



# **PLESK 7.5 RELOADED**

## **CLIENT'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.

Plesk™ and Plesk 7 Reloaded™ are registered trademarks of SWsoft, Inc. All other trademarks and copyrights are the property of their respective owners.

13755 Sunrise Valley Drive, Suite 325, Herndon, VA, 20171 USA, Ph.: +1 (703) 815-5670, Fax.: +1 (703) 815-5675

---

---

# Table of Contents

1. About Plesk .....	1
Plesk Interface Specific Features .....	1
2. Performing Administrative Tasks .....	3
Editing Your Account Information and Password .....	3
Setting Up Interface Preferences and Logo .....	4
Viewing Permissions and Resource Usage Limits .....	6
Managing IP Pool .....	6
Managing Domain Templates .....	8
Managing Virtual Host Skeleton .....	11
Managing Custom Buttons .....	13
Viewing the Status Report and Traffic Statistics .....	14
Scheduling Report Deliveries .....	16
Managing User Sessions .....	17
Using Help Desk .....	18
3. Administering Domains .....	21
Creating a Domain .....	21
Managing Hosting .....	23
Uploading Site Content .....	29
Using Custom Error Documents .....	30
Using Site Preview .....	33
Setting Domain Level Limits .....	33
Managing SSL Certificates .....	35
Managing DNS Zones .....	41
Managing Mail .....	45
Managing Mailing Lists .....	58
Setting Up a Domain Administrator Account .....	61
Registering a Domain with MPC .....	62
Accessing Additional Services (Extras) .....	62
Managing Databases .....	62
Managing Java Applications .....	65
Managing Web Users .....	67
Managing Subdomains .....	70
Managing Protected Directories .....	71
Managing Anonymous FTP Access .....	74
Managing Log Files and Log Rotation .....	75
Scheduling Crontab Tasks .....	78
Using File Manager .....	80
Using the Domain Application Vault .....	83
Accessing the Mambo Content Management Software .....	84
Accessing Microsoft FrontPage Web Administrator .....	84
Backing Up and Restoring Domains .....	84
Deactivating/Activating a Domain .....	87

Renaming Domains .....	88
Performing Group Operations on Domains .....	89
Removing Domains .....	91
Managing Domains via Remote XML Interface .....	91
A. Glossary of Terms .....	93

# Chapter 1. About Plesk

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.

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.

## 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 screenshot displays the Plesk control panel interface. On the left is a navigation pane with sections: General (Home), System (Sessions, Log out), and Help & Support (Help Desk, Help, Client home page). The main content area shows a user profile for 'Alec' and a 'Tools' section with icons for Edit, Report, Preferences, Permissions, Limits, IP Pool, Skeleton, Logo Setup, and Custom Buttons. Below this is an 'Info' section showing '1 domains, 1 active domains, 0 B disk space used, 0 B traffic used'. The 'Domains' section features a search bar and a table with columns: P, S, H, Domain name, Creation date, Subdomains, Disk usage, and Traffic. The table contains one entry for 'domain.com' created on July 9, 2004, with 0 subdomains and 0.00 MB of disk usage.

P	S	H	Domain name	Creation date	Subdomains	Disk usage	Traffic
✓	✓	✓	domain.com	July 9, 2004	0	0.00 MB	0.00 MB/Month

- The Home shortcut opens your Home page (also referred to as the Client Home page), which gives you access to major administrative functions available for your account.
- The Sessions shortcut is used for managing currently active user sessions.
- The Log out shortcut ends your control panel session.
- The Help Desk allows you to report your problems to the server administrator.

## 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), 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. Performing Administrative Tasks

This chapter focuses on administrative tasks you perform within your Plesk™ environment. The operations described are available only when you are logged on as client to your system.

## Editing Your Account Information and Password

Occasionally, you may need to change the information in your record. To do it, follow these steps:

1. Click the  Edit icon on the Home page. The account details will be

displayed:

Alec >  
**Alec's account details** [Up Level](#)

Client form

Company name	<input type="text" value="SWsoft"/>
Contact name	<input type="text" value="Alec"/>
Login *	<input type="text" value="client"/>
Old password	<input type="text" value="*****"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Phone *	<input type="text" value="1111222"/>
Fax	<input type="text"/>
E-mail *	<input type="text" value="email@domain.com"/>
Address	<input type="text"/>
City	<input type="text"/>
State/Province	<input type="text"/>
Postal/ZIP code	<input type="text" value="11122333"/>
Country	<input type="text" value="United States"/>

\* Required fields

2. To modify an item, click in a specific text box to enter data, or use the Tab key to move from one text box to the next.

### NOTE

Use only alphanumeric symbols in the login name.

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

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

### **IMPORTANT**

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


### **If you forget your password**

If you forget your password, you can use the password reminder feature available from the control panel login screen.

## Setting Up Interface Preferences and Logo


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 length of interface button labels, and allow/disallow multiple sessions under your login.

To change the interface preferences, follow these steps:

1. Click the  Preferences icon at the Home page. The client preferences page opens.
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, which will be visible to domain and mail users when they log in to the control panel. You can also 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 Home page. The Logo Setup page appears.
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 URL for logo 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.

## Viewing Permissions and Resource Usage Limits

To view the permissions for operations you can perform within your environment, click the  Permissions icon on the Home page. The Client

permissions page will appear listing all available operations.


To view the resource usage limits defined by the administrator for your account, click the  Limits icon on the Home page. The Client limits page will

appear listing the resource types and limits defined.


## Managing IP Pool

The IP pool is the location within which your IP addresses are managed. You are given IPs and then are able to utilize them within your own domains. IPs are able to be granted as either *exclusive*, meaning that you become the user with exclusive rights to this IP, or *shared*, meaning that this IP is shared among many other 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. You can immediately see the complete list of allocated IPs and identify the locations on which each IP is currently being used within your environment.



Click the  IP Pool icon on the Home page to access the IP pool. It




displays the list of IP addresses that were granted (exclusively or as shared):

Alec >  
**IP pool of client Alec**  Up Level


IP Addresses




IP Addresses (2)

 Search  Show All

S	T	IP Address ▲	Hosting
		10.1.211.1	<a href="#">0</a>
		<a href="#">10.1.211.101</a>	<a href="#">1</a>

**Table 2.1. The IP state/type icons.**

Icon	Meaning
<b>The state icon indicates the system state of the IP address:</b>	
	means that the IP address functions properly

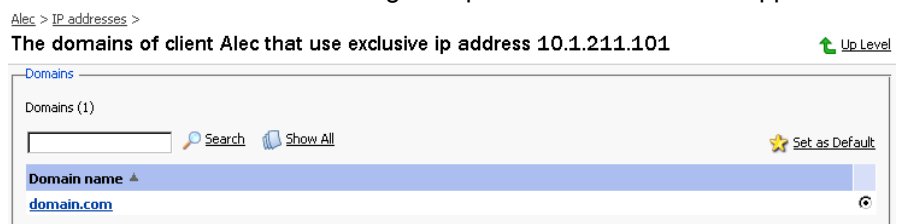
Icon	Meaning
<b>The state icon indicates the system state of the IP address:</b>	
	means that something is wrong with the IP address.
<b>The type icon indicates how the IP address was granted:</b>	
	means that the IP address was granted exclusively
	means that the IP address was granted as shared


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

## 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 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:



2. To jump to the 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 IP pool management page.

## Assigning an SSL certificate for an exclusively granted IP address

You can assign SSL certificates to the exclusively granted IP addresses in your IP pool.

1. At the IP pool, 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.

## 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,

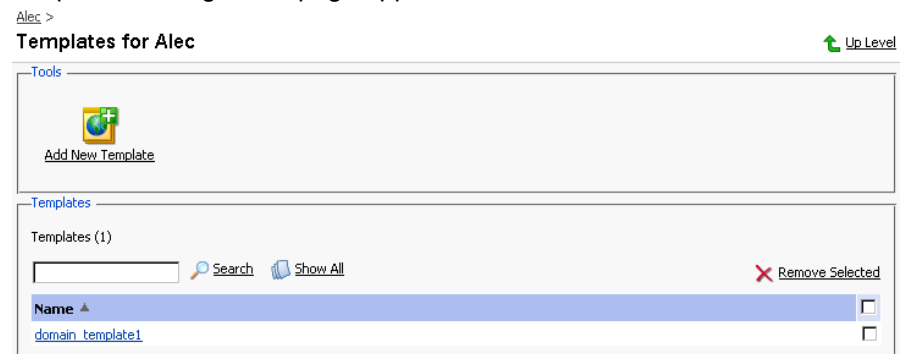
- Microsoft FrontPage authoring
- Apache ASP support
- SSI support
- PHP support
- CGI support
- mod\_perl support
- mod\_python support
- ColdFusion support
- Web statistics
- Use of Custom Error Documents


## Creating a domain template

To add a new domain template, follow these steps:

1. On the Home page click the  Domain Templates icon. The Domain

templates management page appears:



2. Click  Add New Template. The Template creation and editing page appears.
3. Enter the name for the domain template in the Template name field.
4. Specify how to deal with the mail directed at nonexistent users in this domain, and enable access to Webmail, if desired.
5. 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.
6. 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).
7. 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.

8. To enable Mailing lists, select the corresponding checkbox.
9. To retain the traffic statistics for domains, select the corresponding checkbox and specify the retention period in the Retain traffic statistics for ... Months field.
10. Select the domain DNS zone type using the Master or Slave radio button.
11. To enable physical hosting for domain, select the Physical hosting checkbox.
12. Specify the hard disk quota in the appropriate field, if needed.
13. SSL support checkbox enables the maintenance of https protocol. By default the data accessible via secure encrypted SSL protocol and non-encrypted HTTP are stored in two different directories within a virtual host. To have all data stored in the same directory, select the Use a single directory for housing SSL and non-SSL content check box.
14. 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.
15. 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 access statistics for the domain. You can

choose to password protect access to statistics.

- Custom Error Documents: allow the use of custom pages in case of web server errors.

16. 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.

### 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 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, \*.tar, \*.tar.gz 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 icon on the Home 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.

## 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 the repository of custom buttons can be placed in any of the following locations:

- Navigation pane;
- Home page;
- Domain Administration pages of all domains.


You access the repository of custom buttons clicking the  Custom

Buttons icon on your Home page.

### NOTE

If you wish to create individual buttons that will be placed only on 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.

## Viewing the Status Report and Traffic Statistics

Plesk keeps a summary of important data for every control panel user. The client report is a brief overview of the account-specific system information.


To view the report, click the  Report icon on the 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 your domains over a period of time.

1. Click the  Traffic History icon at the Client report page.
2. The 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 your 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 Domains

To view the statistical information on traffic used by domains, on the Home page click  Current 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 %)
<a href="#">domain.com</a>	0.00 MB	Unlimited	-	-

Presented in the table are the data on amount of traffic used within your account, and your 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.

## Scheduling Report Deliveries

You can schedule daily, weekly, or monthly deliveries for report on your account status and reports on domains.

For the account status report, you can choose to deliver:

- to your e-mail address, registered in the system.
- to any other e-mail address.

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 client's e-mail address (i.e. your e-mail, registered in the system),
- a report on a specific domain to the domain administrator's e-mail address,
- reports on every domain to the respective domain administrators.

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

To manage account status report deliveries, click the Report icon on your 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.

## 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 Client's session,  for Domain Administrator'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 Administrator's sessions,  for subdomain administrator'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.

## Using Help Desk

To submit a new trouble ticket, follow these steps:

1. Select the Help Desk shortcut in the navigation pane. The Help Desk system interface will open displaying the list of existing tickets. The list is empty when there are no tickets submitted.
2. Click  Add New Ticket. The ticket submission page opens.
3. Enter ticket subject, select the category the issue is related to, and type in the problem description.
4. Click OK. The ticket is now submitted to the system, and the appropriate record is added to the list.

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

1. On the page listing tickets, click on a ticket id or subject. The page will open displaying all comments made to the ticket, and allowing you to change the ticket properties and add new comments.
2. 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.
3. Click OK to submit all changes.



---

# Chapter 3. 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](http://www.sw-soft.com) is the name of the domain where SWsoft's information resides on its servers.

### 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. Click  Add New Domain icon on your Home page.
2. 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.
3. Select a template to be applied from the drop-down list, if you wish this domain to be created by a template.
4. Select the IP address to be used for hosting from the drop-down list.

5. Check (or leave checked) the Proceed to hosting setup checkbox if you wish to set up hosting for the domain after it is created.

### 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.





6. 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.

Once a domain name has been created, it is displayed in the list of domains at the bottom of your Home page accompanied by the following icons:

**Table 3.1.**

Icon	Meaning
<b>The state icon indicates the system state of the domain:</b>	
	means that the domain is operating within defined disk space and traffic parameters
	means that the allocated disk space or traffic limitations are exceeded at this particular domain. The Plesk system evaluates disk space and traffic every 24 hours
<b>The status icon indicates if the domain is activated/deactivated:</b>	
	means that the domain is activated
	means that this domain is presently deactivated and inaccessible
<b>The hosting type icon indicates the type of hosting set-up for the domain:</b>	

Icon	Meaning
<b>The state icon indicates the system state of the domain:</b>	
	indicates Physical Hosting
	indicates Standard Forwarding
	indicates Frame Forwarding
	indicates that no hosting was configured for the domain
<b>Additional:</b>	
	used for accessing the domain URL in browser

## 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 customer. The customer 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 your customer'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 your customer'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. Access your Home page. The page opens listing all existing domains at the bottom:

✓ ✓ Alec

Tools

Disable Edit Report Preferences Permissions Limits

IP Pool Skeleton Logo Setup Custom Buttons

Add New Domain Domain Templates Register Manage Extras Traffic

Info


1 domains, 1 active domains, 284 KB disk space used, 0 B traffic used

Domains

Domains (1)

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

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

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

Hosting type

Hosting type


Physical hosting

Standard forwarding

Frame forwarding

\* Required fields

1. On your Home page, click on the domain name to access the Domain administration page.

2. Click the  Setup icon. The Hosting Type Selection page

appears:

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:

1. On the Hosting Type Selection page, select the **Physical hosting** radio button. Click OK. The Physical hosting setup page appears.

2. 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 users to implement an SSL certificate, make sure a check mark appears in the SSL support box.

By default the data accessible via secure encrypted SSL protocol and non-encrypted HTTP are stored in two different directories within a virtual host. To have all data stored in the same directory, select the Use a single directory for housing SSL and non-SSL content check 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. Use the Shell access to server with FTP user's credentials option if you

need to allow a user to access his/her home directory on the server through SSH or Telnet. Depending on the permissions defined, the user might also be able to browse the server filesystem outside the home directory, unless you choose the "chrooted shell" option. It is advised that you forbid shell access for security reasons.

** NOTE**

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. Authoring will be disabled by default. For security reasons, authoring 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 Administrator logins to the control panel. 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 you want 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 for creating dynamic Web pages. If you want 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 you want 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 you want 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 you want 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.

## NOTES

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. For security reasons, we recommend that you use different passwords for logging in to your FTP account and accessing the statistics. You can change the password for accessing the statistics directory 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 customer'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 customer'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.

## Uploading Site Content

You can upload site content in any of the following ways: via FTP, via SSH, using Plesk File Manager or Microsoft FrontPage. We recommend uploading via FTP, as it is the simplest way.

### Via FTP

1. Connect to server using your FTP account credentials
2. Upload files and directories that should be accessible via HTTP protocol to the httpdocs directory, and files/directories that should be transferred securely over SSL protocol to the httpsdocs directory. Place your CGI scripts into the cgi-bin directory.
3. Close your FTP session.

### Using Plesk File Manager

1. In the Plesk control panel, click the File Manager button on the Domain Administration page.
2. You can create and upload files and directories only in the following directories: httpdocs, httpsdocs, private and cgi-bin. You should place files and directories that should be accessible via HTTP protocol to the httpdocs directory, and files/directories that should be transferred securely over SSL protocol to the httpsdocs directory. Place your CGI scripts into the cgi-bin directory.

- Use the Add New Directory button to create new directories.
- To create new files in the required directory, click Add New File, in the File creation section specify the file name, select the Use html template checkbox, if you want file manager to insert some basic html tags to the new file, and click OK. A page will open allowing you to enter the content or html-formatted source of a new file. After you are done, click OK.
- To upload a file from the local machine, click Add New File, specify the path to its location in the File source box (or use the Browse button to locate it), and click OK.

## Via SSH (only for Linux and FreeBSD users)

Use the scp command to copy files and directories to the server: `scp your_file_name login@remoteserver.com:path` to copy files, and `scp -r your_directory_name login@remoteserver.com:path` to copy entire directories.

The users of Microsoft Windows can use Microsoft FrontPage to publish the site content via FTP or HTTP. Please, consult the MS FrontPage user documentation for details.

## Using Custom Error Documents

To inform Internet users of web server errors and help figure out what caused the problem, web servers generate and display standard HTML pages. Following is a list of error documents with descriptions.

**Table 3.2.**

400 Bad File Request	Usually means the syntax used in the URL is incorrect (e.g., uppercase letter should be lowercase letter; wrong punctuation marks).
401 Unauthorized	Server is looking for some encryption key from the client and is not getting it. Also, wrong password may have been entered.
403 Forbidden/Access Denied	Similar to 401; special permission needed to access the site - a password and/or username if it is a registration issue.

404 File Not Found	Server cannot find the requested file. File has either been moved or deleted, or the wrong URL or document name was entered.
408 Request Timeout	Client stopped the request before the server finished retrieving it. Usually occurs when servers are slow or file sizes are large.
500 Internal Error	Could not retrieve the HTML document because of server-configuration problems.
501 Not Implemented	Web server does not support a requested feature.
502 Service Temporarily Overloaded	Server congestion; too many connections; high traffic.
503 Service Unavailable	Server busy, site may have moved, or Internet connection was lost.
Connection Refused by Host	User either does not have permission to access the site or password is incorrect.
File Contains No Data	Page is there but is not showing anything. Error occurs in the document. Attributed to bad table formatting, or stripped header information.
Bad File Request	Browser may not support the form or other coding the user is trying to access.
Failed DNS Lookup	The Domain Name Server cannot translate domain request into a valid Internet address. Server may be busy or down, or incorrect URL was entered.
Host Unavailable	Host server down.
Unable to Locate Host	Host server is down, Internet connection is lost, or URL typed incorrectly.
Network Connection Refused by the Server	The Web server is busy.

With Plesk 7.5 you can customize only the following error messages:

- 400 Bad File Request
- 401 Unauthorized
- 403 Forbidden/Access denied
- 404 File Not Found

- 500 Internal Server Error

If you would like Plesk web server to show your custom error pages instead of standard ones, follow these steps:

1. Switch on support for custom error documents through Plesk interface. Go to a specific domain's administration page, click Setup, and select the Custom Error Documents checkbox.
2. If you access Plesk remotely, connect to your FTP account on the Plesk server, and go to the error\_docs directory. If you access Plesk locally, go to the directory /vhosts/domain\_name.tld/error\_docs/
3. Edit or replace the respective files. Be sure to preserve the correct file names:
  - 400 Bad File Request - bad\_request.html
  - 401 Unauthorized - unauthorized.html
  - 403 Forbidden/Access denied - forbidden.html
  - 404 File Not Found - not\_found.html
  - 500 Internal Server Error - internal\_server\_error.html
4. Once done editing, restart the web server manually, or wait till it is restarted. After that, the web server will start using your error documents.

## Using Site Preview

Once you have set up hosting for the domain and uploaded the site content, you can preview the site prior to DNS propagation. To do this, click the



Site Preview icon on the Domain administration page.

### Note

Site preview does not work for the web sites and web pages that include absolute paths to other files (like `<a href="http://domain.tld/image.gif">` or `<a href="/image.gif">`).

## 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.

To adjust the traffic statistics retention time for a given domain, follow these


steps:

1. Click the  Report icon at the Domain administration page.
2. Click the  Traffic History icon.
3. Select the Retain traffic statistics for [ ] Months checkbox, and type the number in the input box provided.
4. Click OK.

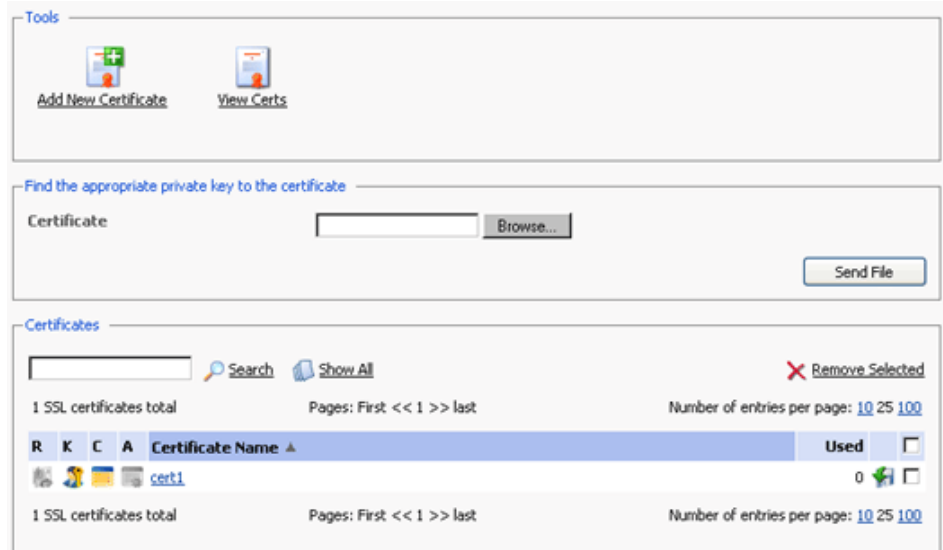
## Managing SSL Certificates

Secure Socket Layer protocol is the web standard for network security and secure e-commerce web hosting authorization. It ensures secure transactions between web servers and browsers while using a third party, a Certificate Authority (CA), to identify one end or both ends of the transactions.

Within each domain, there are independent certificate repositories, from where you can view properties of SSL certificates, add and remove certificates to/from the repository.

To access the repository within the specific domain, click the domain name in the list, and then click the  Certificates icon in the Tools group.

A list of available SSL certificates will open.



The screenshot displays the SSL Certificate management interface. At the top, under the 'Tools' group, there are two buttons: 'Add New Certificate' and 'View Certs'. Below this is a search section with the text 'Find the appropriate private key to the certificate'. It includes a text input field labeled 'Certificate', a 'Browse...' button, and a 'Send File' button. The main section is titled 'Certificates' and contains a search bar, a 'Search' button, and a 'Show All' button. There is also a 'Remove Selected' button with a red 'X' icon. Below the search bar, it indicates '1 SSL certificates total' and provides pagination options: 'Pages: First << 1 >> last' and 'Number of entries per page: 10 25 100'. A table lists the certificates with columns for 'R', 'K', 'C', 'A', 'Certificate Name', and 'Used'. The table contains one entry: 'cert1'. The 'Used' column has a checkbox that is currently unchecked. At the bottom, it again shows '1 SSL certificates total' and the same pagination and per-page options.

The SSL certificates are listed in a table with the following columns:

- Certificate Signing (R)equest - an icon shown in color indicates that a Certificate Signing Request for a certificate is present in the repository.
- Private (K)ey - an icon shown in color indicates that a private key for a certificate is stored in the repository.
- (C)ertificate - an icon shown in color indicates that a certificate file is stored in the repository.
- Certification (A)uthority - an icon shown in color indicates that a CA certificate is stored in the repository.

- Certificate name - Name of the certificate displayed in the control panel. Click it to edit the name or upload the parts for the certificate.
- Used - number of IP addresses that are assigned this certificate.

## Adding SSL Certificates to Repository

In order to implement SSL support within a virtual host, you should add a SSL certificate to SSL certificates repository and then assign the certificate to a specific IP address.

You can:

- generate a self-signed certificate,
- generate a certificate signing request, and purchase an SSL certificate from certification authority,
- buy a certificate via MyPlesk.com online store.

To use any of these options:

1. Access the SSL Certificates repository (Domain name > Certificates).
2. Click Add Certificate icon. The SSL certificate creation page will open. From this page you will be able to generate a self-signed certificate, generate certificate signing request, purchase a SSL certificate, upload the certificate you already have, or add the certificate parts to a certificate saved in the repository.

### Note

When acquiring or generating new certificates, make sure that the values you enter into the fields 'domain name', 'e-mail address', 'state or province', 'location', 'organization name', and 'department name' do not exceed the limit of 64 symbols.

## 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 (1024 bits are recommended for regular certificates).
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 the 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 private key and certificate signing request will be generated and added to the repository. You will be able to add the other certificate parts later on.

Once the CSR is generated, you can download it to the local machine by clicking the corresponding Download icon in the list of certificates, and then send the Request part (including the BEGIN and END tags) of it to the Certification Authority that will generate an SSL certificate in accordance with the information you supplied in the CSR.

Make sure you do not send or show your Private Key (which might be stored inside the certificate file) to the Certification Authority or anybody else.

## Purchasing Certificates Using MyPlesk.com Online Store

To purchase a new certificate through MyPlesk.com online store, 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 box.
3. Select your country from the drop-down box.
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 administrator's e-mail address in the appropriate field.
7. Make sure that all the provided information is correct and accurate, as it will be used to generate the private key. Then click the Buy Certificate button. Private key and certificate signing request will be generated (do not delete them!). MyPlesk.com login page will open in a new browser window.
8. Register or login to an existing MyPlesk.com account and you will be taken step by step through the certificate purchase procedure.
9. Choose a certificate type to purchase.
10. Click Proceed to Buy and order the certificate. In the Approver E-Mail drop-down box, please select the correct Approver e-mail.

** Note**

The approver e-mail is an e-mail address that can confirm that certificate for specific domain name was requested by an authorized person.

11. Your certificate request will be processed by GeoTrust, Inc., then you'll be asked for confirmation from GeoTrust, Inc., and the certificate will be sent to you by e-mail.
12. When you receive your SSL certificate, save it on your local machine or network.
13. Return to the SSL Certificates repository (Domain name > Certificates).
14. Click the Browse button in the middle of the page and navigate to the location of the saved certificate. Select it, and then click Send File. This will upload and install the certificate against the corresponding private key.

## Uploading Certificates or Certificate Parts to SSL Certificates Repository

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

1. At the SSL certificates repository, click the Add Certificate icon to create a new certificate, or click the certificate name in the list to modify an existing certificate.
2. Upload the certificate data in any of the two ways:
  - Upload the three certificate parts as files: choose the files from the local machine or network and click Send File.
  - Upload the three certificate parts as text: copy them to the clipboard and paste into the input fields, and click Send Text.

## Uploading CA Certificates

For the certificates purchased through some certification authorities you may need to install a so-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 SSL certificates repository, select a certificate from the list. You will be taken to the certificate properties page.
2. Use the Browse button, within the section related to the certificate uploading, to locate the appropriate CA Certificate file and click Send File, or copy the CA certificate contents to the clipboard, paste them into the corresponding input field and click the Send Text button.

## Generating 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 SSL certificates repository, select from the list a certificate, which has the private key part only. You will be taken to the SSL certificate properties screen.
2. Click Request.

## Removing Certificate Parts

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 SSL certificates repository, click on the certificate name in the list.
2. Click the Remove button located next to the CA certificate field.

## Assigning SSL Certificates to IP Addresses and Domains

When you add a certificate to repository, it is not installed automatically onto the domain or assigned to an IP address, but rather saved for the future uses. You can assign a certificate to an IP address from your IP pool management screen, or during hosting setup on an exclusively granted IP.

To assign SSL certificates to IP addresses:

- If domain's IP is exclusively allocated to you, then go to IP Pool > domain's IP address > select the required SSL certificate name from the SSL certificate drop-down box.

To assign SSL certificates to domains:

- From the list of domains located at the bottom of your home page, click the Physical hosting icon to the left of the domain name you need and then select the required SSL certificate from the SSL certificate drop-down box.

## Viewing Information on SSL Certificates Purchased through MyPlesk.com

If you purchased SSL certificates from MyPlesk.com online store, you can use a link in the Plesk control panel to track your certificate orders and view the details on certificates:

1. In the SSL certificates repository, click View Certificates.
2. In the new browser window that will open, enter the login and password for access to your MyPlesk.com account.
3. You will be taken to the Certificates section of the online store.

## Downloading SSL Certificates from Repository

To download any certificate from the repository to your local machine, in the list of certificates, click the Download icon corresponding to the required certificate

name. Select the location when prompted, specify the file name and click Save to save it.

## Removing SSL Certificates from Repository

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

## Managing DNS Zones

For each domain name, Plesk automatically creates a DNS zone in accordance with the DNS configuration presets that are changeable only by the server administrator. However, Plesk users allotted domain administration privileges can customize DNS zones for their own domains.


We would recommend modifying zones only to the users who have a good knowledge of DNS. Improper setup of DNS zone may result in improper functioning (or rather inaccessibility) of Web, mail, and FTP services.


If you use Plesk's DNS service for serving the hosted domains, you may be interested in reading the sections Adding and removing resource records to/from the zones and Changing zone type. If you don't, Plesk gives you the capabilities to validate zones on the authoritative DNS server against the hosting configuration of the domains served by Plesk. This is explained in the section If your Plesk is not authoritative for the zone.

To view and manage the zone for a specific domain, in the list of domains located at the bottom of your home page, click the domain name you need, and then click the DNS button under Services group.

The DNS zone properties screen will open.

**Tools**

  
Disable

  
Switch

**Add a DNS record**

Record type: A

**Restoring the DNS zone by the template**

IP Address: 10.1.36.100

WWW prefix:

**DNS records**

Search
Show All
✗ Remove Selected

9 DNS records total Pages: First << 1 >> last Number of entries per page: [10](#) [25](#) [100](#)

Host	Record type	Value	
10.1.36.100 / 24	PTR	d1.client1.ru.	<input type="checkbox"/>
d1.client1.ru.	MX (10)	mail.d1.client1.ru.	<input type="checkbox"/>
ftp.d1.client1.ru.	CNAME	d1.client1.ru.	<input type="checkbox"/>
www.d1.client1.ru.	CNAME	d1.client1.ru.	<input type="checkbox"/>
ns.d1.client1.ru.	A	10.1.36.100	<input type="checkbox"/>
d1.client1.ru.	A	10.1.36.100	<input type="checkbox"/>
webmail.d1.client1.ru.	A	10.1.36.100	<input type="checkbox"/>
mail.d1.client1.ru.	A	10.1.36.100	<input type="checkbox"/>
d1.client1.ru.	NS	ns.d1.client1.ru.	<input type="checkbox"/>

9 DNS records total Pages: First << 1 >> last Number of entries per page: [10](#) [25](#) [100](#)

From this screen you can:

- Add/remove resource records to/from the zone, and restore the original zone configuration.
- Change zone type.
- Switch local DNS service off for a given domain. You should do this if another server is authoritative for your domain.

## Adding and removing resource records to/from the zone

To add a new resource record to the zone, select a record type and click Add. Then you will need to specify the data appropriate for the selected resource record type:

- 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.

- 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).
- 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 is the highest and 50 is the lowest. Keep in mind you would also need to add the appropriate A record, and/or CNAME if applicable for the remote mail exchange server.
- 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.
- 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.
- For a TXT record, you will be able to enter an arbitrary text string, which could be a description or an SPF record.
- Click OK to submit the data.

To remove a resource record from the zone, in the list of resource records, select a corresponding check box, click Remove Selected, and then confirm removal.

To restore the original zone configuration by the DNS template, in the IP address drop-down box, select the IP address to be used with a template, specify whether a WWW alias is required for the domain, and click the Default button.


## Changing zone type


You can specify whether Plesk's DNS server should act as a master or slave name server when serving a zone. A DNS master server stores locally the zone file it serves, while a slave server only retrieves a copy of this file from the master.

By default, when a new domain name is created, the Plesk's domain name server is instructed to act a master for this zone. If you have another machine

serving this zone as a master, and wish to make this Plesk server act as slave, you should switch the zone type to slave.


To switch the zone type from master to slave:

1. At the zone properties screen (Domain name > DNS) click  Switch icon. The DNS Zone Properties page will open and the DNS zone type will change to slave.
2. Specify the IP address of the master DNS server.
3. Click Add.

To make the Plesk's DNS server act a master for this zone, at the zone properties screen (Domain name > DNS) click  Switch icon. The

appropriate resource records for the zone will be restored as they were retained before you switched the zone type.

## If your Plesk server is not authoritative for a zone

You should switch off the control panel's DNS service for each individual zone served by external name servers. To do this, at the zone properties screen (Domain name > DNS), click the  Disable icon. Turning the DNS service

off for the zone will refresh the screen, so that only a list of name servers remains.

### Note

The listed NS records have no effect on the system. They are only presented as clickable links on the screen to give you a chance to validate the configuration of the zone maintained on the external authoritative name servers through the control panel.

If you wish to validate the configuration of the zone maintained on the authoritative name servers:

1. Add to the list the entries pointing to the appropriate name servers that are authoritative for the zone: click Add, specify a name server, and click OK. Repeat this for each name server you would like to test. The records will appear in the list.
2. Click on the records that you just created. Plesk will retrieve the zone file from a remote name server, and check the resource records to make sure


that domain's resources are properly resolved. The results are interpreted and displayed on the screen.

## Managing Mail

Using Plesk, you can create and manage e-mail boxes for individuals within a domain, or your customers (domain owners) can manage the e-mail accounts via domain self-administration. 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 administrators, 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:




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/disallow access from the control panel to web-based mail interface (Webmail), and specify the settings for handling incoming mail addressed to the users not existing at this domain:

1. Click  Preferences
2. For the mail to nonexistent users, you can choose any of the following options: Bounce with message, Forward to address, or Reject.
  - Select the Bounce with message option to have the mail returned to sender with the bounce message you specify.
  - Select the Forward to address option to have the mail forwarded to the address you specify.
  - Select the Reject option to have the mail rejected during SMTP session without queueing for delivery. This option can save bandwidth and server resources.
3. If you wish to use a web-interface for working with mailboxes in this domain, select the WebMail checkbox. You will then be able to access the web interface by specifying the URL: `webmail.domain_name.tld` in the web browser, or by clicking the WebMail icon on the Mail Name Properties screen.
4. Click OK to submit the settings.

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 English

Interface skin WinXP Blue

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 specify 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, click 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 whether mail user is allowed to access the control panel for managing his/her account,
-  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.

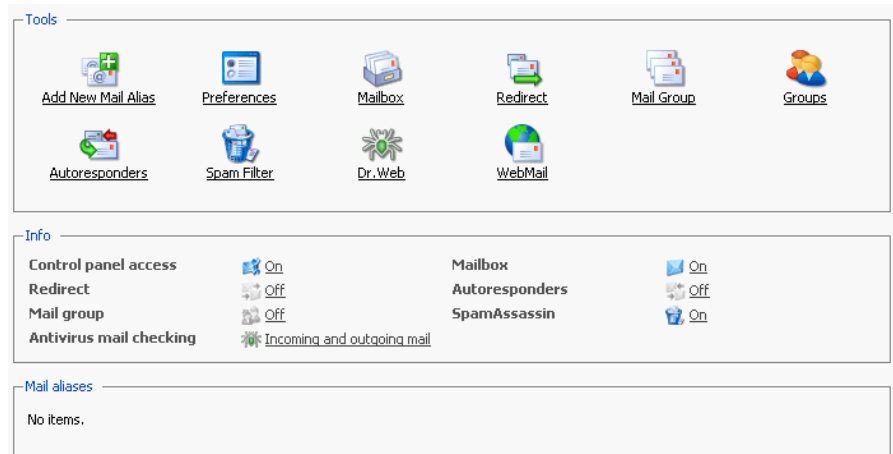
To switch to displaying the mail aliases for the mail names in the list, click the Show Aliases button, to hide them use the Hide Aliases button.

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:



- 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.

- To edit the mail name preferences, click



Preferences.

- To edit mailbox quota and enable spam filtering, click



Mailbox.

- To set up mail forwarding - a redirect, click



Redirect.

- To enable a mail group service for the mail name and add new members to the mail group, click



Mail Group.

- To manage mail groups membership, click




Groups.


- 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. You can enable forwarding of incoming messages that match the autoresponder conditions. To do this, specify an e-mail address in the appropriate input box.
5. In the Conditions group, you can determine whether a given autoresponder should respond when specific words are found in the subject line or body of the incoming e-mail message, or you can set it to respond to any e-mail messages directed at this mail name.
6. By default, the subject line of incoming e-mail will be inserted into the automated reply. To use a custom subject, type it into the Reply subject input box.
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 have an option to specify the autoresponder message format (plain text or HTML) and encoding (UTF-8 is recommended). If you use HTML tags in your auto-reply message, you should select the HTML option.
9. You can enter text to be included into the autoresponder in the Reply with text field.
10. 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.
11. You can limit the number of automated responses per day to the same e-mail address. To do this, enter the desired number in the respective input box. The default setting is to respond not more than 10 times in one day to the same e-mail address.

12. 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.
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.

## Training Spam Filter

You can train your mail filters on actual messages you receive. To do this:

1. Click the Training icon in the Tools group. All e-mail messages from your mail box are presented on the screen. Each message is accompanied by an icon in the left column, which tells if a message is recognized as spam - , non-spam - , or not recognized at all - . If you have already trained your spam filter on a message and the results were recorded in the Bayesian database, an icon  is shown in the right column.
2. To mark a message as spam, select the corresponding check box and click 'It's Spam!' To mark a message as not spam, select the corresponding check box and click 'It's Not Spam'. To remove any information on a given message from the spam filter database, select the corresponding check box and click 'Forget It'.

**i Note:**

to view a message source, click the respective message subject. To remove a message from your mail box, select the respective check box and click Remove Selected.

- When finished with training, click Up Level to return to the previous screen.

A spam filter database can become corrupt, or the data inside it unreliable. This may happen when many non-spam e-mails have been learned as spam, or vice versa, and the spam filter subsequently produces incorrect results. If the spam filter appears to be working incorrectly, clear its database and start afresh. To do this, click the 'Clear Spam Filter Database' button.

## Enabling Antivirus Filtering For Mailboxes

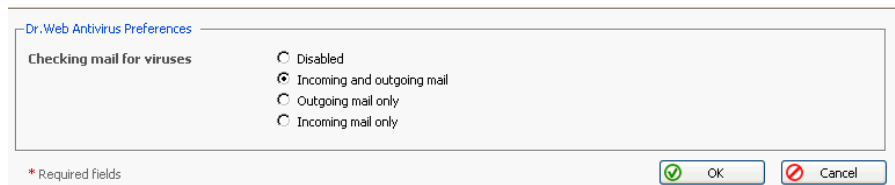
For a user's mailbox you can enable the antivirus scanner to work in one of the following modes: checking incoming and outgoing mail, checking outgoing mail only, and checking only incoming mail.

When antivirus scanning is enabled, all e-mail messages containing viruses are intercepted.

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

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

preferences page will appear:



Dr.Web Antivirus Preferences

Checking mail for viruses

Disabled  
 Incoming and outgoing mail  
 Outgoing mail only  
 Incoming mail only

\* Required fields


OK Cancel

- 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  Mail icon

at the Domain administration page, then select the Mailing lists tab 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 3.3. The Mailing lists service/mailling lists status icons**



Icon	Meaning
<b>The Mailing lists service status</b>	
	means that the Mailing lists service is activated

Icon	Meaning
<b>The Mailing lists service status</b>	
	means that this mailing list is presently deactivated.
<b>The mailing list status</b>	
	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 Administrator Account


If you wish to allow a domain administrator or domain owner to use Plesk control panel for managing his/her domain, you should create a domain administrator account in Plesk. When a user is logged in to a domain administrator 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 administrator account, a user should specify his/her domain name as the control panel login name.

### To set up the Domain Administrator account:


1. Click the  Domain Administrator icon at the Domain administration page. The Domain Administrator Account Settings page appears.
2. To allow access to the control panel for the domain administrator, select the Allow domain administrator access checkbox, enter and confirm the password.
3. Set the visual preferences for the domain administrator's environment: language, skin, number of entries displayed in various control panel object listings per page, and limit the button label length, if desired.
4. Select the Allow multiple sessions checkbox to allow several simultaneous sessions under the same domain administrator'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 administrator's 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:




**Databases for domain domain.com**  Up Level


**Tools**

 [Add New Database](#)

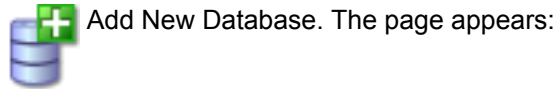
**Databases**

Databases (1)

 Search  Show All  Remove Selected

T Name ▲	☐
 base1	☐

- 2.



**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:

**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:

**The database user addition for database2 database** [Up Level](#)

[Database user](#)

Database user name

Old password NONE

New password

Confirm 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:

**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](#) [Remove Selected](#)

Name ▲	<input type="checkbox"/>
user2	<input type="checkbox"/>

2. To add database users to the selected database, click  Add New


Database User. The Database user addition page appears:

**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.

## Managing Java Applications

Plesk supports deploying and managing Java 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 Java Applications Management functions.






At this page you can activate/deactivate the Tomcat service that serves the Java applications, upload the application archive files (.WAR files) and remove them, start/stop/restart applications, and access them.

### **IMPORTANT**

Users can only manage the Java application through Plesk interface. Managing them through the Tomcat manager was disabled in order to maintain coherence of Plesk Tomcat configuration.

The status of Tomcat service and the status of an application are represented by the following icons:

**Table 3.4. The Tomcat service/application status icons**

Icon	Meaning
<b>The Tomcat service status</b>	
	means that the Tomcat service is activated
	means that the Tomcat service for the domain is presently deactivated.
<b>The application status</b>	
	means that the application is activated
	means that this application is presently deactivated and inaccessible.
	means that 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 Java



applications also change their status to 'inaccessible' while all inactive applications remain unchanged.

Activation of the Tomcat service enables access to active applications.

### **i** 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:

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

## Uploading Java web application archive files

To upload a new Java application archive file, follow these steps:

1. Click  Add New Java Application.
2. Select the 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.

## Restarting web applications



You can restart the installed Java applications directly from the control panel. In order to stop, start or restart an application follow these steps:

1. Select the application at the applications list on the Java Applications Management page.

2. To start an application: click the  icon (Start the web application).

To stop an application: click the  icon (Stop the web application).

To restart an application: click the  icon (Restart the web application).

The current application state will be indicated with an icon:  (ON) for a web application running, and  (OFF) for a web application stopped.

## Accessing Java applications

An application can be accessed simply by clicking on its name in the Tomcat web applications list. The selected application's interface will open in a new browser window.

### NOTE

If an application is disabled, it cannot be accessed, and therefore, the link to it is also disabled.

## Removing applications

You can remove one or several applications at the same time. To remove an application:


1. In the list of applications, select a checkbox corresponding to the application you wish to remove.
2. Click Remove Selected.
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](http://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:


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:

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.

4. To add a web user, click  Add Web User. You will be taken to the

Web User Configuration page:

**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 contain the login name as its part.

- 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:

Subdomains of domain domain.com [Up Level](#)


Tools

 [Add New Subdomain](#)


Subdomains


Subdomains (1)

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

Subdomain name ▲	Login	
<a href="#">dominio_domain.com</a>	ftlogin	 <input type="checkbox"/>

To create a subdomain, follow these steps:

1. Click  Add New Subdomain. The Subdomain creation page will open:

**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


For storing sensitive data, you can create password-protected directories within domains on physical hosting. 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:



**Protected directories for domain domain.com** Up Level



Tools

 [Add New Directory](#)

Protected directories

Protected directories (1)

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:

**Create new protected directory on domain domain.com** Up Level

Preferences

Directory name	<input type="text" value="/directory2"/>
Directory location	<input checked="" type="checkbox"/> Non-SSL <input checked="" type="checkbox"/> SSL
Header Text	<input type="text" value="My private folder"/>

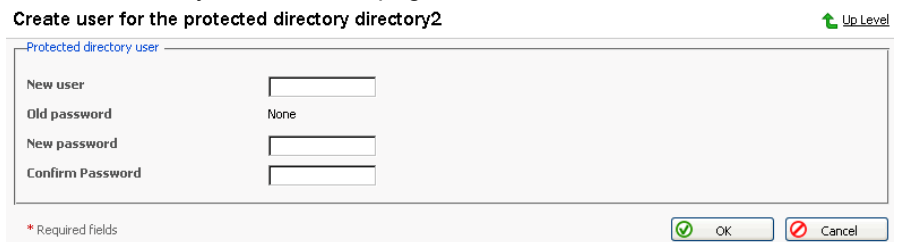
\* Required fields

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.
5. 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.

### 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:

- 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 you 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. You 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.



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, select OK to submit all changes.

## 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:

**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	
Jan 30, 2004 04:07 AM	<a href="#">access_log</a>	0 B	<input type="checkbox"/>
Jan 30, 2004 04:07 AM	<a href="#">access_log.processed</a>	294 B	<input type="checkbox"/>
Jan 30, 2004 04:07 AM	<a href="#">access_ssl_log</a>	0 B	<input type="checkbox"/>
Jan 29, 2004 04:07 AM	<a href="#">access_ssl_log.processed</a>	0 B	<input type="checkbox"/>
Jan 29, 2004 07:46 AM	<a href="#">error_log</a>	1.08 KB	<input type="checkbox"/>
Jan 30, 2004 05:03 AM	<a href="#">error_ssl_log</a>	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:

**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.

## Scheduling Crontab Tasks

To access the crontab management functions, click the  Crontab

Manager icon on the Domain administration page. The Crontab management page will open:

**Crntab tasks** [Up Level](#)

**Tools**

 [Add New Task](#)

**Preferences**

Show Crontab of:

Send Crontab messages to address:

**Tasks**

Crntab tasks (1)

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

S	M	H	DM	M	DW	Command	
	0	12	1	1	1	<a href="#">backup_httpdocs.sh</a>	<input type="checkbox"/>

On this page, you can view scheduled tasks of various system users, set the e-mail address for the crontab output messages delivery, 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:

 **Editing the Crontab task of ftplogin**  Up Level

**Tools**

 [Disable](#)

**Task**

Minute \*

Hour \*


Day of the Month \*


Month \*

Day of the Week \*

Command \*

\* Required fields

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 7 (0 or 7 for 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.

## 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	
	<a href="#">anon_ftp</a>	4.00 KB	Jan 28, 2004	ftplugin	psaserv	750	
	<a href="#">bin</a>	4.00 KB	Jan 28, 2004	root	psaserv	755	
	<a href="#">cgi-bin</a>	4.00 KB	Jan 28, 2004	ftplugin	psachn	755	
	<a href="#">conf</a>	4.00 KB	Jan 30, 2004	root	psaserv	750	
	<a href="#">error_docs</a>	4.00 KB	Jan 28, 2004	ftplugin	psaserv	755	
	<a href="#">httpdocs</a>	4.00 KB	Jan 30, 2004	ftplugin	psachn	751	
	<a href="#">httpsdocs</a>	4.00 KB	Jan 30, 2004	ftplugin	psachn	751	
	<a href="#">pd</a>	4.00 KB	Jan 30, 2004	root	psaserv	750	
	<a href="#">private</a>	4.00 KB	Jan 28, 2004	ftplugin	root	700	
	<a href="#">statistics</a>	4.00 KB	Jan 28, 2004	root	psaserv	550	
	<a href="#">subdomains</a>	4.00 KB	Jan 30, 2004	root	psaserv	755	
	<a href="#">web_users</a>	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's source, click the corresponding  icon. Edit the contents of file, and click Save to save the changes made.

Note that File Manager automatically detects page encoding, and if it does not detect it properly, please select the proper encoding manually and click Change Encoding to reload the page view.

To restore the original file and discard your changes, click Reset.

To save the file and quit the editing mode, click OK. If you wish to leave the editing mode and discard the unsaved changes, click Cancel.

- To edit a file in the built-in visual editor, click the corresponding  icon.

Edit the contents of file, and click Save to save the changes made.

To view file in another encoding, select the encoding in the drop-down box and click Change Encoding to reload the page view.

To switch to the visual editing mode (design view), click the Design tab. To switch to the source code editing mode, click the HTML tab.

To save the file and quit the editing mode, click OK. If you wish to leave the editing mode and discard the unsaved changes, click Cancel.

## 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 to the left of the site application name indicate the site application usage rules defined by the administrator:

-  - free of charge;
-  - commercial, available under certain conditions (i.e. upon purchase).

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 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, or on the administration pages of all domains, managed by you.

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 the Mambo Content Management Software

Plesk is shipped with Mambo software intended to simplify the process of creating and deploying web sites. In order to use it, 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 Mambo CMS icon for the first time. After the application is installed and configured, use the



Mambo CMS 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



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. To create a multivolume backup, select the Create a multivolume backup check box and specify size of each volume in megabytes.
7. 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 from the local machine to the server, click Upload, specify file location using the Browse button, then click Upload. To upload a multivolume backup, specify the first part of the volume, then click the "Specify the next volume" link, and specify the next volume. Repeat it until you have specified all volumes of the backup. When finished, 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. To create a backup file and store it in the repository, select the "create backup file and store in local repository" option.


To create the backup file and store it on the remote FTP server, select the "create the backup file and store on remote FTP server" option.

To create a backup file and download it to your local machine without storing it in the backup files repository, select the "do not store the backup file in repository, only download it" option.

3. To create a multivolume backup, select the "Create a multivolume backup" check box and specify size of each volume in megabytes.
4. If you have chosen to save your backup file to remote FTP server:
  - specify the FTP server name in the "FTP server" input box
  - type the name of the directory on FTP server, where the domain backups should be stored in the "Path to backup files repository on FTP server" input box
  - enter the FTP server login in the "FTP Login" input box
  - enter the FTP password in the "FTP Password" input box
5. Type in your comments or backup file description in the "Comments" text field.
6. If you wish to receive notifications of backup procedures start and completion, select the "Notify by e-mail" check box and specify the e-mail address.

7. 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.


**i 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 

## Renaming Domains

If required, you can rename a domain name directly through the control panel. However, for the new (renamed) domain to be properly resolved on the Internet, you must register the new name with a domain registrar and make sure that the name servers are properly specified.

Once you have changed a domain name, you should obtain a new SSL certificate, if SSL support is required.

**! Important!**

Renaming a domain may result in problems with the software running on that domain.


To change the domain name and requirement for www prefix, follow these steps:

1. At the domain administration page, click the Domain administrator icon.
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. Edit the domain name as desired, and click OK.

## 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. On your Home page, select the domains, whose settings or limits you wish to modify by checking the corresponding checkboxes.
2. 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.
3. To edit limit settings for a particular resource type:
  - 3.1. 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
  - 3.2. Then specify the value of the new resource limit in the corresponding input field.
  - 3.3. 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.

4. To change the hosting-related settings, select **Do not change**, **Enable** or **Disable** radio button for the corresponding type of setting. You can edit 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

### **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.

5. 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 users in a domain; you can choose to **Bounce with message**, **Forward to an e-mail address**, or **Reject**
6. 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

7. 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. On your Home page, select the domains that you wish to remove by checking the corresponding checkboxes.
2. Click Remove Selected. The Removal confirmation page appears.
3. Confirm removing, and click OK.

## Managing Domains via Remote XML Interface

If your provider granted you permission to manage domains through Plesk XML interface, you may want to take advantage of automated creation of domains in Plesk as your customers purchase domain names and hosting plans through your web site. To implement such mechanisms, you should possess a strong knowledge of programming languages, and be experienced in web application development.

To learn more about using Plesk XML interface (also referred to as Plesk API RPC), please visit

[http://download1.sw-soft.com/Plesk/Plesk7.5/Doc/plesk-7.5r-sdk-html/docs/plesk\\_agent/ch01.html](http://download1.sw-soft.com/Plesk/Plesk7.5/Doc/plesk-7.5r-sdk-html/docs/plesk_agent/ch01.html)

### Note

Plesk client accounts can be authorized to perform only the following operations through Plesk API RPC: creating and removing domains in Plesk, modifying miscellaneous domain preferences and hosting services, retrieving information on domains.



---

# Appendix A. 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
- two 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](http://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.