime	<daily weekly monthly>	enables log rotation by time (default: daily)

Command	Parameter	Action
-log_max_num	<number>	defines maximum number of log file instances (default: 3)
-log_compress	<true false>	enables log files compression (default: true)
-log_email	<email>	enables sending log files to e-mail
-clogin	<login>	login of existing client the domain will belong to (required for domain creation)
-mail_service	<true false>	turns on/off the mail service for the domain (default: true)
-notify	<true false>	enables disables notifying of domain creation

To manage domain level preferences, use the domain_pref.sh utility located in `/usr/local/psa/bin/`. The following commands and options can be used:

Table A.4.

Command	Parameter	Action
--update or -u	domain_name	sets domain preferences
--info or -i	domain_name	retrieves domain preferences information
--help or -h		displays the help on utility usage
Option	Parameter	Note
-disk_space	<MB>	limits amount of available disk space
-max_traffic	<MB/Month>	limits the amount of traffic for a domain
-max_box	<number>	limits number of mailboxes
-mbox_quota	<KB>	limits mailbox quota
-max_redir	<number>	limits the number of mail redirects

Command	Parameter	Action
-max_mg	<number>	limits number of mail groups
-max_resp	<number>	limits the number of mail autoresponders
-max_wu	<number>	limits the number of web users
-max_db	<number>	limits the number of databases
-max_maillists	<number>	limits the number of mailing lists
-max_webapps	<number>	limits the number of allowed web applications
-max_subdom	<number>	limits the number of subdomains
-expiration	<YYYY-MM-DD>	limits a validity period for the domain
-www	<true false>	www prefix for the domain
-wuscripts	<true false>	enables web users' scripting support
-webmail	<true false>	allows use of webmail
-no_usr	<bounce:txt email>	sets up bounce or catch-all for nonexisting user mail (obsolete and will be removed from future releases)
-keep_traf_stat	<number>	sets the system to retain traffic statistics for N months (specify 0 if you wish not to delete statistics)

To manage mail accounts, use the mail.sh utility located in `/usr/local/psa/bin`. The following commands and options can be used:

Table A.5.

Command	Parameter	Action
--create or -c	<mail_name>@<domain>	creates mail account
--update or -u	<mail_name>@<domain>	updates mail account parameters
--remove or -r	<mail_name>@<domain>	removes mail account

Command	Parameter	Action
--on	<domain>	enables mail service for domain
--off	<domain>	disables mail service for domain
--info or -i	<mail_name>@<domain>	retrieves mail account information
--help or -h		displays help on utility usage
Option	Parameter	Note
-cp_access	<true false>	enables control panel access
-mailbox	<true false>	creates/removes mailbox
-passwd	<passwd>	sets mailbox password
-boxpass	<passwd>	obsolete alias for option "passwd" (this option may be removed from future releases)
-passwd_type	<plain crypt>	specifies the type of mailbox password, ignored if no password specified
-mbox_quota	<KB>	limits the mailbox quota to the desired amount
-aliases	<add del>:<name1[,name2]>	Adds or deletes mail alias(es) to/from mail name
-mgroups	<add del>:<list1[,list2]>	adds or removes mail name to/from mail group
-redirect	<true false>	switches mail redirect on/off
-rediraddr	<addr>	sets redirect to address (required if redirect is enabled)
-group	<true false>	switches mail group on/off
-groupmem	<add del>:<addr1[,addr2]>	adds/removes address(-es) to/from mail group
-repo	<add del>:<file1[,file2]>	adds/removes file to/from attachments repository
-autorsp	<true false>	switches all autoresponders on/off

Command	Parameter	Action
-autoname	<name>	autoresponder name (required for all autoresponder options)
-autostatus	<true false>	switches on/off autoresponder with specified name
-autoreq	<subj body>:<string> or <always>	defines the condition for the autoresponder to be activated whether the specified pattern is encountered in the subject or body, or to respond always.
-autosubj	<original string>	the subject line to be set up into autoresponder ("Re: <incoming subject>") or a custom string.
-auto_replyto	<string>	return address that will be set up into the autoresponder's messages
-autotext	<string>	autoresponder message text
-autoatch	<add del>:<file1[,file2]>	adds/removes autoresponder attachment files
-autofrq	<number>	defines the maximum number of responses to a unique e-mail address per day
-autostor	<number>	defines the number of unique addresses to be stored for autoresponder
-autoored	<addr>	defines the e-mail address to forward all incoming mail to
-drweb	<in out inout off>	manages antivirus filtering

For managing subdomains, use the subdomain.sh utility located in `/usr/local/psa/bin`. The following commands and options can be used:

Table A.6.

Command	Parameter	Action
--create or -c	<subdomain>	creates a subdomain for domain specified with -domain option

Command	Parameter	Action
--update or -u	<subdomain>	updates an existing subdomain for domain specified with -domain option
--remove or -r	<subdomain>	removes subdomains specified with -subdomains option from the domain, specified with -domain option.
--info or -i		retrieves information on subdomains
--help or -h		displays help on utility usage
Option	Parameter	Note
-domain or -d	<domain_name>	use to specify the main (parent) domain for creating the subdomain for
-new_name	<new_subdomain>	change the subdomain name to the specified one (the option cannot be used when creating new subdomains)
-ftp_user	<native main>	use a separate FTP user account for this subdomain (native) or the same FTP user as that of the main domain (main). By default the FTP account of the main (parent) domain is used for managing the subdomain
-login	<login>	FTP user login name (can be specified if separate FTP account is used)
-passwd	<password>	FTP password (no password is set by default, and it may be specified when separate FTP account is used)
-hard_quota	<MB>	hard disk quota (use 0 for unlimited, which is set by default). You can specify this option when using a separate FTP account.

Command	Parameter	Action
-ssi	<true false>	SSI support on subdomain (default: false)
-php	<true false>	PHP support on subdomain (default: false)
-cgi	<true false>	CGI support on subdomain (default: false)
-perl	<true false>	Perl support on subdomain (default: false)
-asp	<true false>	ASP support on subdomain (default: false)
-python	<true false>	Python support on subdomain (default: false)
-coldfusion	<true false>	ColdFusion support on subdomain (default: false)
-subdomains or -s	<subdomain[,...]>	use for specifying the subdomains to be removed or to retrieve subdomain information (--remove and --info commands respectively). By default, the --info command outputs information on all existing subdomains.

For managing mailing lists, use the maillist.sh utility located in `/usr/local/psa/bin`. The following commands and options can be used:

Table A.7.

Command	Parameter	Action
--create or -c	<maillist>	creates a mailing list
--update or -u	<maillist>	updates mailing list properties
--remove or -r	<maillist>	removes mailing list
--info or -i	<maillist>	displays mailing list subscribers
--help or -h		displays help on utility usage

Command	Parameter	Action
-domain or -d	<domain_name>	use to specify the main (parent) domain for creating the subdomain for
-passwd	<password>	Set mailing list administrator's password (may be specified only with the 'create' command)
-email	<email>	Set mailing lists administrator's email (may be specified only with the 'create' command)
-notify	<true false>	Notify mailing list administrator about mailing list creation (default: true, may be specified only with the 'create' command)
-status	<true false>	Turns mailing list on/off (default: true)
-members	<add del>:<email1>,...,<emailN>	Adds/deletes email addresses to/from mailing list

For managing databases, use the database.sh utility located in `/usr/local/psa/bin`. The following commands and options can be used:

Table A.8.

Command	Parameter	Action
--create or -c	<db_name>	creates a database
--update or -u	<db_name>	updates database: add, edit, remove db user
--remove or -r	<db_name>	deletes database
--help or -h		displays help on utility usage
Option	Parameter	Note
-domain	<domain_name>	domain name
-type	<mysql>	Type of database

Command	Parameter	Action
-passwd	<passwd>	Set user password
-add_user	<login_name>	Add user with given name
-update_user	<login_name>	Update user with given name
-remove_user	<login_name>	Remove user with given name
-user_name	<login_name>	Set login name (may be specified with "update_user" option)

Customizable httpd.include per domain

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

```
/home/httpd/vhosts/<domain-name>/conf/httpd.include
```

This file is overwritten each time the virtual host configuration is changed, thus any manual alterations made to the file are discarded. To use custom directives or redefine those inserted by Plesk, you need to create the files `vhost.conf` and/or `vhost_ssl.conf` with necessary directives in the directory

```
/home/httpd/vhosts/<domain-name>/conf/
```

If any (or both) of these files exist by the time the main configuration file is generated, Plesk inserts the appropriate directive `Include /home/httpd/vhosts/<domain-name>/conf/vhost.conf` or `Include /home/httpd/vhosts/<domain-name>/conf/vhost_ssl.conf` into the HTTP and/or HTTPS virtual host context respectively.

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

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

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

Global access control list in named.conf

To allow DNS transfers server-wide on Plesk, the administrator can use global access control list in `named.conf`.

To set up an acl, the administrator should insert into the Plesk database the values describing servers to which DNS transfers are allowed. It can be done with mysql query:

```
insert into misc (param,val) values ('DNS_Allow_Transfer1', '1.1.1.1/24');
```

To specify more hosts, use the parameters like "DNS_Allow_Transfer2" and so on:

```
insert into misc (param,val) values ('DNS_Allow_Transfer2', '2.2.2.2');
```

Hosts should be specified by IP address and optional mask.

Once you added all the required IPs, run the following command to update `/etc/named.conf`:

```
admin/sbin/dnsmng update any.of.your.domains
```

After that, the `named.conf` file will be updated with the following entries:

```
acl common-allow-transfer {
    1.1.1.1/24;
    2.2.2.2;
};
```

Name of this `acl` will be added to the `allow-transfer` section of each DNS zone.

```
zone "zone1.com" {
    type master;
    file "zone1.com";
    allow-transfer {
        common-allow-transfer;
    };
};
```

Chili!Soft ASP support

Chili!Soft ASP allows to run Microsoft ASP and VBScript/JScript applications on an Apache server.

As Chili!Soft ASP has its own web based control panel Plesk has no built-in support for it. However, Chili!Soft ASP can be easily used with Plesk. Follow the instructions below to install:

1. Download the Sun Chili!Soft ASP package from the web server to the temporary directory.
2. Extract the files of Sun Chili!Soft ASP using the command `# tar xvf chiliasp-3.6.2L.1047a.tar`
3. Run the `install.sh` script: `# ./install.sh`
4. Read the license agreement and confirm acceptance by entering "yes"
5. Press Enter to install Sun Chili!Soft ASP by default to the directory `/opt/casp`
6. Press "y" to confirm entering the serial number, then enter the serial number when prompted. If you do not have the serial number to supply, press "n".
7. When the wizard prompts to install the bundled Apache, press "n".
8. Select the language. Press Enter for default.
9. Select the first option (Use the bundled 1.3.1 JRE) to install the bundled JRE 1.3.1 and confirm

installing, pressing the y button.

10. At this step you are prompted to define how to search for the web server the Chili!Soft ASP will work with. Select the option 4 (Don't search) for the installer to skip search and go to the next step.
11. Select option 3 (Do not configure a Web server)
12. At this step you are suggested to set the administrator's shell configuration. Select the option 1 (Default configuration)
13. The installation script work finishes at this step, however the installation is not yet finished as the web server needs to be properly configured, which will require several additional steps.
14. Determine the Apache version installed:

```
# rpm -q apache. Press Enter.
```

```
apache-1.3.23-14
#
```

So you can see that the Apache version is apache 1.3.23. After that you need to check whether there is an appropriate module in the Sun Chili!Soft ASP product installation.

```
# ls -l /opt/casp/module/linux2_optimized/ Press Enter.
```

```
apache_1.3.11
apache_1.3.12
apache_1.3.14
apache_1.3.19
apache_1.3.20
apache_1.3.22
apache_1.3.6
apache_1.3.9
netscape
netscape_4.x
netscape_6.x
zeus
#
```

As you can see there is no appropriate Apache version and the latest apache version that can be used is apache_1.3.22. That is why you can simply copy this directory recursively to the directory with number of your Apache:

```
# cp -pR /opt/casp/module/linux2_optimized/apache_1.3.22
/opt/casp/module/linux2_optimized/apache_1.3.23 Press Enter.
```

15. Now you need to configure the ASP server to work with the client Apache:
 - 15.1. Run the configuration script: `# /opt/casp/configure-server`
 - 15.2. Select the option 1 (Configure the ASP Server)

-
- 15.3. Select the option 1 (Specify the Web server)
 - 15.4. Select the option 1 (Apache)
 - 15.5. Specify the path to the client Apache configuration file `/etc/httpd/conf/httpd.conf`
 - 15.6. Specify the path to the apache binary `/usr/sbin/httpd`
 - 15.7. Select the option 1 (Apache Web server) to configure the web server that you specified at the previous steps.
 - 15.8. Enter "y" to confirm that all the entered information is correct.
 - 15.9. Select the option 1 (Default configuration)

That's it. The Chili!Soft ASP is completely installed.

Now you can manage the ASP server via the control panel, which is accessible at URL `http://yourservername.com:5100`

Restoring mail configuration

Mchk is an internal utility intended for use by Plesk Control Panel. However, as administrator, you can use it for restoring the Qmail and Courier-imap configuration by internal Plesk database when needed. By default mchk is running in the background mode, to execute it in the foreground, use the `-v` option.

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

NOTE

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

Manageable Tomcat connectors ports

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

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

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

i NOTE

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

Appendix B. Glossary of Terms

APACHE

Apache is an open source Web server that is distributed free. Apache runs on Unix-based operating systems (including Linux and Solaris) and Windows 95/98/NT. Apache was originally based on the NCSA server, but is now an independent product, supported by the nonprofit Apache Software Foundation.

BROWSER

A browser is a software application that lets you access information on the Internet. Browsers can read HTML and send HTTP or FTP requests for services on the Internet. Browsers are usually associated with the World Wide Web portion of the Internet.

CGI

CGI, or the common gateway interface, provides a standardized method for Web servers to send a user request to an application and to receive information back for the user. For example, when you click on a URL link, the Web server sends the requested page to you. CGI is part of the HTTP protocol. CGI works in many different languages, and across several different platforms.

CLIENT

A client is a company or individual requesting services from an Internet presence provider. A client is a customer of a Web hosting company, or a user of Internet services. In hardware terminology, a client is a computer system or a software package that requests services or information from another application that resides across the network. Think of the client as your PC or workstation, through which you access programs and data across a network or the Internet, usually on a server. In very simple terms, a client is a user.

DB WebAdmin

DB WebAdmin is a web-based administration tool that allows to manage a whole MySQL server as well as a single database.

DNS

DNS, short for Domain Name System, is a distributed database that maps names and IP addresses for computers using the Internet. DNS is a standardized system that identifies domain name servers.

DOMAIN

A domain is a virtual address on the Internet for any organization or entity. Technically, a domain is a group of networked computers (servers) that represent an organization and provide network services. However, several domains could reside on one server, in dedicated space provided by a Web hosting service. To the Internet user, a domain appears as space on one server, regardless of the implementation. Domains are identified by their familiar Internet URL (uniform resource locator) addresses. For example, `www.sw-soft.com` is the name of the domain where SWsoft information resides on its servers. Syntactically, a domain name is a string of names or words separated by periods. For example, a domain name such as:

hello.house.neighborhood.com includes the names of:

- the host: hello
- the subdomain: house
- the domain: neighborhood
- the organization type: com

Some top-level domain names:

- arpa: ARPAnet (a Defense Department communications system that established the Internet)
- com: Commercial, for-profit organizations and businesses
- edu: Educational institutions
- gov: Government organizations
- int: International organizations
- mil: U. S.-based military
- net: Internet access providers
- org: Non-profit organizations
- aero: Air-transport industry
- biz: Businesses
- coop: Cooperatives
- info: Information
- museum: Museums
- name: For registration by individuals
- pro: Accountants, lawyers, physicians, and other professionals
- 2-alphabetic characters: the country code top-level domains (ccTLDs), such as, for instance .uk for United Kingdom.

FTP

FTP, or File Transfer Protocol, is a method used to transfer files to (upload) and from (download) a remote server. You can use the FTP command to:

- Copy a file from the Internet to your PC
- Move a file from your PC up to the Internet

-
- Rename an existing file
 - Delete a file
 - Update an existing file with more recent data

GATEWAY

A gateway is a combination of hardware and software allowing dissimilar systems to communicate by filtering data through standardized protocols. Think of a gateway as a translator that allows your PC to talk with other computers on the network.

HOST

In a network, a host is usually a computer that stores software applications and data that may be accessed or retrieved by other users. But a host can be any addressable device on the network, not just a computer. The host provides services to other computers or users. An Internet Service Provider may also be referred to as a Web hosting company.

HTML

HTML, or HyperText Markup Language, is a standardized language for presenting information, graphics, and multimedia on the World Wide Web. HTML consists of hundreds of codes, tags, and symbols that define the type of information and how it should be displayed in a browser. HTML is universally understood on a wide variety of platforms.

HTTP

HTTP, or HyperText Transfer Protocol, is a standard for sharing World Wide Web files. HTTP lets you communicate across the Internet by carrying messages from your browser to a server.

IMAP

IMAP, or Internet Message Access Protocol, is a method for receiving e-mail messages from other Internet users on your local server. IMAP lets you see message headers before choosing and viewing the entire text of mail messages. You can selectively retrieve mail messages with IMAP. Compare IMAP to the POP and SMTP mail protocols.

IP ADDRESS

An IP address (Internet Protocol address) is an internal number that identifies a host on the Internet or a network. IP numbers are invisible to end users, replaced in your user interface by the more familiar domain names and URLs.

IP POOL

IP address pool is the range of available IP addresses.

MAIL AUTORESPONDER

Mail autoresponders are automatic replies to email sent to a particular mail name. Autoresponders can

include both a text message and attached files. This mail function is often used on mail accounts for individuals who are away for a certain period of time, or are unable to check their mail for any number of reasons.

MAIL GROUP

Mail groups are used for sending e-mail to a group of people through one address rather than to each individual address. Mail groups save you time and effort in reaching several people at once; you only have to create one e-mail message to the group, rather than several identical messages to everyone.

MAILMAN

Mailman is software to help manage email discussion lists, much like Majordomo and SmartList. Unlike most similar products, Mailman gives each mailing list a web page, and allows users to subscribe, unsubscribe, etc. over the web. Even the list manager can administer his or her list entirely from the web. Mailman also integrates most things people want to do with mailing lists, including archiving, mail-to-news gateways, integrated bounce handling, spam prevention, email-based admin commands, direct SMTP delivery (with fast bulk mailing), support for virtual domains, and more. Mailman runs on most Un*x-like systems, is compatible with most web servers and browsers, and most SMTP servers.

MAIL REDIRECT

Mail redirects are used to forward or redirect email from one POP3 mailbox to another email address. By creating an email redirect or alias, messages are sent to a different email box without the sender needing to know the new address. Email can be redirected to an address outside the domain.

MySQL

SQL is a Structured Query Language that was created as a standardized method of defining, manipulating, and searching data in a database. It is currently the most commonly used database language. MySQL is a fast, easy-to-use, multi-user SQL database server in a standard client/server environment. MySQL handles graphics as well as text. For more information, visit <http://www.mysql.com>.

NETWORK

A network is a system of interconnected computers and peripheral devices (such as printers).

PACKET

Data that is transported across the Internet is divided into small, manageable units called packets. Data packets can be sent more quickly and efficiently across a network than the full stream of data in a message or file.

PERL

Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use it for a vast number of automation tasks. Many CGI programs are written in Perl.

PHP

PHP (originally meaning Personal Home Page) is a server-based HTML embedded scripting language that

runs on multiple platforms, primarily on Linux servers. PHP accesses and manipulates data in a MySQL database, and helps you create dynamic Web pages. You write HTML and embed code in the HTML that performs a specific function. The embedded code is the PHP portion of the script, identified in the HTML by special start and stop tags. A PHP file has an extension of .php or .php3 or phtml. All PHP code is executed on a server, unlike a language such as JavaScript that is executed on the client system. For more information, visit <http://www.php3.org>.

POP3

POP3, or Post Office Protocol Version 3, is a method used to receive electronic mail across the Internet, accommodating different mail software packages and systems. POP3 receives and holds all your e-mail on a server. You can then download all your messages when you connect to the mail server; you cannot selectively retrieve messages. Compare POP to the IMAP mail protocol.

POSTGRESQL

PostgreSQL is an open source database system, that began as an enhancement to the POSTGRES research prototype DBMS. Where POSTGRES used the PostQuel query language, PostgreSQL uses a subset of SQL.

PROTECTED DIRECTORY

A directory is an organized collection of files and subdirectory folders on a computer. A protected directory is one that cannot be accessed by all public users; you must have access privileges to read information in a protected directory.

PYTHON

Python is an interpreted high-level programming language. You can write web-based applications in Python that will run many times faster than traditional CGI and will have access to advanced features such as ability to retain database connections and other data between hits and access to Apache internals.

QMAIL

Qmail is a secure and highly reliable e-mail message handling system. It replaces the sendmail daemon on Unix and Linux systems. Qmail is fast and uses little memory. Users can create their own mail lists, and system administration is minimal. Qmail uses the Simple Mail Transfer Protocol (SMTP) for message exchange with other systems.

REBOOT

Rebooting simply means restarting a computer. You should not reboot a server that has users accessing it until you have informed the users that the server must be shut down temporarily. Sometimes, an emergency necessitates rebooting a server immediately, but it is not a recommended practice.

SECURE HTTP

Secure HTTP (S-HTTP or HTTPS) is an encryption method uses to protect documents on the World Wide Web. An alternative to S-HTTP is an SSL certificate (or Secure Socket Layer) that secures an entire session, not just a document or a file. S-HTTP supports several different message encryption formats, and

works with any communication between clients and servers.

SECURITY

There are several different ways to control access to a computer or network, to protect proprietary data, and to maintain privacy. Security measures can be defined at several different levels (at the server level, on a directory, for an individual file, etc.) for optimum protection.

SERVER

A server is a computer system (a combination of hardware and software) that runs programs, stores files, directs traffic, and controls communications on a network or the Internet. Clients (also called users or workstations) access a server for specific information and services.

SHARED IP

An IP address that can be used for hosting by several clients.

SKELETON DIRECTORY

In Plesk, this term refers to a set of directories and files that get copied into a newly created virtual host directory structure at the time the virtual host is created. It may be used to have a set of CGI scripts included with every account created in Plesk. It is very useful if you are looking to have a more informative, customized welcoming index.html page, and it is also helpful if you have anything else that needs to be included by default within the directories of the virtual host.

SMTP

SMTP, or Simple Mail Transfer Protocol, is a standard for transmitting mail messages across different computers on a TCP/IP network. SMTP can only be used when both the mail sender and receiver are ready. If the destination PC is not ready, a 'post office' must temporarily store the mail. In that case, a post office protocol such as IMAP or POP is used to retrieve the mail.

SSI

SSI stands for 'server-side includes', a type of HTML comment that directs the webserver to dynamically generate data for the Web page whenever information is requested. SSIs can also be used to execute programs and insert the results; therefore they represent a powerful tool for web developers.

SSL

SSL stands for Secure Socket Layer, and is a set of rules used for exchanging information between two computer devices using a public encryption system. SSL establishes secure communications between servers and clients. SSL provides a safe and authenticated method of handling e-commerce transactions. Only authorized users can access and read an SSL-encrypted data stream. An alternative to SSL is Secure HTTP (S-HTTP), used to encrypt World Wide Web documents (rather than securing an entire session, as does SSL).

SSL CERTIFICATE

An SSL certificate is an electronic key that encrypts transmissions between two computers on a public

network, providing privacy and security to the session. Think of an SSL certificate as an electronic ID card for an individual or a computer service. An SSL certificate confirms that a message that you receive actually did come from the person identified. The certificate key is issued by a third party. SSL certificates are used for secure e-commerce communications, protecting information such as credit card numbers and personal data. You can generate an SSL certificate with a utility such as SSLeay. Then, submit it to a certificate authority such as GeoTrust, Inc (www.geotrust.com).

TCP

TCP stands for Transmission Control Protocol, and is the primary data transport protocol on the Internet. TCP transmissions are fast, reliable, and full-duplexed.

TCP/IP

Transmission Control Protocol/Internet Protocol, commonly known as TCP/IP, is a data transmission protocol that was developed by ARPA, the Advanced Research Projects Agency. ARPA is the founding organization of the Internet.

TELNET

Telnet is a method of accessing another remote computer. You can only access the other computer if you have permission to do so. Telnet differs from other protocols that simply request information from a host computer, because it actually logs you on to the remote computer as a user.

TOMCAT

Tomcat is a server solution based on the Java Platform that supports the Servlet and JSP specifications. Managed by the Apache Jakarta Project, it is developed in an open and participatory environment.

URL

A URL is a Uniform Resource Locator used to identify an organization or domain on the Internet. URLs are standardized names that are typically found on the World Wide Web portion of the Internet. URL addresses identify domains on the network. Read about Domains for more detail.

USER

Simply put, a user is a client. In hardware terminology, a client is the PC that you use to access information from other computers (usually servers) on the Internet or network.

WEBMAIL

WebMail is a Web based interface to Unix system mailboxes. It allows a user to access and administer his IMAP/POP3 mailbox via the world wide web.

WEB USER

A web user is a user account within Apache that is used to define locations for personalized web pages with individual FTP access.

WORKSTATION

A workstation is a user or client that accesses information from other computers (usually servers) on a network.