SWsoft

PLESK 7.5 FOR WINDOWS

ADMINISTRATOR'S MANUAL

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

Table of Contents

Chapter 1. About Plesk 7.5

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

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

The perfect solution for both dedicated server and shared domain management, Plesk 7.5 deploys and configures all of the systems you need to run a webserver. Tiered login levels provided encrypted and secure access to for system administrators and domain resellers as well as their clients and domain owners.

Plesk 7.5 Capabilities

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

- System Management
  - Hardware Reboot and Shutdown
  - IP addresses management
  - Use of firewall
  - System time setting
  - Server level statistics retrieval
  - Server support request submission
- Services Management
  - Manage system services and schedule tasks
  - Set up server-wide mail limits, mail relay capabilities and mail blockers
  - Enable support for external mail abuse prevention system (MAPS)
  - Enable and configure the integrated SpamAssassin mail filter
  - Set up DNS server default zone template
  - Manage SSL certificates repository
  - Manage the Databases admin account
  - Add value to the hosting services offered: Application Vault houses various useful application packages that can be easily deployed on any domain hosted on server.
  - Enable support for ColdFusion scripting
  - Use skeletons for defining the structure of new virtual hosts

- Control Panel Management
  - Co-brand using company logo and link
  - Set up control panel access security and adjust sessions time settings
  - Allow discounted domain registration and SSL certificate purchasing
  - Customize control panel interface appearance, select language, skin, paging options, and add customizable buttons.
  - Adjust the server-wide statistics calculation to meet your requirements
  - Set up the notification system, which will inform you of the ongoing system events
  - Set up system-wide client and domain templates intended to simplify new client account and domain creation procedures with automatic assignment of all necessary restrictions
  - Log various actions performed within the system

- Centralized management of multiple Plesk enabled servers by means of Master feature

- User sessions management

- Integrated Help Desk solution

- Additional security measure allowing to restrict access to control panel from specific IPs.
- Client Management
  - Create, edit, and delete client accounts
  - Allow reseller capabilities
  - Set up various limits for client accounts.
  - Retrieve statistics and reports on resource usage
  - Perform group operations on client accounts
- My.Plesk.Com Service Management
  - Manage access to additional server and domain tools purchasing
- Domains and hosting accounts management
  - Create, edit and delete domains and hosting accounts
  - Set up web and ftp server allowances, support for scripting capabilities
  - Set up domain level resource usage limits
  - Manage mail, web and domain user accounts and services
  - Manage DNS zones
  - Backup and restore domain data
  - Manage mailing lists
  - Handle log files and log rotation
  - Operate files and directories using file manager
  - Create site content using Site Builder
  - Deploy ste applications and java servlets on domains

Additional Benefits

Ease of Use

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

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

Security

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

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

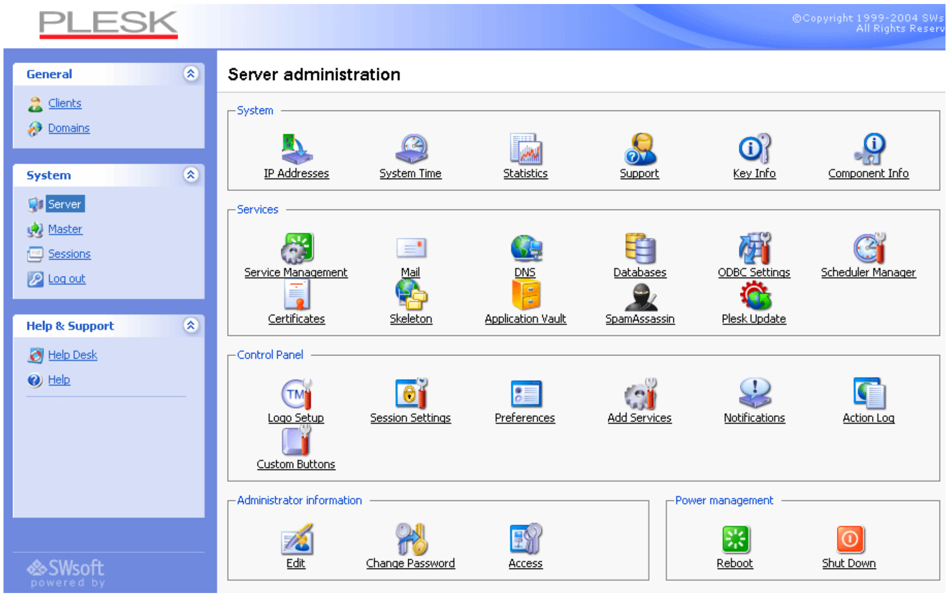
- Plesk provides additional security measures, allowing the administrator to restrict control panel access from certain IP addresses.

Plesk Interface Specific Features

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

Navigation

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



- The Clients shortcut opens the list of client accounts, and gives you access to user management functions.
- The Domains shortcut opens the list of domains hosted on server, and allows you to administer them.
- Using the Server shortcut you access the server administration functions.
- The Master function is used for centralized management of Plesk enabled servers.
- The Sessions shortcut is used for managing currently active user sessions.
- The Log out shortcut ends your control panel session.
- The Help Desk shortcut is used for accessing the Help Desk.

Pathbar

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

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

Help

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

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

Working with Lists of Objects

You may have considerable number of objects within Plesk system. In order to facilitate working with the different lists of objects (for example, lists of domains, client accounts, etc.), the special tools are provided: search and sorting.

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

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

Chapter 2. Configuring Your System

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

Configuring Access Policy

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

1. Allow access from all IP's except those added to the list.

2. Deny access from IP's, which are not in the list.

Notes on access restriction policies

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

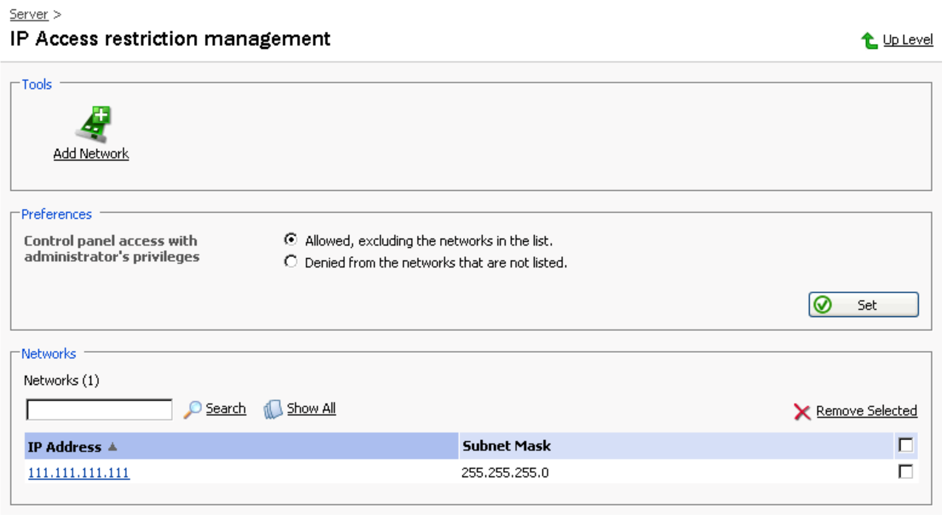
When you attempt to switch to the mode 2 with empty list, you are warned of impossibility of such action.

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

Managing control panel access

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

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



Server >

IP Access restriction management

Up Level

Tools

Add Network

Preferences

Control panel access with administrator's privileges

● Allowed, excluding the networks in the list.

○ Denied from the networks that are not listed.

Set

Networks

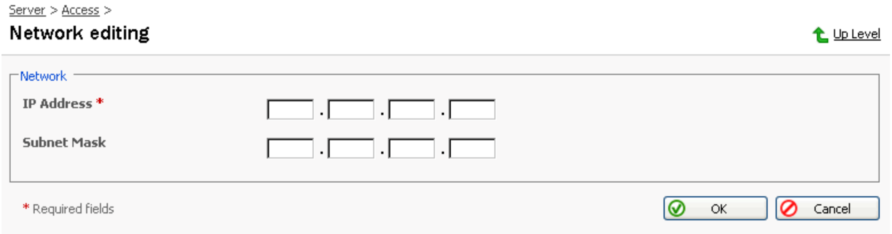
Networks (1)

Search Show All Remove Selected

IP Address ▲	Subnet Mask	□
111.111.111.111	255.255.255.0	□

To add a network to the list:

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



Server > Access >

Network editing

Up Level

Network

IP Address * ___ . ___ . ___ . ___

Subnet Mask ___ . ___ . ___ . ___

* Required fields

OK Cancel

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

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

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

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

IMPORTANT

By default Plesk allows multiple simultaneous sessions for several users logged into the control panel using the same login and password combination. This feature might be useful when delegating the management functions to other users or in case if you accidentally close your browser without logging out, thus becoming unable to log in again until your sessions expires. Being the administrator you can choose to disable this capability.

To disable multiple sessions under administrator's login:

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

Enabling Plesk Firewall

Firewall is a protection measure aimed at prohibiting specific incoming network connections that may be used to compromise your server.

Plesk Firewall operates on the base of rules, which specify parameters of connections, which are to be blocked or passed through.

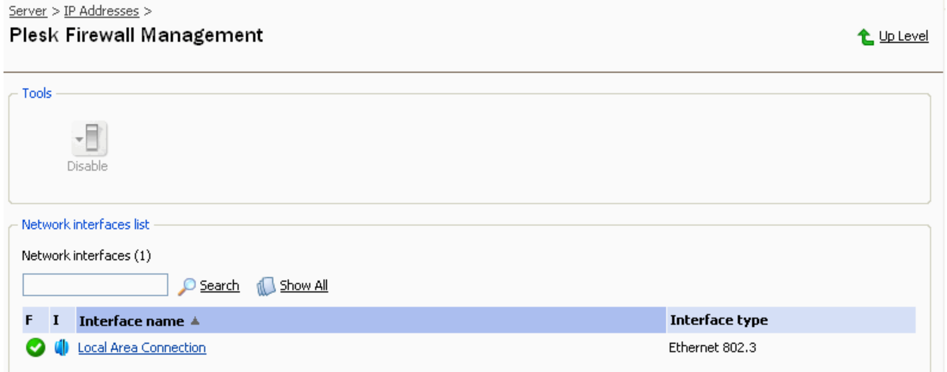
It filters only incoming IP connections for TCP and UDP protocols. All outcoming connections are allowed. Each rule controls filtering only for one specific network interface (adapter).

Some rules for widespread protocols are predefined, and you can only enable or disable them.

Note, that if some protocol is not controlled by some rule, its messages are filtered too. For example, if you do not have a rule for protocol XYZ, all incoming messages sent via this protocol will not be passed by Plesk Firewall.

This behavior has an exception, Plesk Firewall does not filter both incoming and outcoming messages of ICMP protocol, regardless of message's type.

To start setting up the firewall, click the Server > IP Addresses > Firewall icon.The page allows seeing and changing status of firewall protection for the network interfaces installed on the server.



Plesk Firewall Management

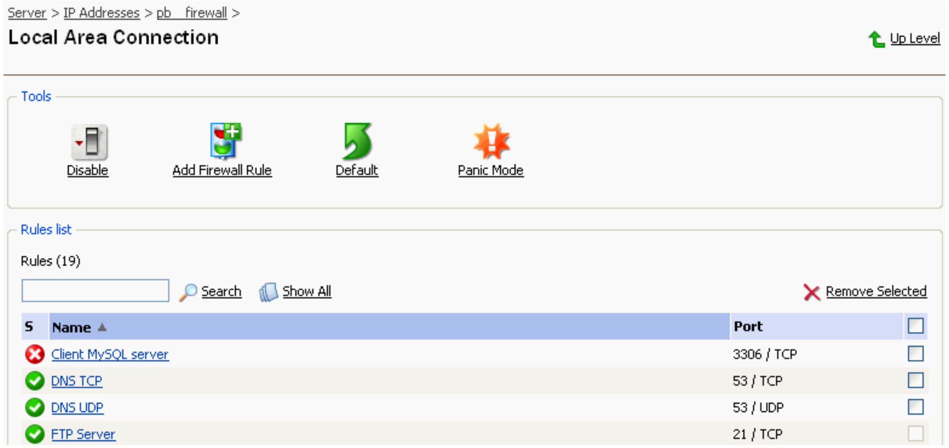
Network interfaces (1)

F	I	Interface name ▲	Interface type
✓	◐	Local Area Connection	Ethernet 802.3

This page has a list of all network interfaces on server accompanied by icons symbolizing status of firewall protection (F column), status of network interface connection activity (I column), and textual fields for name and type of network interface.

Click the icon in the F column to switch the status of firewall protection for the corresponding network interface.

Click the interface name for opening a page, which gives you precise control over firewall rules for this interface.



Server > IP Addresses > pb firewall >

Local Area Connection

Up Level

Tools

Rules list

Rules (19)

S	Name ▲	Port	□
✗	Client MySQL server	3306 / TCP	□
✓	DNS TCP	53 / TCP	□
✓	DNS UDP	53 / UDP	□
✓	FTP Server	21 / TCP	□

A rule has a symbolic name and consists of port number and protocol name for the connection to be filtered or passed through.

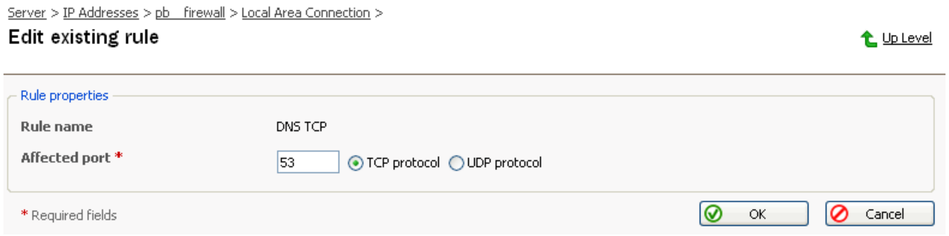
The Default button restores the original Plesk Firewall configuration by deleting all user-defined rules and setting all predefined rules in pass-through state.

The Panic button enables special mode to protect the server from unknown worms, etc. It closes the box as tightly as possible, disabling all incoming and outgoing connections except for accessing Plesk Control Panel and Remote Desktop administering. Note that the panic mode disables access to the client's sites; it is only recommended to use it when there are no other options left, e.g. if the server was compromised.

The Enable/Disable button allows controlling firewall activity on the network interface you selected before entering this page.

The list at the bottom of the page contains all firewall rules, registered for use on the selected network interface. Each rule has an icon in the S column, which indicates the state of this rule, whether it is enabled or disabled. When the icon is green, Plesk Firewall does not filter messages of the protocol, corresponding to the rule, passing them through to concrete programs using this protocol for communication. When it is red, firewall rule is 'active', prohibiting messages matching the rule to pass through. To edit parameters of an existing rule, click on its name.

To add your own rule, click the Add Firewall Rule button. A page will open where you have to specify rule's properties. To edit properties of an existing rule, click on its name. The screen of editing an existing rule is very similar to the screen of adding a new rule, except that it does not allow renaming the rule.



Server > IP Addresses > pb_firewall > Local Area Connection >

Edit existing rule

Rule properties

Rule name DNS TCP

Affected port * 53 ● TCP protocol ○ UDP protocol

* Required fields

If you are adding a new rule, provide its name in the Rule name field. It is only for your reference and convenience. Next, you should choose what type of network protocol you want to create rule for, this can be either TCP or UDP protocols. Finally, type number of port, which you want to monitor in the Affected port field. The exact port numbers depend on the configuration of the system services on your system, e.g. web server, FTP server etc.

Click the OK button to submit your changes or Cancel to return to the previous page without submitting anything.

Setting Session Security Parameters

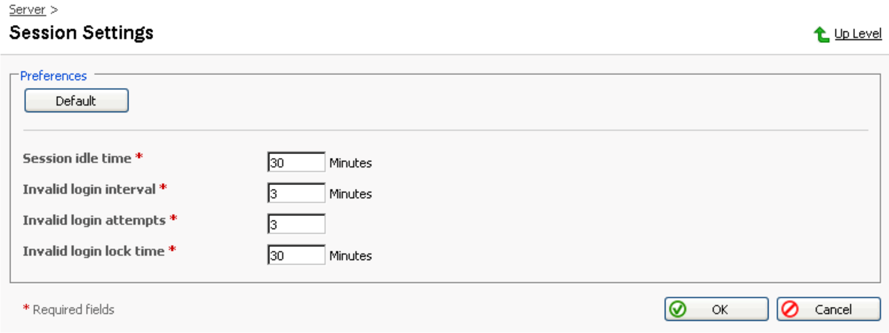
You can set the following parameters for any user session in Plesk:

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

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

1. Select the Session Settings icon on the Server administration

page. The Sessions Settings page appears:



Server >

Session Settings

Up Level

Preferences

Default

Session idle time * 30 Minutes

Invalid login interval * 3 Minutes

Invalid login attempts * 3

Invalid login lock time * 30 Minutes

* Required fields

OK Cancel

2. Adjust the required settings as desired.

3. Click OK to submit.

To reset the session parameters, click Default.

Managing IIS Application Pools

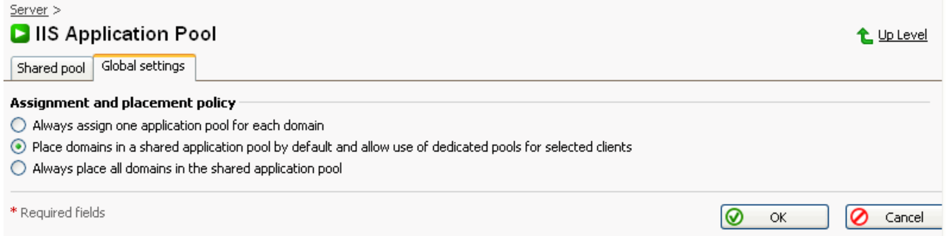
Choosing Application Pools Assignment Policy

One of the new features of the IIS 6.0 web server is worker process isolation mode where each web site has the possibility to allocate a separate process pool for execution of its web applications. This way, malfunction in one application will not cause stopping of all the others.

Plesk has a shared application pool; each domain can use dedicated application pool if administrator and client policy permit this. Plesk has three modes of working:

- Always assign one application pool for each domain
- Place domains in a shared application pool by default and allow use of dedicated pools for selected clients
- Always place all domains in the shared application pool

To choose the application pool assignment policy, go to the Global Settings tab and choose one of the three aforementioned strategies.



Server >

IIS Application Pool

Up Level

Shared pool | Global settings

Assignment and placement policy

○ Always assign one application pool for each domain

● Place domains in a shared application pool by default and allow use of dedicated pools for selected clients

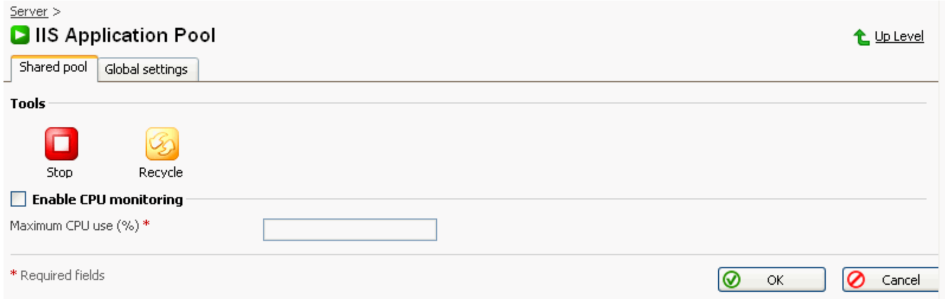
○ Always place all domains in the shared application pool

* Required fields

OK Cancel

Configuring Shared Pool

The Shared pool tab allows controlling the shared application pool.



You can either Start/Stop the Shared Application Pool functioning or Recycle the pool. When an Application Pool is stopped, all web applications which use it are stopped too. Therefore users will not be able to use functions given by those application.

The Recycle button stops all the applications running in the application pool and starts them again. This can be handy if some applications have memory leaks or become unstable after working for a long time.

Also, you can set the maximum amount of CPU resources this application pool can use. In order to do this, check the Enable CPU monitoring checkbox and enter your percent limit in the provided field below.

Enabling Application Pool Management for Clients

If the second mode of global application pools assignment policy was selected ("Place domains in a shared application pool by default and allow use of dedicated pools for selected clients"), you need to set up, which clients will be able to use dedicated pools.

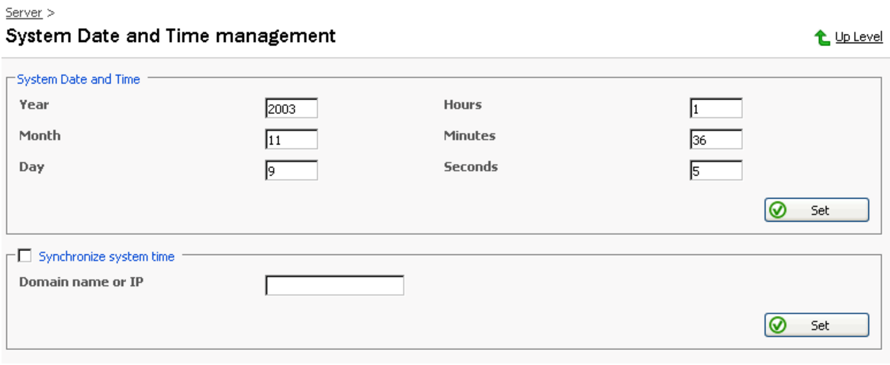
To do this, go to the client's Limits page and edit the Maximum number of IIS application pools edit field or set the Unlimited checkbox. Now you or client can enable using the dedicated pool for a specific domain by going to the Domain Administration Page > Setup page and setting the Use dedicated pool checkbox there.

If a client allowed to use maximum N of dedicated application pools, then first N domains of this client, which enable the checkbox will be given dedicated pools. After the limit on number of application pools is reached for the client, its domains will use the shared application pool.

Setting System Date and Time

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

1. Click the System Time icon on the Server administration page. The system date and time management page will open:



Server >

System Date and Time management

System Date and Time

Year	2003	Hours	1
Month	11	Minutes	36
Day	9	Seconds	5

□ Synchronize system time

Domain name or IP

2. Edit the time and date settings as desired, and click Set.

3. To synchronize your server time with that of a server running the Network Time Protocol, select the Synchronize system time checkbox. Once this checkbox is checked, this function is enabled.

4. Enter a valid IP address or a domain name and click Set.

NOTE

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

Setting Up Server-wide Mail and Spam Filtering

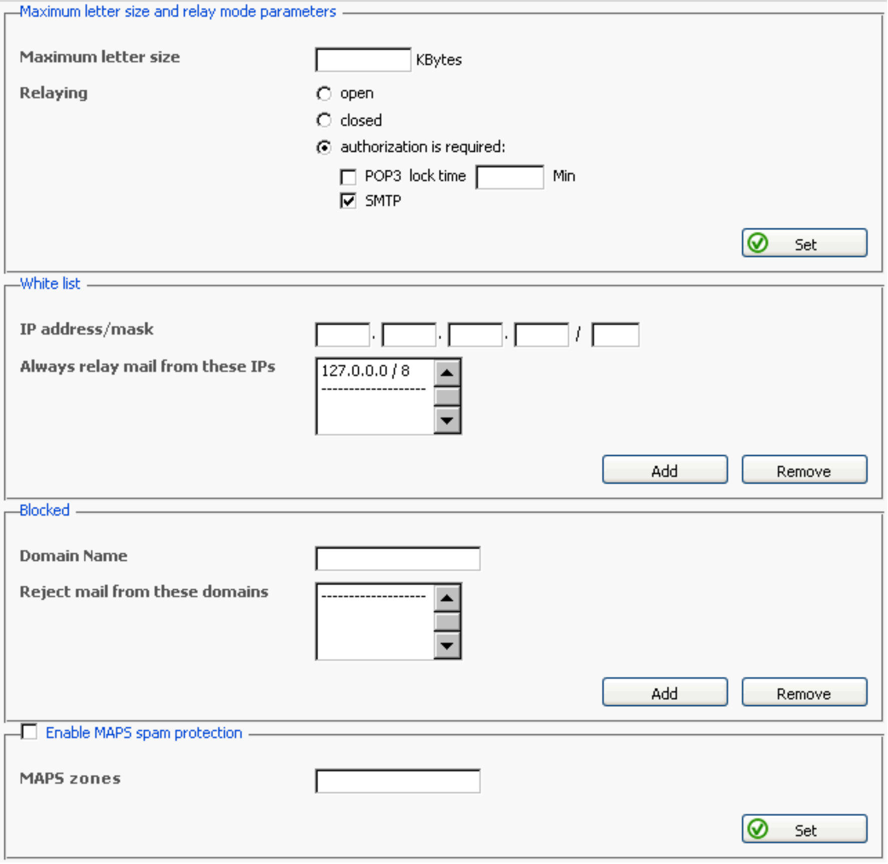
Configuring Mail

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

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

In order to set up the mail system, follow these steps:

1. Click the Mail icon on the Server administration page. The Mail system management page will open:



Maximum letter size and relay mode parameters

Maximum letter size [ ] KBytes

Relaying
○ open
○ closed
● authorization is required:
□ POP3 lock time [ ] Min
☑ SMTP

White list

IP address/mask [ ] . [ ] . [ ] . [ ] / [ ]

Always relay mail from these IPs
127.0.0.0 / 8

Blocked

Domain Name [ ]

Reject mail from these domains

□ Enable MAPS spam protection

MAPS zones [ ]

2. To set the maximum letter size allowed on the server, click in the Maximum letter size text box and enter the desired value in Kilobytes. Click Set to submit.

3. To set the mail system relay mode, select a corresponding radio button. For relaying that requires authorization, select the Authorization is required radio button. You must then select an authorization type, which can be POP3, SMTP or both.

   - POP3 - Click in the checkbox next to POP3 to enable this mode of authorization. You must then set the lock time; the default setting is 20 minutes.

   - SMTP - Click in the checkbox next to SMTP to enable this authorization mode.

   Click Set to submit.

4. To add an IP address/mask to the White List, type in the appropriate IP address and mask in the fields provided. Click Add to submit. The address selected will appear in the IP list.

5. To remove an IP address/mask from the White List, select the IP address you wish to delete from the IP list. Click Remove.

6. To add a mail blocker, click in the text box in the Domain Name field and enter the domain name from which you want the mail to be rejected. Click Add to submit. The domain you selected will appear in the list of blocked domains.

7. To remove a mail blocker, select the domain you wish to remove from the list of blocked domains. Click Remove.

8. To enable the external Mail Abuse Prevention System (MAPS) select the Enable MAPS spam protection checkbox, specify the MAPS zone in the MAPS zone(s) field and click Set.

Configuring the Server-wide Spam Filter

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

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

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

To access the server-wide spam filter settings, click the SpamAssassin icon on the Server administration page. The Spam filter configuration page will open.

1. To enable filtering mail on the server, check the 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.

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

1. In order to activate/deactivate the option of modifying the spam messages subject, check the Modify spam mail subject;

2. To change the text of the string, click into the input field and enter the new text;

3. Click Set to save the changes.

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 patters, using wildcards (‘*’, e.g.: entry ‘*@spammers.online.com will cause all messages coming from the domain spammers.onine.com be marked as spam, regardless of what the exact mail name is).

NOTE

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

1. Enter the E-mail address or pattern into the Email pattern input field;

2. Click Add to add the new entry to the black list.

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

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

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

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

Setting Up Database Administrator's Account

To set up the database server connection and/or change administrator's login and password follow these steps:

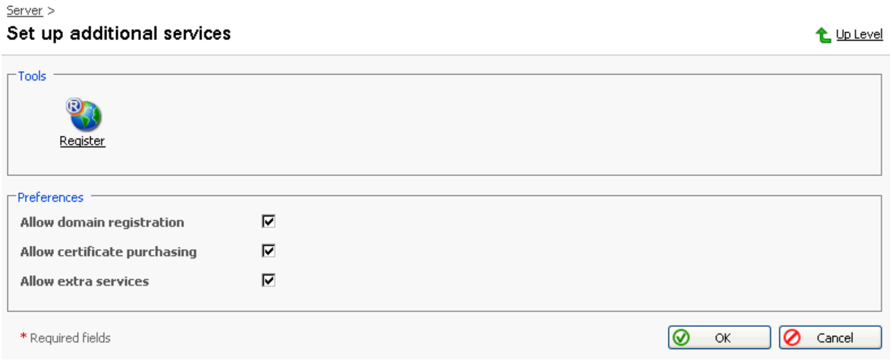
1. Click the Databases icon on the Server administration page.
2. Type in the server name, administrator's login and password.
3. To change the password for an existing database user, click Change Password.
4. Click OK to submit.

Registering Your Server and Managing Access to Additional Services

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

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

1. On the Server administration page click Add Services. The Additional Services Setup page appears:



Server >

Set up additional services

Tools

Preferences

Allow domain registration ☑

Allow certificate purchasing ☑

Allow extra services ☑

* Required fields

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

To register your server with MPC, follow these steps:

1. Click Register. The MPC Login page will open in a new browser window.
2. Enter your Login name and Password in the fields provided, click Log In to enter. You will be taken to the page My Commissions, and prompted to register your server.
3. Click the button Register Server Now. The Server Registration page will open displaying your Plesk software license key number and your IP address.
4. Click OK to confirm your server registration.

Managing Control Panel SSL Certificates

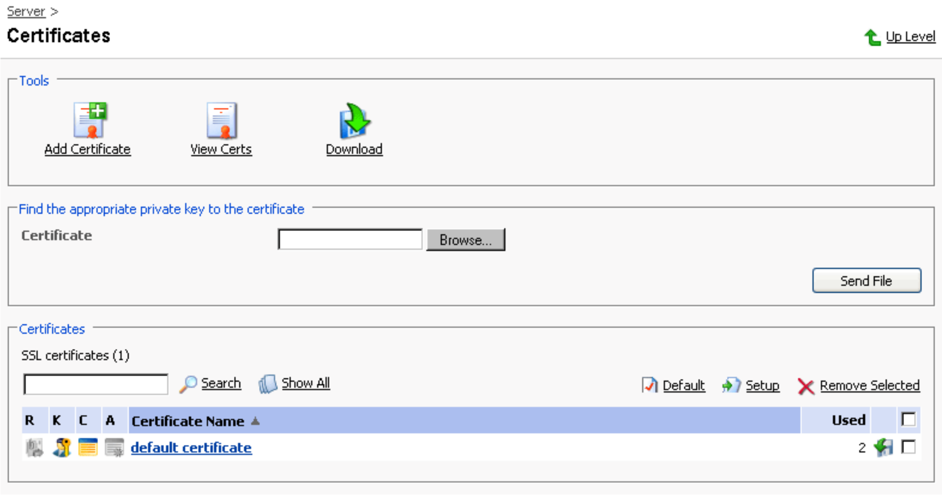
An SSL certificate represents a set of rules used when exchanging encrypted information between two computers. Certificates ensure secure communications; this is especially important when handling e-commerce transactions and other private transmittals. Only authorized users can access and read an encrypted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

Notes on Certificates:

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

Accessing the Control Panel SSL Certificates Repository

To access the Control Panel certificates repository, click the Certificates icon at the Server administration page. The certificates repository page will open displaying the list of available certificates:



Certificate

SSL certificates (1)

R	K	C	A	Certificate Name ▲	Used	□
				default certificate	2	□

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

Uploading a certificate file with finding the appropriate private key

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

Changing certificate name

To change a certificate name follow these steps:

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

Viewing purchased certificates

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

Downloading a certificate from repository to the local machine

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

Removing a certificate from repository

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

Downloading the certificate currently installed at the Control Panel

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

Setting the Control Panel certificate

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

Adding a certificate to the repository

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

Generating a self-signed certificate

To generate a self-signed certificate follow these steps:

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

Generating a Certificate Signing Request

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

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

Purchasing a Certificate

To purchase a new certificate follow these steps:

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

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

Uploading certificate parts

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

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

NOTE

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

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

You can upload an existing certificate in two ways:

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

Uploading a CA certificate

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

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

You can upload an existing certificate in two ways:

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

Generating a CSR using an existing private key

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

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

Removing a certificate part

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

1. At the certificate repository page, select a certificate from the list. You will be taken to the SSL certificate properties page.

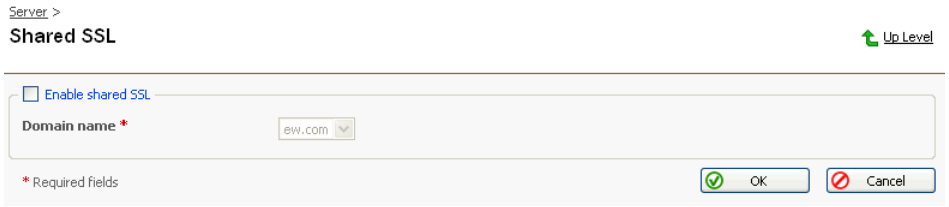
2. Click the Remove button located next to the CA certificate field.

Managing Shared SSL

SSL stands for "Secure Socket Layer" and you can use this feature to protect all data exchanged between your Web site and the client. Shared SSL is a means of secure Web server access without requiring users to purchase a digital key.

In this case, only one domain should have real SSL sertificate. We will call it Master SSL Domain. Other domains, which are set up to use Shared SSL will use its resources.

To choose the Master SSL Domain from the list of domains which have SSL support enabled, go to the Server > Shared SSL page. In order to do this, set the Enable shared SSL checkbox and choose, which domain you want to be the Master SSL Domain.



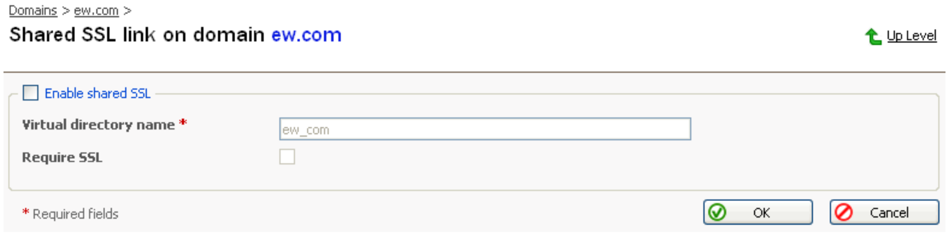
□ Enable shared SSL

Domain name * ew.com

* Required fields

After you have defined the Master SSL Domain, you can give your clients ability to set up shared SSL links. To do it, go to the client's limits page and edit the Maximum number of shared SSL links field or set the Unlimited checkbox.

After that, you or clients can enable Shared SSL support on per-domain basis. To make a domain use shared SSL, go to the Domain Administration page and press the Shared SSL button. The following screen will appear:



□ Enable shared SSL

Virtual directory name * ew_com

Require SSL □

* Required fields

To make the domain use Shared SSL, set the Enable Shared SSL checkbox. The documents, which will be accessible through Shared SSL should be placed into the httpsdocs folder of user's domain.

Now you need to fill the Virtual directory name field. The virtual directory with the supplied name will be created at the Master SSL Domain. It will be used for accessing your site through SSL. Let us suppose domain user has domain named domain.hoster.com and Master SSL Domain is master_ssl_host.hoster.com. Now, to access user's site through the SSL, one needs to supply the following address:

https://master_ssl_host.hoster.com/virtual_directory_name_you_supplied. Note that you cannot use domain address domain.hoster.com to access the site via SSL if you are using the shared SSL mode.

If you set the Require SSL checkbox, the domain will be accessible via SSL only.

Setting System-wide Preferences and Logo

You can set the following system-wide preferences:

- The number of lines displayed on the pages containing lists (i.e.: list of domains, list of clients, etc.),
- Default interface language and skin that will be used for control panel sessions initiated by other users,
- Administrator's interface language and skin,
- Allowance of multiple simultaneous sessions under administrator's login,
- Checking for mailboxes passwords in the vocabulary to ensure they are not easy to guess,
- Server-wide statistics parameters.

To set the server-wide preferences follow these steps:

1. Click the Preferences icon on the Server administration page. The Server preferences page appears.
2. To set the number of lines per page, enter the value into the appropriate input field. The maximum value can contain not more than 4 digits. Entering zero will enable Plesk to display all entries at once on a single page.
3. To set the default interface language, and the language for your interface, select the needed language from the drop-down lists.
4. To change the way your Plesk 7.5 system interface looks, and to set the default skin, select the desired skin from the drop-down lists.
5. To allow multiple users with login name 'admin' access and manage the system, check the Allow multiple sessions under administrator's login checkbox.
6. In order to ensure that the mailboxes passwords are not easy to guess, select the Check the passwords for mailboxes in the vocabulary checkbox.
7. Specify the statistics retention time in the Retain traffic statistics for ...Months field.

8. For the Plesk 7.5 system to know whether to take into account log files, databases, mailboxes, tomcat web applications, mailing lists, and domain backup files when the disk space usage statistics calculation is carried out, specify the necessary options by putting the check marks in appropriate fields.

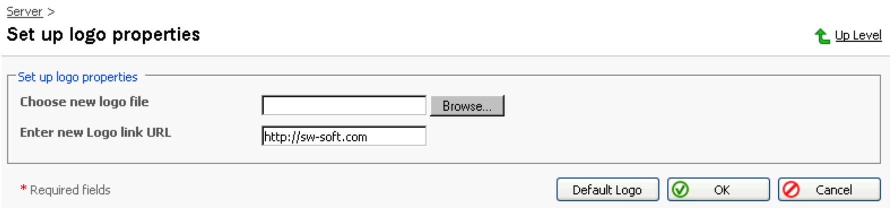
9. To adjust the traffic calculation procedure, at the Include in the traffic calculation section, use the appropriate radio button to select from the inbound and outbound traffic, only inbound traffic, or only outbound traffic settings.

10. Click OK to apply all the changes made.

Setting Up Your Logo

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

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



Server >

Set up logo properties

Set up logo properties

Choose new logo file:

Enter new Logo link URL: http://sw-soft.com

2. Click in the Choose new logo file text box and enter the name of the logo file you wish to use, or click the Browse... button and locate the desired file.

> **NOTE**
>
> You should use a GIF, JPEG or PNG format file for your logo, preferably not larger than 100 kilobytes to minimize the download time. It is recommended that you use an image of 50 pixels in height.

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

4. Click OK to activate the hyperlink.

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

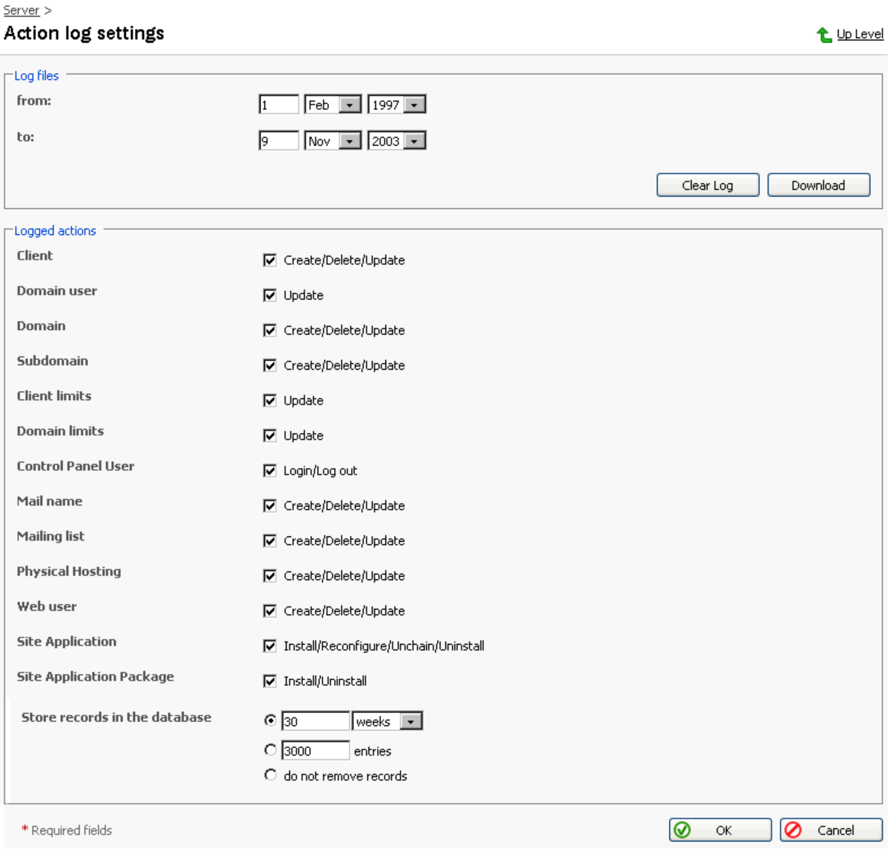
Tracking User Actions

You may wish to keep track of actions performed by various users in the system. All actions will be recorded in a log file that you will be able to download for viewing later on. The following system events can be logged:

- Client account created, deleted, personal or system information changed,
- Domain level user account properties changed,
- Domain created, deleted, settings changed,
- Subdomain created, deleted, settings changed,
- Client account limits changed,
- Domain limits changed,
- Users logged in and out of the Control Panel,
- Mail names created, deleted, changed,
- Mailing list created, deleted, changed,
- Physical hosting created, deleted, changed,
- Web user account created, deleted, changed,
- Site Application installed, reconfigured, unchained, uninstalled,
- Site Application Package installed, uninstalled.

To configure the action log settings, follow these steps:

1. Click the Action Log icon on the Server administration page. The Action log settings page will open:



Server >

Action log settings

Log files

from:	1 Feb 1997
to:	9 Nov 2003

Logged actions

Client	☑ Create/Delete/Update
Domain user	☑ Update
Domain	☑ Create/Delete/Update
Subdomain	☑ Create/Delete/Update
Client limits	☑ Update
Domain limits	☑ Update
Control Panel User	☑ Login/Log out
Mail name	☑ Create/Delete/Update
Mailing list	☑ Create/Delete/Update
Physical Hosting	☑ Create/Delete/Update
Web user	☑ Create/Delete/Update
Site Application	☑ Install/Reconfigure/Unchain/Uninstall
Site Application Package	☑ Install/Uninstall
Store records in the database	● 30 weeks ○ 3000 entries ○ do not remove records

* Required fields

2. In the Logged actions group, select the actions to be logged using the checkboxes.

3. In the Store records in the database field, specify the action log cleaning options: on a daily, weekly or monthly basis, or in accordance with the specified number of records stored in the database. To retain all action log records, select the Do not remove records radio button.

4. To apply all the changes made, click OK.

To download the action log to the local machine, in the Log files section, select the time period using the drop-down boxes, and click Download. The dialog window will open, prompting you to select the location for the downloaded log file to be saved to. Select the location, and click Save.

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

Using Event Manager

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

Adding an Event Handler

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

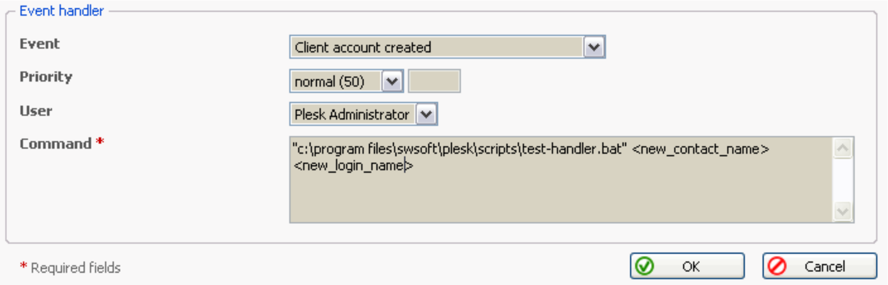
```
-------------------------------------------------------------------
echo "--------------" >> c:\windows\temp\event_handler.log
rem information on the event date and time
date /T   >> c:\windows\temp\event_handler.log
rem information on the created client account
echo "client created" >> c:\windows\temp\event_handler.log
rem client's name
echo "name: %1"       >> c:\windows\temp\event_handler.log
rem client's login
echo "login: %2"      >> c:\windows\temp\event_handler.log
echo "--------------" >> c:\windows\temp\event_handler.log
-------------------------------------------------------------------
```

This script prints some information to a file so that we could control its execution.

Suppose, that our script is located in the directory c:\program files\swsoft\plesk\scripts\. Let's register it by creating an event handler via the control panel:

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

   The Event Manager page appears.
3. Click the Add New Event Handler icon. The event handler setup page appears:



Event handler

Event	Client account created
Priority	normal (50)
User	Plesk Administrator
Command *	"c:\program files\swsoft\plesk\scripts\test-handler.bat" <new_contact_name> <new_login_name>

4. Select the event, you wish to assign a handler to in the Event drop-down box.

5. Select the priority for handler execution, or specify a custom value. To do this, select custom in the Priority drop-down list and type in the value. Note, when assigning several handlers to a single event you can specify the handler execution sequence, setting different priorities (higher value corresponds to a higher priority).

6. Select the system user, on behalf of which the handler will be executed.

7. In the Command input field, specify the path to a file to be executed upon the selected event. In our example it is "c:\program files\swsoft\plesk\scripts\test-handler.bat" <new_contact_name> <new_login_name>

   Note that if directory names or the file name contains spaces, the path should be quoted.

8. Click OK.

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

```
--------------
        Sat Jun 26 21:46:34 NOVT 2004
        client created
        name: Some client
        login: some_client
        --------------
```

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

Removing Event Handlers

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

Available Event Handler Parameter Templates

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

Table 2.1.

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

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

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

Component name/description	Command line parameter		Notes
	Old component value	New component value	
Domain Name	old_domain_name	new_domain_name	required
Web user Name	old_webuser_name	new_webuser_name	required
For the events 'Web user created', 'Web user updated'			
Domain Name	old_domain_name	new_domain_name	required
Web User Name	old_webuser_name	new_webuser_name	required
Web User Password	old_webuser_password	new_webuser_password	
SSI Support	old_ssi_support	new_ssi_support	
PHP Support	old_php_support	new_php_support	
CGI Support	old_cgi_support	new_cgi_support	
Mod Perl Support	old_mod_perl_support	new_mod_perl_support	
Mod Python Support	old_mod_python_support	new_mod_python_support	
Apache ASP Support	old_apache_asp_support	new_apache_asp_support	
Hard Disk Quota	old_hard_disk_quota	new_hard_disk_quota	
For the event 'Client limits updated'			
Contact Name	old_contact_name	new_contact_name	required
Maximum Number of Domains	old_maximum_domains	new_maximum_domains	
Maximum Amount of Disk Space	old_maximum_disk_space	new_maximum_disk_space	
Maximum Amount of Traffic	old_maximum_traffic	new_maximum_traffic	
Maximum Number of Web Users	old_maximum_webusers	new_maximum_webusers	
Maximum Number of Databases	old_maximum_databases	new_maximum_databases	

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

Component name/description	Command line parameter		Notes
	Old component value	New component value	
Maximum Number of Mail Groups	old_maximum_mail_groups	new_maximum_mail_groups	
Maximum Number of Mail Autoresponders	old_maximum_mail_autoresponders	new_maximum_mail_autoresponders	
Maximum Number of Mailing Lists	old_maximum_mail_lists	new_maximum_mail_lists	
Maximum Number of Java Applications	old_maximum_tomcat_web_applications	new_maximum_tomcat_web_applications	
Expiration Date	old_expiration_date	new_expiration_date	
For the events 'Mailing list created', 'Mailing list updated', 'Mailing list deleted'			
Domain Name	old_domain_name	new_domain_name	required
Mailing list name	old_mail_list_name	new_mail_list_name	required
Mailing list enabled	old_mail_list_enabled	new_mail_list_enabled	
For the events 'Control panel user logged in', 'Control panel user logged out'			
Contact Name	old_contact_name	new_contact_name	
For the event 'Domain user account updated'			
Allow domain user access	old_allow_domain_user_access	new_allow_domain_user_access	
Login Name	old_login_name	new_login_name	required
Domain Name	old_domain_name	new_domain_name	required
Contact Name	old_contact_name	new_contact_name	
Company Name	old_company_name	new_company_name	
Phone	old_phone	new_phone	
Fax	old_fax	new_fax	
E-mail	old_email	new_email	
Address	old_address	new_address	
City	old_city	new_city	

Component name/description	Command line parameter		Notes
	Old component value	New component value	
State/Province	old_state_province	new_state_province	
Postal/ZIP Code	old_postal_zip_code	new_postal_zip_code	
Country	old_country	new_country	
For the events 'Site application installed', 'Site application reconfigured', Site application uninstalled'			
Site application package name	old_site_application_package_name	new_site_application_package_name	required
Domain type (domain or subdomain)	old_site_application_domain_type	new_site_application_domain_type	required
Installation path (httpdocs or httpsdocs)	old_site_application_directory	new_site_application_directory	required
Installation path within the destination directory	old_site_application_installation_prefix	new_site_application_installation_prefix	required
For the events 'Site application package installed', 'Site application package uninstalled'			
Site application package name	old_site_application_package_name	new_site_application_package_name	required
For the events 'Service stopped, started, or restarted'			
Service	old_service	new_service	required
For the events 'IP address created, changed, or deleted'			
IP address	old_ip_address	new_ip_address	required
IP mask	old_ip_mask	new_ip_mask	
Interface	old_interface	new_interface	
IP type	old_ip_type	new_ip_type	
For the events 'Forwarding created, changed, deleted'			
Domain name	old_domain_name	new_domain_name	required
Forwarding type	old_forwarding_type	new_forwarding_type	
URL	old_url	new_url	

Component name/description	Command line parameter		Notes
	Old component value	New component value	
For the event 'Administrator information changed'			
Login name	old_login_name	new_login_name	required
Contact name	old_contact_name	new_contact_name	
Company name	old_company_name	new_company_name	
Phone number	old_phone	new_phone	
Fax	old_fax	new_fax	
E-mail	old_email	new_email	
Address	old_address	new_address	
CIty	old_city	new_city	
State/Province	old_state_province	new_state_province	
Postal/Zip code	old_postal_zip_code	new_postal_zip_code	
Country	old_country	new_country	
For the events 'Site application installed, reconfigured, uninstalled'			
Site application name	old_package_name	new_package_name	required
For the events 'Client status updated'			
Contact name	old_contact_name	new_contact_name	required
Login name	old_login_name	new_login_name	required
Status	old_status	new_status	
For the events 'Client preferences updated'			
Contact name	old_contact_name	new_contact_name	required
Login name	old_login_name	new_login_name	required
Page size	old_lines_per_page	new_lines_per_page	
Interface skin	old_interface_skin	new_interface_skin	
For the event 'Client's IP pool changed'			
Contact name	old_contact_name	new_contact_name	required

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

Enabling E-mail Notification

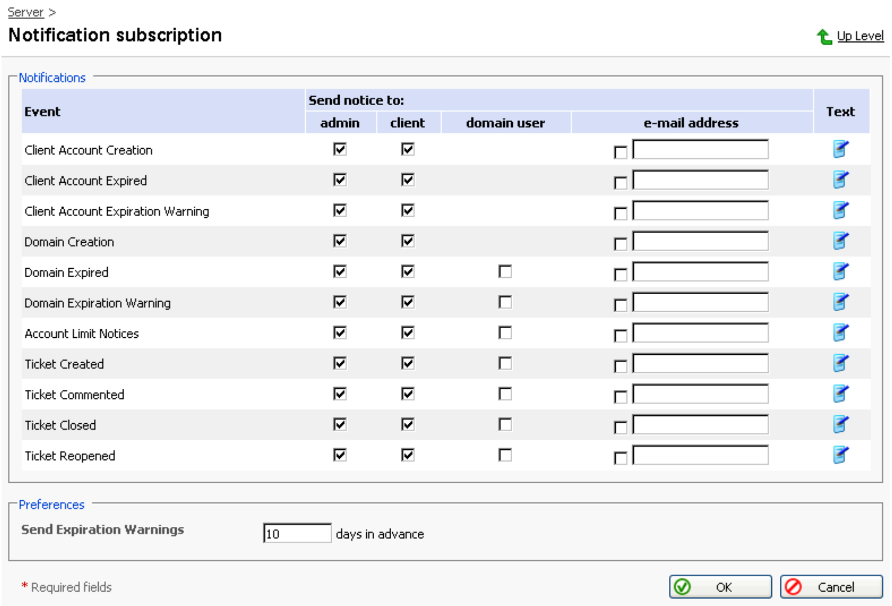
You can configure Plesk so as to notify you or other control panel users by e-mail of the following system events:

- client account creation,
- client account expiration,

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

To enable e-mail notifications, follow these steps:

1. On the Server administration page click the Notifications icon. The Notification Subscription page appears:



Server >

Notification subscription

Notifications

Event	Send notice to:				Text
	admin	client	domain user	e-mail address	
Client Account Creation	☑	☑		□	✎
Client Account Expired	☑	☑		□	✎
Client Account Expiration Warning	☑	☑		□	✎
Domain Creation	☑	☑		□	✎
Domain Expired	☑	☑	□	□	✎
Domain Expiration Warning	☑	☑	□	□	✎
Account Limit Notices	☑	☑	□	□	✎
Ticket Created	☑	☑	□	□	✎
Ticket Commented	☑	☑	□	□	✎
Ticket Closed	☑	☑	□	□	✎
Ticket Reopened	☑	☑	□	□	✎

Preferences

Send Expiration Warnings 10 days in advance

* Required fields

2. Select the events and the appropriate types of users you wish to be notified using the checkboxes in the Send notice to: admin, client, domain user, and e-mail address columns.

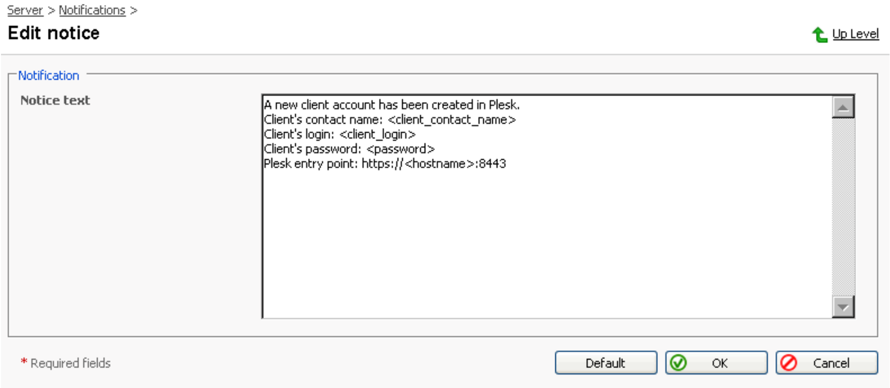
3. Enable sending expiration warnings in advance by specifying the necessary value in the appropriate field. Note that expiration warning message is sent once in a specified number of days prior to the domain or client account expiration date.

4. Click OK to submit all changes.

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

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

appears:



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

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

3. Click OK.

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

Creation of a client account

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

Client account expiration

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

Client account expiration warning

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

New domain creation

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

Domain expiration

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

Domain expiration warning

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

Account limit notices

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

Help Desk system notices

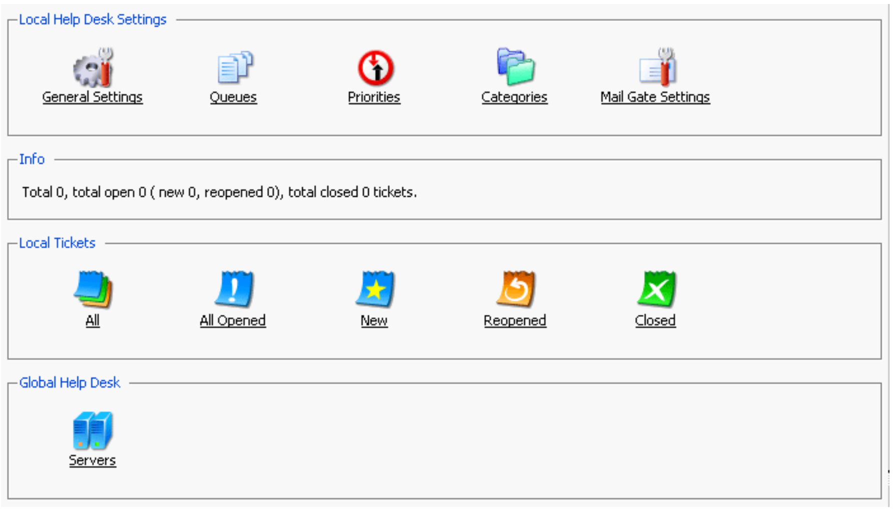
- <ticket_id> - trouble ticket identification number
- <ticket_comment> - trouble ticket comment

Configuring the Help Desk

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

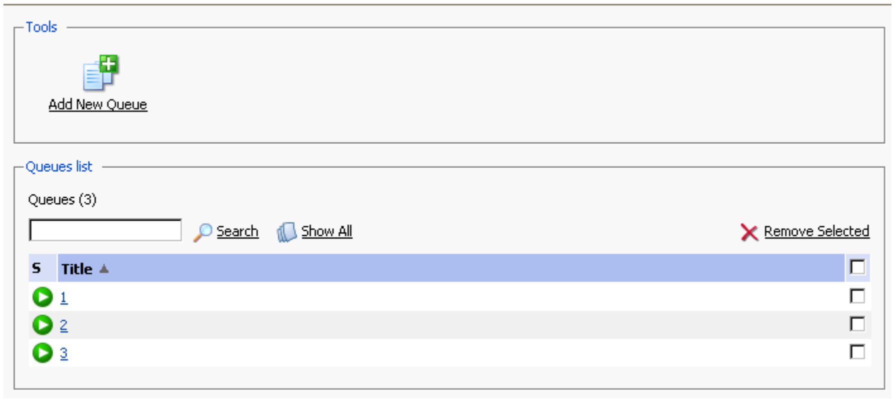
Before users are able to submit the trouble tickets, you should perform an initial configuration of Help Desk. To this effect, you should create at least one instance of Queue, Priority and Category and then activate the Help Desk:

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



Total 0, total open 0 (new 0, reopened 0), total closed 0 tickets.

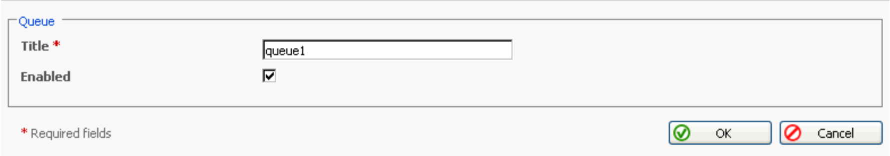
2. To create a new Queue, select the Queues icon. The page opens displaying the queues registered in the system:



Queues (3)

S	Title ▲	□
▶	1	□
▶	2	□
▶	3	□

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



Title * queue1

Enabled ☑

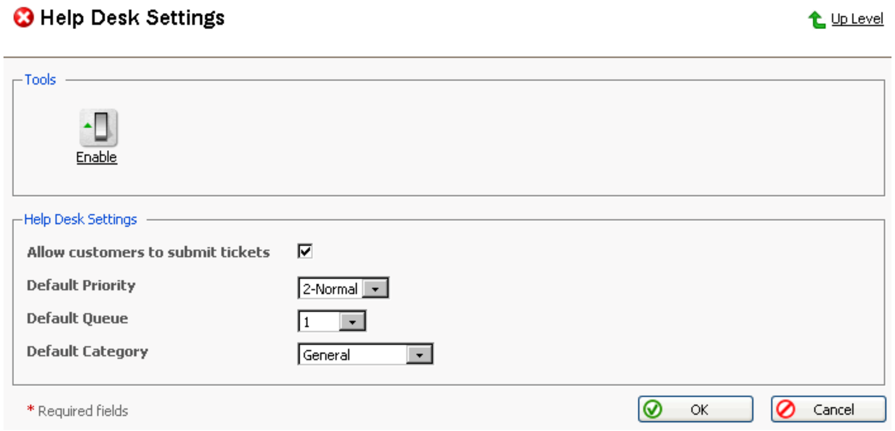
* Required fields

4. Enter a title, select the Enabled checkbox and click OK.

5. In the same manner create at least one Priority and one Category using respective Priorities and Categories icons on the main Help Desk System’s page.

6. Once the queue, priority and category are created, return to the main Help

Desk page and click General Settings. The General Settings page opens:



Help Desk Settings

Up Level

Tools

Enable

Help Desk Settings

Allow customers to submit tickets	☑
Default Priority	2-Normal ▾
Default Queue	1 ▾
Default Category	General ▾

* Required fields

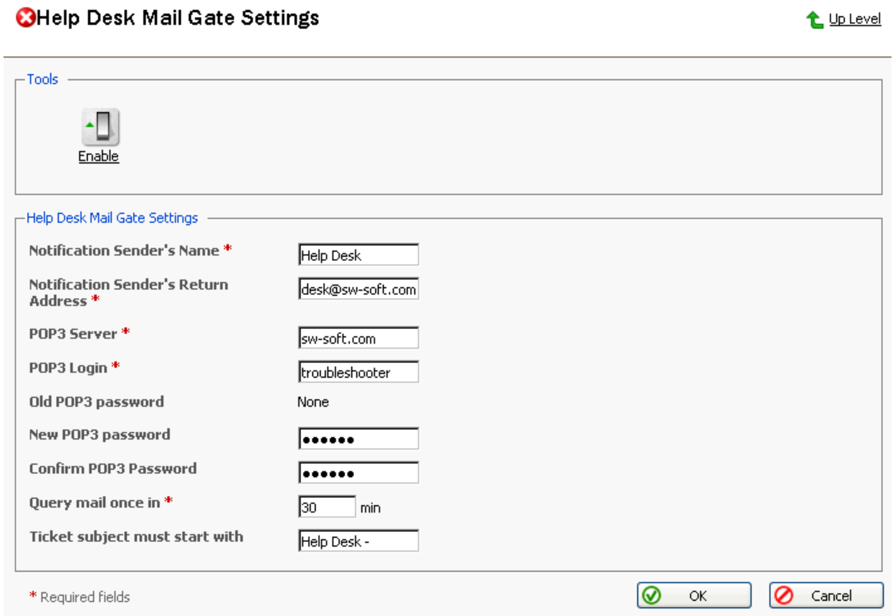
OK Cancel

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

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

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

   The mail gate configuration page opens:



Help Desk Mail Gate Settings

Up Level

Tools

Enable

Help Desk Mail Gate Settings

Notification Sender's Name *	Help Desk
Notification Sender's Return Address *	desk@sw-soft.com
POP3 Server *	sw-soft.com
POP3 Login *	troubleshooter
Old POP3 password	None
New POP3 password	••••••
Confirm POP3 Password	••••••
Query mail once in *	30 min
Ticket subject must start with	Help Desk -

* Required fields

OK Cancel

2. Fill out the following fields:

- Notification Sender's Name - the name that will be set up in the e-mail notification messages
- Notification Sender's Return Address - the notification sender’s return e-mail address
- POP3 Server - POP3 server, the mail should be fetched from
- POP3 Login - login name for accessing the POP3 server
- New POP3 password - POP3 password that will be used for getting mail
- Confirm POP3 Password - password confirmation
- Query mail once in - [ ] min – define the time interval between mail queries.
- Ticket subject must start with [ ] – specify the combination of symbols the subject line of mail messages must start with. This can help to filter out spam.

3. Once the required fields are filled out, click Enable. The mail gate is activated.
4. Click OK to return to the main page.

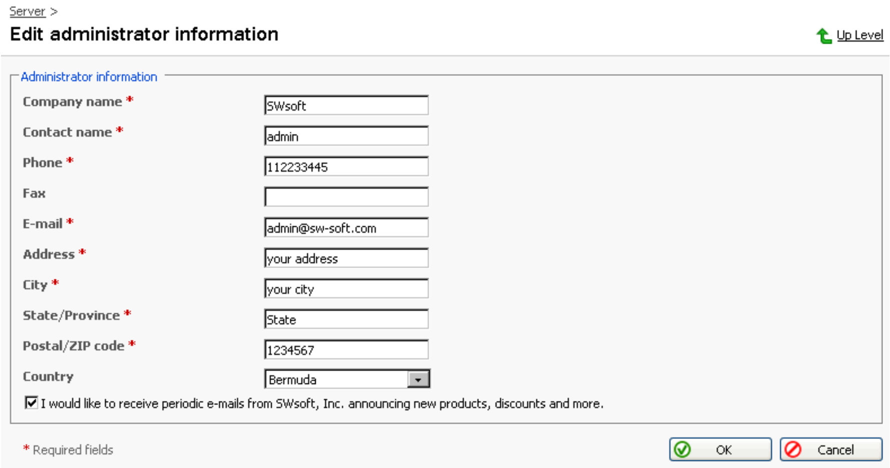
Chapter 3. Performing Administrative Tasks

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

Editing Administrator's Information and Password

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

1. On the Server administration page, click Edit. The Administrator's information editing page appears:



Server >

Edit administrator information

Administrator information

Company name *	SWsoft
Contact name *	admin
Phone *	112233445
Fax	
E-mail *	admin@sw-soft.com
Address *	your address
City *	your city
State/Province *	State
Postal/ZIP code *	1234567
Country	Bermuda

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

* Required fields

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

3. Click OK to submit.

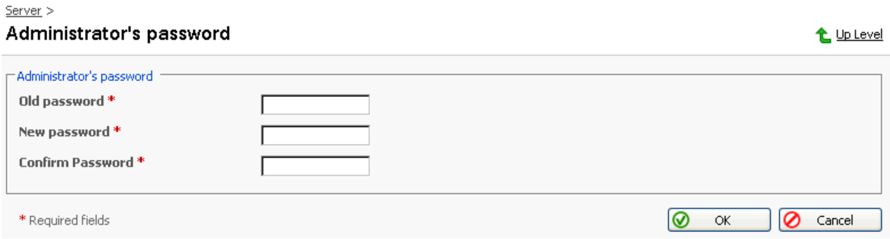
NOTE

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

To change the administrative password follow these steps:

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

Administrator's password page appears:



Server >

Administrator's password

Up Level

Administrator's password

Old password * ____

New password * ____

Confirm Password * ____

* Required fields

OK Cancel

2. Click in the Old password text box and enter your current password.

3. Click in the New password text box and enter the password you wish to change to.

4. Click in the Confirm Password text box and re-enter the new password, exactly as you entered it in the New password text box.

5. Click OK.

If you forget your password

If you forget your password, you can use the plesksrvclient.exe utility located in <plesk installation directory>\admin\bin to set up a new password.

Managing Plesk Services

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

1. Click the ⚙ Service Management icon on the Server administration page. The Services management page appears. The current state of a service is marked by an icon: ▶ (On) for the service running, ✖ (Off) for the service stopped, and ● if service is not installed or its management capabilities are not supported by the license key.

2. To start a service: click ▶ (Start service).

   To stop a service: click ■ (Stop service).

   To restart a service: click ○ (Restart service).

Using the Plesk Service Control Utility

In addition to the service management facilities provided within control panel, there is the Service Control utility available from the system taskbar. It allows managing the following services:

- Plesk Control Panel - the control panel's web server engine,
- Plesk Management Service - handles control panel settings, security and statistics,
- Plesk Miscellaneous Service - handles IP assignment, time management, Plesk utilities and user accounts,
- Plesk Scheduler - task scheduling and management,
- Plesk List Connector - mail service,
- Plesk Mail Transfer Agent - mail service,
- Plesk POP Service - mail service,
- Plesk Postoffice Connector - mail service,
- Plesk SMTP Connector - mail service,
- Plesk SQL Server - MySQL database that stores all Plesk objects,
- Stunnel - enables SSL support for mail server,
- Plesk Name Server - DNS service,
- Plesk Java Servlet Container - enables support for Java applets.

To start a service, select the corresponding checkbox, and click the Start button.

To stop a service, select the corresponding checkbox, and click Stop.

To restart a service, select the corresponding checkbox, and click Restart.

To select all services, use the Select All button. To deselect the services, click Clear All.

Click Refresh to refresh the list of services.

Click Delete Sessions to clear all user sessions.

Managing Server IP Addresses

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

To do this, click the IP Addresses icon on the Server administration page. The IP addresses management page appears displaying the list of IP addresses available in the system.

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

NOTE

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

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

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

NOTE

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

IMPORTANT

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

Adding a new IP address

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

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

NOTE

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

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

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

Selecting a 'default domain'

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

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

1. At the IP addresses management page, click on the number in the Hosting column of the list, corresponding to the necessary IP address. The page will open displaying the list of domains hosted using this IP address.
2. Select the domain using the corresponding radio button.
3. Click Set as Default. Now the default domain is assigned.

Managing the clients granted a specific IP address

Accessing the list of clients sharing the same IP address

To access the list of clients, follow these steps:

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

Adding IP address to client's IP pool

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

1. Select the Add Client icon on this page. The clients selection dialog window will open prompting you to select the clients to add the ip address to.
2. Select a client's name from the list.
3. Click Add.

Removing IP address from client's IP pool

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

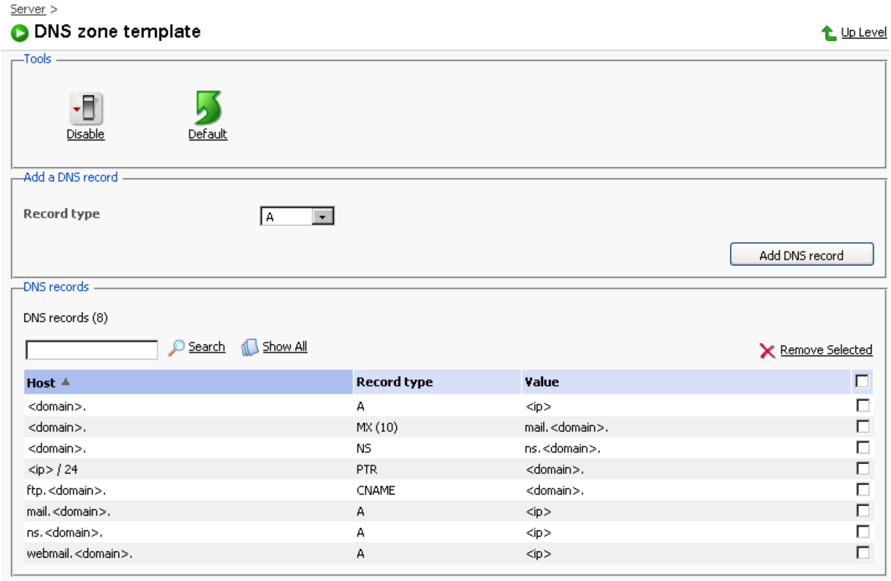
1. Select the client you wish to remove an IP from using the checkbox.
2. Click Remove Selected. The confirmation page appears.
3. Select the checkbox to confirm and click OK.

Managing the DNS Zone Template

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

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

1. Click the DNS icon on the Server administration page. The DNS Zone Template page appears:



Server >

DNS zone template

Add a DNS record

Record type: A

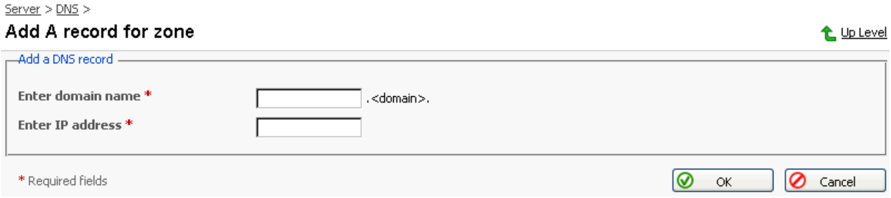
DNS records

DNS records (8)

Host ▲	Record type	Value	□
<domain>.	A	<ip>	□
<domain>.	MX (10)	mail.<domain>.	□
<domain>.	NS	ns.<domain>.	□
<ip> / 24	PTR	<domain>.	□
ftp.<domain>.	CNAME	<domain>.	□
mail.<domain>.	A	<ip>	□
ns.<domain>.	A	<ip>	□
webmail.<domain>.	A	<ip>	□

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

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



Server > DNS >

Add A record for zone

Add a DNS record

Enter domain name * .<domain>.

Enter IP address *

* Required fields

3. Fill the required information into the input fields (the type of the information required depends on the type of the DNS record selected).

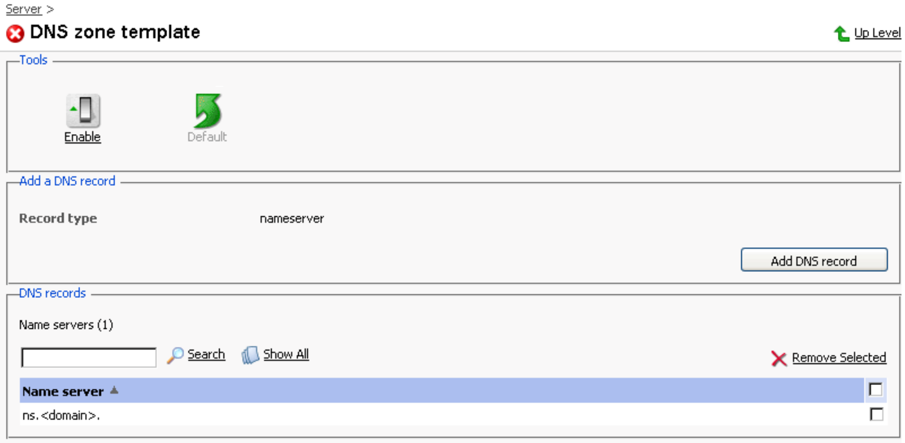
4. Click OK to submit the entered data and add the new record to the template.

NOTE

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

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

- If you wish to turn the DNS on for the template, click Enable, or click Disable to turn it off.
- Turning the DNS zone off will refresh the page, so that only a list of nameservers remains:



Record type nameserver

Name servers (1)

Name server ▲	□
ns.<domain>.	□

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

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

Configuring SOA records parameters

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

- SOA_TTL
- SOA_Refresh
- SOA_Retry
- SOA_Expire
- SOA_Minimum

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

Example:

```
mysql -uadmin -p -D psa -e "INSERT INTO misc VALUES
('SOA_TTL','86400');"
```

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

```
mysql -uadmin -p -D psa -e "UPDATE misc SET val='43200'
WHERE param='SOA_TTL';"
```

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

```
C:\SWsoft\PLESK\admin\bin\dnsmng.exe update
domain.name.com
```

Managing Client Templates

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

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

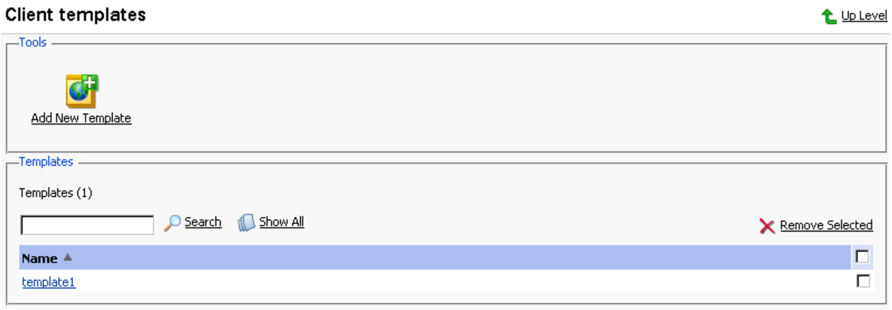
- Ability to create domains
- Ability to manage physical hosting
- Ability to manage hard disk quota

- Ability to manage subdomains
- Ability to change domain limits
- Ability to manage DNS zone
- Ability to manage log rotation
- Ability to manage scheduler
- Ability to manage anonymous FTP
- Ability to manage web applications
- Ability to manage system access
- Ability to manage mailing lists
- Ability to use the backup/restore functions
- Maximum number of domains and subdomains
- Amount of disk space available
- Amount of traffic allowed
- Maximum number of web users
- Maximum number of MS SQL databases
- Maximum number of MySQL databases
- Maximum number of mailboxes
- Mailbox quota
- Maximum number of mail redirects
- Maximum number of mail groups
- Maximum number of mail autoresponders
- Maximum number of mailing lists
- Maximum number of Tomcat web applications
- Client account validity period
- IP addresses allocation
- Number of lines to be displayed in the interface pages viewed by client

Creating a client template

To create a new client template, follow these steps:

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



Name ▲	☐
template1	☐

3. Click Add New Template. The Template creation and editing page appears.

4. Enter the name for the client template in the Template name field. In the Permissions group, select the appropriate checkboxes to grant all necessary permissions to the client. In the Limits group specify the limits to be applied: uncheck the "Unlimited" checkboxes and type in the values for the parameters. The Mailbox quota limit defines the amount of disk space that a given client is allowed to have per mail box on a single domain. Note, that you can impose the tighter limit on the mailbox size from the Domain Limits page and in the mailbox properties. To limit the client account validity period, uncheck the corresponding "Unlimited" checkbox, select the time unit in the drop-down list (it can be Years, Months, Days) and type in the value.

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

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

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

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

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

Editing a client template

To edit a client template:

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

2. Click OK after you are done with configuring the template.

Removing a client template

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

Managing Domain Templates

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

Use the domain template to assign the following parameters:

- Mail to nonexistent user mode
- Maximum number of subdomains
- Disk space limit
- Maximum amount of traffic allowed
- Maximum number of web users
- Maximum number of MS SQL databases
- Maximum number of MySQL 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
- Microsoft ASP and ASP.NET support
- SSI support
- PHP support
- CGI support
- Perl support

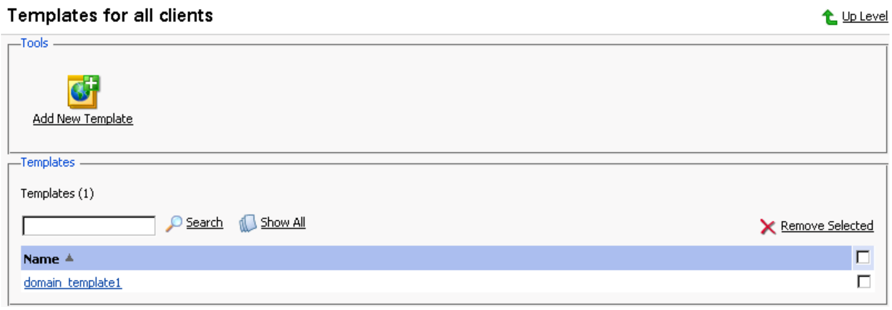
- Python support
- ColdFusion support
- Web statistics
- Use of Custom Error Documents

Creating a domain template

To add a new domain template, follow these steps:

1. Select the Domains shortcut in the navigation pane.

2. Click the Domain Templates icon. The Domain templates management page appears:



Name ▲	☐
domain_template1	☐

3. Click Add New Template. The Template creation and editing page appears.

4. Enter the name for the domain template in the Template name field.

5. Set the Mail to nonexistent user option to Bounce, Catch to address or Discard, and enable Webmail, if desired.

6. Use the Limits group to define the resource usage limits for domains. To set the necessary parameters, deselect the Unlimited checkboxes, and type the limit values into the input fields. Mailbox quota is the amount of disk space that a single mail user in this domain is allowed to have. Note, that you can impose the tighter limit on the mailbox size in the mailbox properties.

7. To define the domain validity period, deselect the Unlimited checkbox, type the value into Validity period input field, and specify the time measurement unit (years, months, or days).

8. Select the Enable log rotation checkbox to enable it. Select the log rotation condition: to be based on log file size, or time (select from Daily, Weekly, Monthly). Specify the maximum number of log files, enable log files compression, and specify an e-mail address for the processed log files to

be delivered to.

> **NOTE**
>
> It is advisable to set the logrotation options appropriately in order to prevent the log files from growing too large to be handled by the statistics utility.

9. To enable Mailing lists, select the corresponding checkbox.

10. To retain the traffic statistics for domains, select the corresponding checkbox and specify the retention period in the Retain traffic statistics for ... Months field.

11. Select the domain DNS zone type using the Master or Slave radio button.

12. To enable physical hosting for domain, select the Physical hosting checkbox.

13. Specify the hard disk quota in the appropriate field, if needed.

14. SSL support checkbox enables the maintenance of https protocol.

15. To allow the use of Microsoft FrontPage Server Extensions, check the checkbox for Microsoft FrontPage support and Microsoft FrontPage over SSL support. Authoring will be disabled by default. For security reasons, authoring should only be enabled when Microsoft FrontPage extensions are in use.

16. Use the remaining checkboxes to enable the following hosting features:
    - Allow the web users scripting: enable support for scripting in web users' pages.
    - ASP support: ASP module enabled.
    - SSI support: Server Side Includes scripting enabled.
    - PHP support: supports html documents that contain PHP scripts.
    - CGI support: an individual cgi-bin directory is created and CGI scripting is enabled.
    - Perl support: Perl scripting enabled.
    - Python support: Python scripting enabled.
    - ColdFusion support: ColdFusion scripting enabled (for information on possible problems see Configuring Physical Hosting section).
    - Web statistics: keeping the access statistics for the domain.
    - Custom Error Documents: allow the use of custom pages in case of web server errors.

17. Click OK to apply the changes made.

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

Editing a domain template

To edit a domain template:

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

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

Removing a domain template

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

Managing Custom Buttons

You can insert into Plesk control panel any additional buttons that will be linked to a specific URL. Thus, when a user clicks on such button, the URL link specified will open in a new browser window. The buttons may be placed either on Domain Administration page of all domains belonging to all clients, or only on the domains of a certain client. The buttons will be placed below the domain management buttons, 4 buttons in a row.

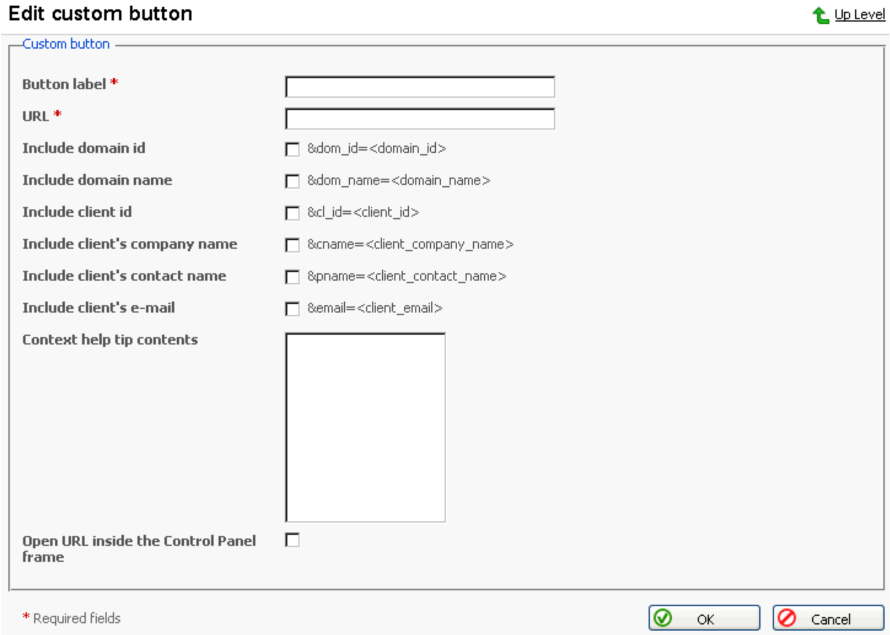
> **NOTE**
>
> The number of customizable buttons is unlimited and does not depend on the license key.

IMPORTANT

- To create and manage the Custom Buttons, which will be displayed for all domains hosted on server, click Custom Buttons on the Server Administration page.
- To create and manage the buttons that will be displayed only for the domains of a certain client, select the required client, and click Custom Buttons on the Client Home page.

To create a new custom button, follow these steps:

1. Click Add New Custom Button on the Custom Buttons Management page. The Custom button editing page opens:



Edit custom button

Custom button

Button label *	
URL *	
Include domain id	□ &dom_id=<domain_id>
Include domain name	□ &dom_name=<domain_name>
Include client id	□ &cl_id=<client_id>
Include client's company name	□ &cname=<client_company_name>
Include client's contact name	□ &pname=<client_contact_name>
Include client's e-mail	□ &email=<client_email>
Context help tip contents	
Open URL inside the Control Panel frame	□

* Required fields

2. Enter the button label in the Button label field.

3. Type the URL link to be attached to the button into the URL field.

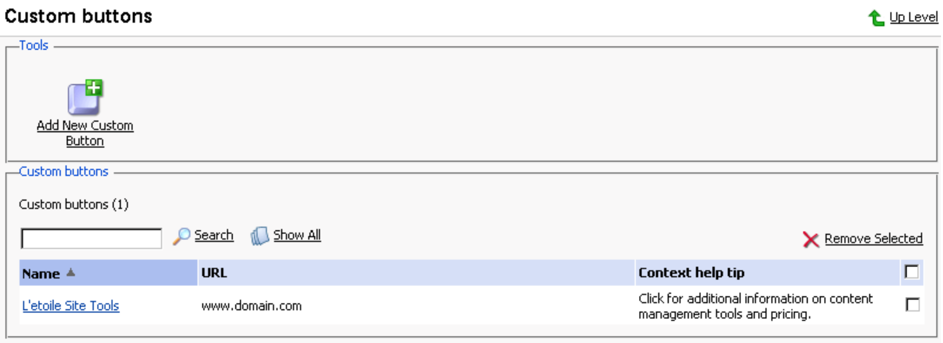
4. Using the checkboxes, specify whether to include the data, such as domain id, client id, company name, client's contact name, and the client's e-mail to be transferred within the URL. These data can be required for processing by external web applications.

5. 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.

6. Select the Open URL inside the Control Panel frame 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.

7. Click OK to complete creation.

Once a new button is created it appears in the list of customizable buttons on the Custom Buttons Management page:



Name ▲	URL	Context help tip	□
L'etoile Site Tools	www.domain.com	Click for additional information on content management tools and pricing.	□

To edit a button, select its label in the list.

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

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
- cgi-bin
- anon_ftp
- error_docs

All other directories will be ignored during skeleton deployment.

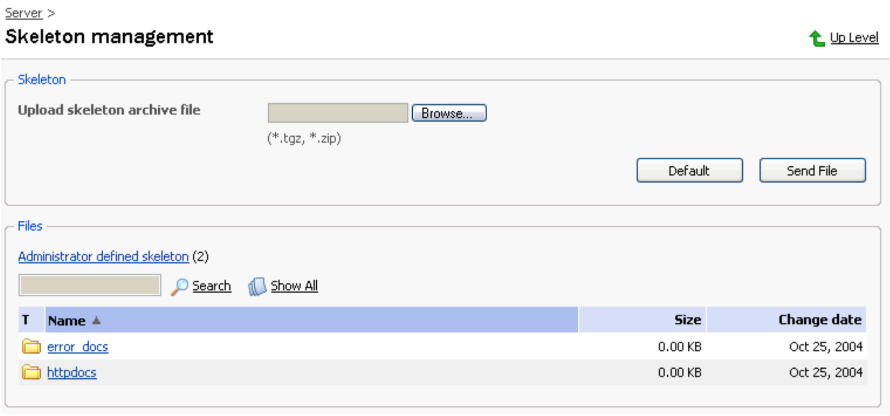
Allowed skeleton file types are *.zip, *.tgz, *.tar, *.gz and *.rar archives.

To activate a new custom skeleton, follow these steps:

NOTE

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

1. Click the Skeleton button on the Server administration page. The Skeleton management page will open:



Skeleton management

Upload skeleton archive file (*.tgz, *.zip)

Administrator defined skeleton (2)

T	Name ▲	Size	Change date
	error_docs	0.00 KB	Oct 25, 2004
	httpdocs	0.00 KB	Oct 25, 2004

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 Scheduler

To access the scheduler management functions, click the Scheduler Manager icon on the Server administration page. The Scheduler management page will open.

At this page, you can view scheduled tasks of various system users, set the e-mail address for the scheduler output messages delivery, schedule new tasks and remove them.

The User 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.

To enable scheduler to send notification to a specified e-mail address, select the required value in the Scheduler notification drop-down box, specify the e-mail address (if required), and click Set. All scheduled tasks from the displayed list that output some information will automatically have their output sent to the specified address.

Each line in the 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 or Description column displays the task description (if supplied by the user) or the command executed within the selected task, which also serves as a link to the page that allows editing the selected scheduled task properties. The Task priority indicates the priority set for the task.

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

To schedule a new task, follow these steps:

1. Click the Add New Task icon. You will be taken to the scheduled task properties page.
2. To activate the task, leave the Enabled checkbox selected. If you wish to temporarily disable the task, clear this checkbox. The disabled tasks are not executed.
3. Provide a short description for the task, if desired. This description will be displayed in the list of all scheduled tasks and will serve as a link to the page that allows editing the task's properties. If no description is specified, the command executed within the task will be displayed.
4. To enable scheduler to send the notification messages to a specified e-mail address, select the required value in the Scheduler notification drop-down box, and specify the e-mail address (if required). Any information output by the task will be automatically sent to the specified address.
5. In the Path to executable file or script box, specify the absolute path to executable file or script. This file may be:

   - a generic windows application,
   - a PHP script (identified by the opening <? or <?PHP tags in the first line),
   - a PHP, Perl or Python script (identified by the first line #!script interpreter name),
   - a file with any of the following extensions: .BAT or .CMD (batch files), .VBS, .VBE, .JS, .JSE (visual basic or java scripts), .PL, .PM (perl scripts), .PY, .PYC (python scripts), .PHP, .PHP3 (php scripts).

   The path to file may include the environment variables related to a user, on behalf of which the application or script is executed, therefore the users may specify the strings like **`%homedrive%%homepath%\application.name`** to run the applications or scripts residing in their home folders.

For example, c:\Inetpub\vhosts\domain.com is a user's home folder. If user specifies %homedrive%%homepath%\httpdocs\application.exe as the application to be executed, the application.exe file located in c:\Inetpub\vhosts\domain.com\httpdocs\ will be run.

6. In the Arguments box, type in the arguments for the application or script to be run with.
7. In the Task priority box, define the priority for the task. High priority may be defined for executing critical tasks, Normal priority may be defined for the most general tasks, and Low priority may be defined for the tasks that require much time to complete.
8. Once you have set the schedule for this task, click OK to submit.

Configuring ODBC

The Open Database Connectivity (ODBC) is an interface used to access data from a variety of database management systems. For example, if you have a program that accesses data in a SQL database, Data Sources (ODBC) will let you use the same program to access data in a Visual FoxPro database. To do this, you must add software components called drivers to your system. The ODBC DSN page within Plesk helps you add, configure, and remove these drivers. You access this page, clicking the ODBC Settings icon on the Server Administration page.

To add a new data source connection from the ODBC management page, follow these steps:

1. Click Add New ODBC DSN.
2. Enter the name you would like to use to refer to the data source in the Connection name box, select the driver for which you are adding a data source and click OK. A driver-specific setup page will appear.
3. Use the Server drop-down box to select the name of SQL server the driver will connect to.
4. Use the Login ID and Password fields to specify the login ID and password the SQL Server driver will use to connect to SQL Server.
5. You may need to supply any additional information, if requested by the driver.
6. Once the required information is supplied, you can use the Test connection option to attempt connecting to the data source with the given credentials.

7. Click Finish to complete creation of the data source name.

After the Data Source Name connection is configured, it appears in the list on the ODBC Management page.

To remove a data source name, select the corresponding checkbox and click Remove Selected. You will then be prompted to confirm removing. Select the checkbox to confirm and click OK.

Using Application Vault

Application vault functionality allows for installing and configuring various web applications.

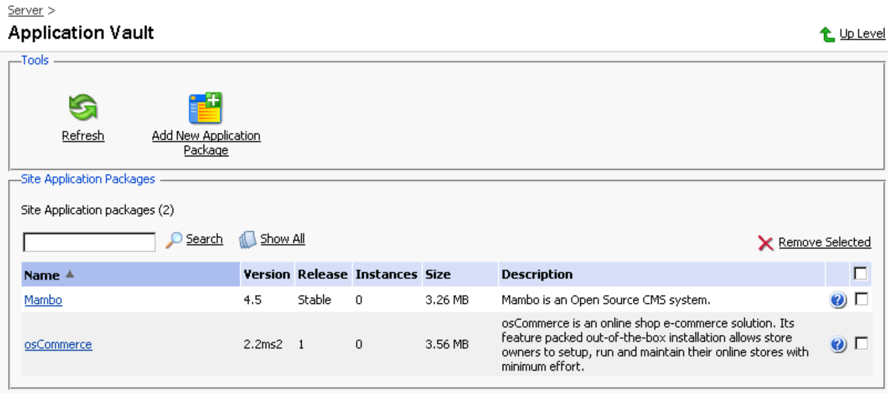
Terminology:

- *Application* – the application itself, installed on the domain and available for usage;
- *Application package* – the set of files and data storing the application archive, from which the application is installed on the domain.

Adding an application package to the Vault

1. Click the Application Vault icon at the Server administration page.

   The Application Vault opens:



Server >

Application Vault

Site Application packages (2)

Name ▲	Version	Release	Instances	Size	Description		□
Mambo	4.5	Stable	0	3.26 MB	Mambo is an Open Source CMS system.	?	□
osCommerce	2.2ms2	1	0	3.56 MB	osCommerce is an online shop e-commerce solution. Its feature packed out-of-the-box installation allows store owners to setup, run and maintain their online stores with minimum effort.	?	□

2. Click Add New Application. Select the application package file using the Browse… button and click Send File. The selected application package will be uploaded and registered in the database.

3. View info on application

You can view information on available application packages by clicking on the application package name in the list.

The information states the name and the version of the package, a brief description as well as a set of requirements that must be fulfilled in the domain hosting setup in order for the application to function.

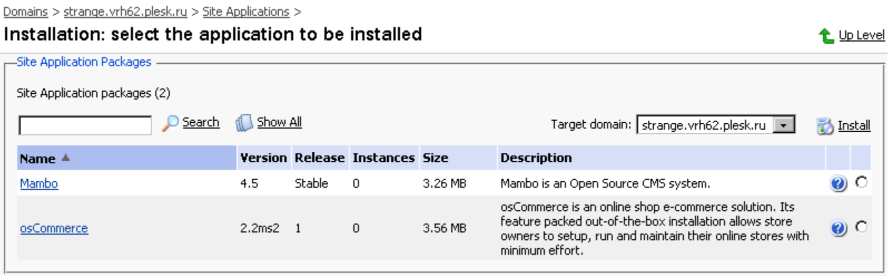
4. Removing application packages

   In order to remove one or several application packages, select the corresponding checkboxes and click Remove selected.

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

Installing application on domain

1. Select a domain with configured physical hosting and click the Application Vault icon in the Hosting group.
2. Click the Add Application icon. The application installation wizard will open:



Domains > strange.vrh62.plesk.ru > Site Applications >

Installation: select the application to be installed

Site Application Packages

Site Application packages (2)

Target domain: strange.vrh62.plesk.ru

Name ▲	Version	Release	Instances	Size	Description		
Mambo	4.5	Stable	0	3.26 MB	Mambo is an Open Source CMS system.	?	○
osCommerce	2.2ms2	1	0	3.56 MB	osCommerce is an online shop e-commerce solution. Its feature packed out-of-the-box installation allows store owners to setup, run and maintain their online stores with minimum effort.	?	○

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

   You can view information on available application packages by clicking on the application package name in the list. If there is a documentation available for the application, it will be accessible through the icon ?.
4. Click Install.
5. Some applications require that certain parameters be entered before executing the installation. Click Finish once you are done editing the

required parameters.

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.

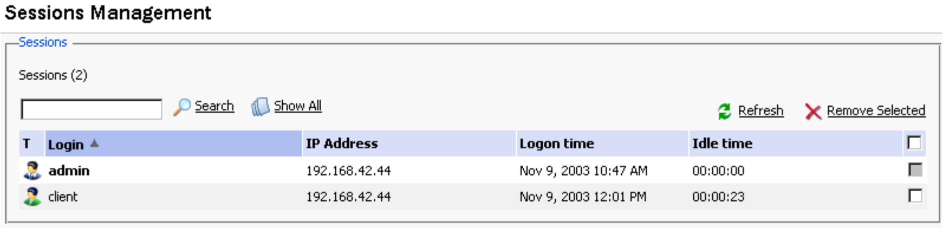
To edit the parameters of an application, click on the corresponding icon ⚙.

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.

Managing User Sessions

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



Sessions Management

Sessions

Sessions (2)

T	Login ▲	IP Address	Logon time	Idle time	□
👤	admin	192.168.42.44	Nov 9, 2003 10:47 AM	00:00:00	□
👤	client	192.168.42.44	Nov 9, 2003 12:01 PM	00:00:23	□

The icon in the T (Type) column identifies a control panel user who established the session. The Login column displays the user's system login, IP address indicates the ip the control panel is accessed from, the Logon time and Idle time columns display the date and time the session was initiated, and the session idle time respectively.

Click Refresh to refresh the list of user sessions.

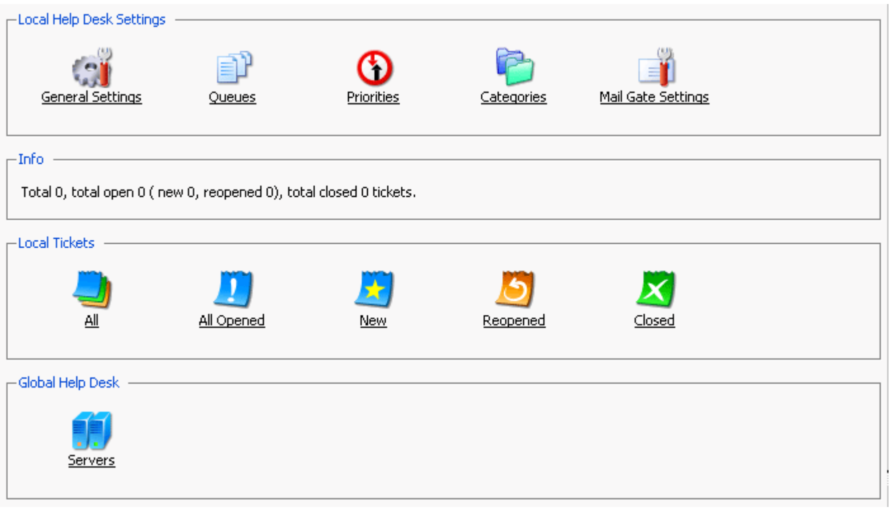
To end a user session, select the corresponding checkbox and click Remove Selected.

Operating Help Desk

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

To view the submitted tickets, follow these steps:

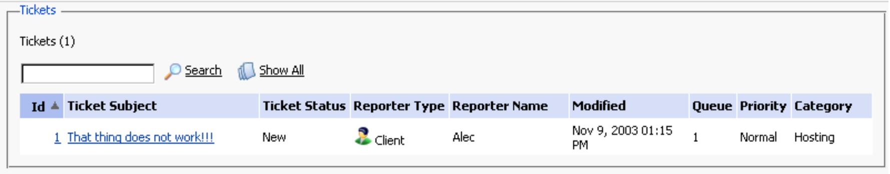
1. Select the Help Desk shortcut in the navigation pane. The Help Desk's main page opens:



Total 0, total open 0 (new 0, reopened 0), total closed 0 tickets.

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

3. Click All to list all existing trouble tickets in any state. The page will open listing all existing trouble tickets and their properties:



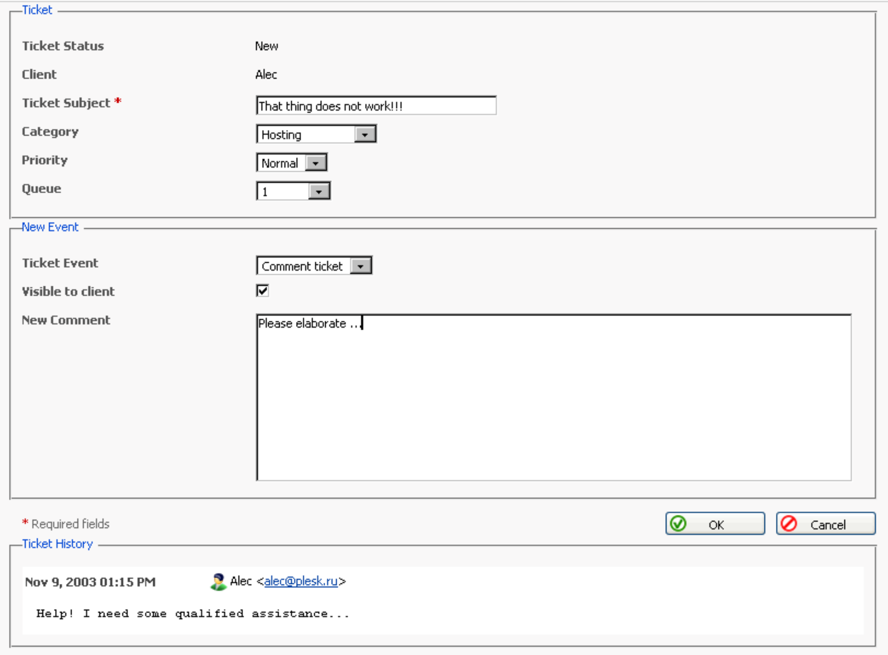
Tickets (1)

Id ▲	Ticket Subject	Ticket Status	Reporter Type	Reporter Name	Modified	Queue	Priority	Category
1	That thing does not work!!!	New	Client	Alec	Nov 9, 2003 01:15 PM	1	Normal	Hosting

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

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

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



Ticket

Ticket Status	New
Client	Alec
Ticket Subject *	That thing does not work!!!
Category	Hosting
Priority	Normal
Queue	1

New Event

Ticket Event	Comment ticket
Visible to client	☑
New Comment	Please elaborate ...

Ticket History

Nov 9, 2003 01:15 PM Alec <alec@plesk.ru>

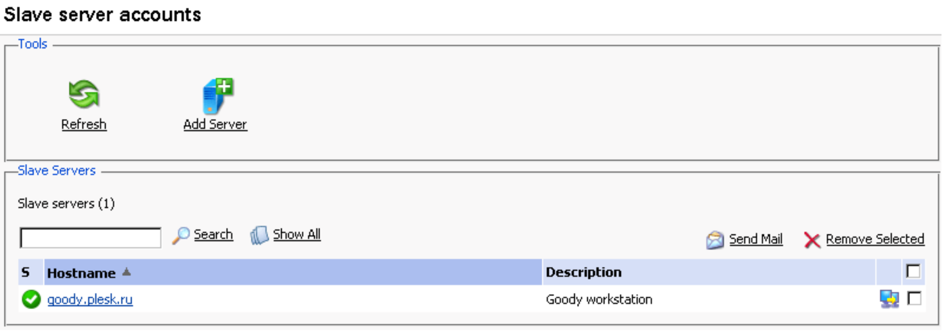
Help! I need some qualified assistance...

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

Using Master Feature

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

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



Slave server accounts

Slave servers (1)

S	Hostname ▲	Description	□
✓	goody.plesk.ru	Goody workstation	□

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

Table 3.1. The slave server status icons.

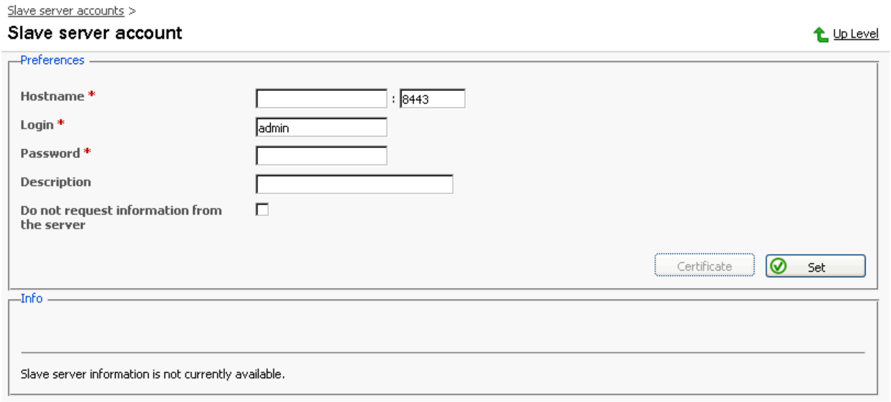
Icon	Meaning
✓	means that the slave server is functioning normally
❗	means that some system service at the slave server is experiencing problems
!	means that on the slave server some client has exceeded allocated disk space or traffic limitations in at least one of the client's domains. The Plesk system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

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

Registering a Slave Server Account

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

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



Slave server accounts >

Slave server account

Preferences

Hostname * : 8443

Login * admin

Password *

Description

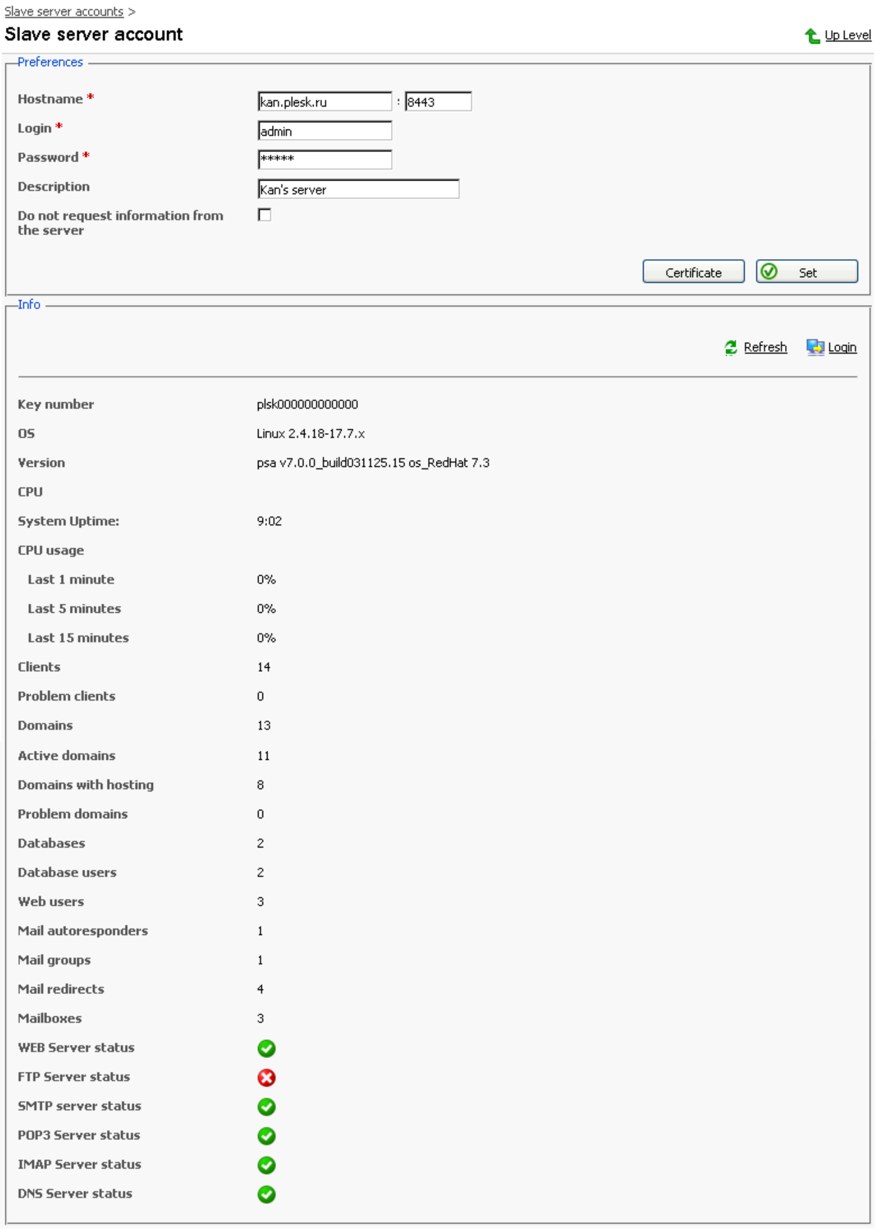
Do not request information from the server □

Info

Slave server information is not currently available.

3. Enter the hostname and port number in the appropriate fields, enter login name, and password for Plesk to be able to log on to the given slave server. You may also wish to type in a description for the slave server. Select the Do not request information from the server checkbox, if you do not wish the detailed slave server information to be retrieved.

4. Click Set. The Slave server account page will be updated with server details and statistics:



Slave server accounts >

Slave server account

Up Level

Preferences

Hostname *	kan.plesk.ru : 8443
Login *	admin
Password *	*****
Description	Kan's server
Do not request information from the server	□

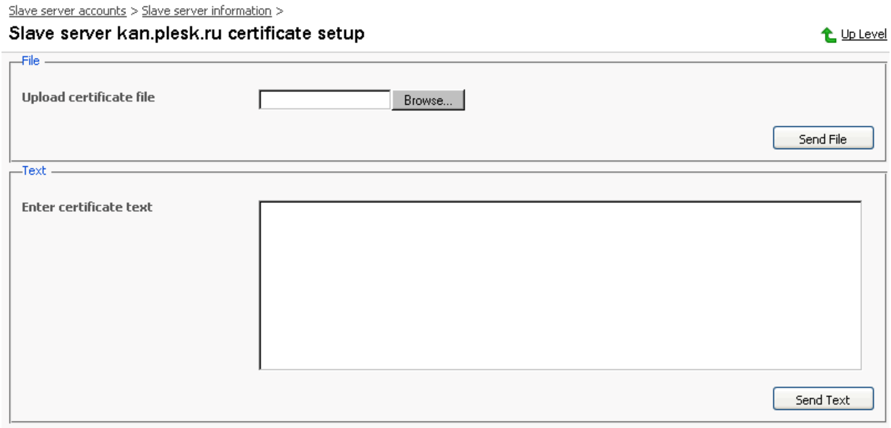
Certificate | Set

Info

Refresh | Login

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

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



Slave server accounts > Slave server information >

Slave server kan.plesk.ru certificate setup

Upload certificate file

Enter certificate text

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

To refresh information on the slave server, click Refresh.

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

Editing a Slave Server Account

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

1. In the list of slave server accounts, click on the host name of the slave server whose account you wish to edit. The Slave server account page appears, displaying detailed slave server account information.

2. Click in any text box to edit the information.

3. When you are done editing, click Set to save the changes made. The changes will take effect immediately.

Logging on to a Slave Server

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

- On the Slave Servers Administration page, select the slave server you wish to log on to and click the corresponding icon.

- You can also use the icon located on the Slave server account page.

Removing a Slave Server Account

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

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

Viewing Server Statistics

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

The report lists several informative statistics:

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

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

OS: Displays operating system version.

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

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

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

Memory Usage: displays the amount of memory used

Swap Usage: displays the amount of swap space used

Hard Disk Usage:

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

Domains:

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

To access the System Statistics page, follow these steps:

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

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

Viewing License Key Properties

To view the detailed information on Plesk capabilities provided by the currently installed license key, click the Key Info icon on the Server Administration page.

The license key information is arranged in the form of table, displaying names of various functionality properties provided by the key in the left part, and the values of limits set by the key for each of the properties in the right part.

Viewing Information on Plesk Components

To access information on the components controllable under Plesk that are installed on the current server, select the Component Info icon on the Server Administration page.

NOTE

The component version information is refreshed every 24 hours. When updating system components, you might have to reboot the server or restart the "Plesk Management Service" to have the component versions displayed correctly.

Submitting a Request for Online Server Support

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

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

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

NOTE

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

Rebooting the System

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

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

IMPORTANT

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

Shutting Down the System

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

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

IMPORTANT

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

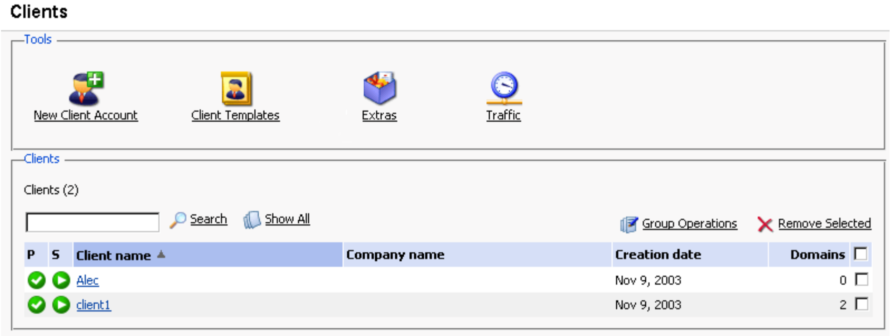
Chapter 4. Managing User Accounts

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

Creating a New Client Account

Follow these instructions to create a new client account:

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



P	S	Client name ▲	Company name	Creation date	Domains ☐
✓	▶	Alec		Nov 9, 2003	0 ☐
✓	▶	client1		Nov 9, 2003	2 ☐

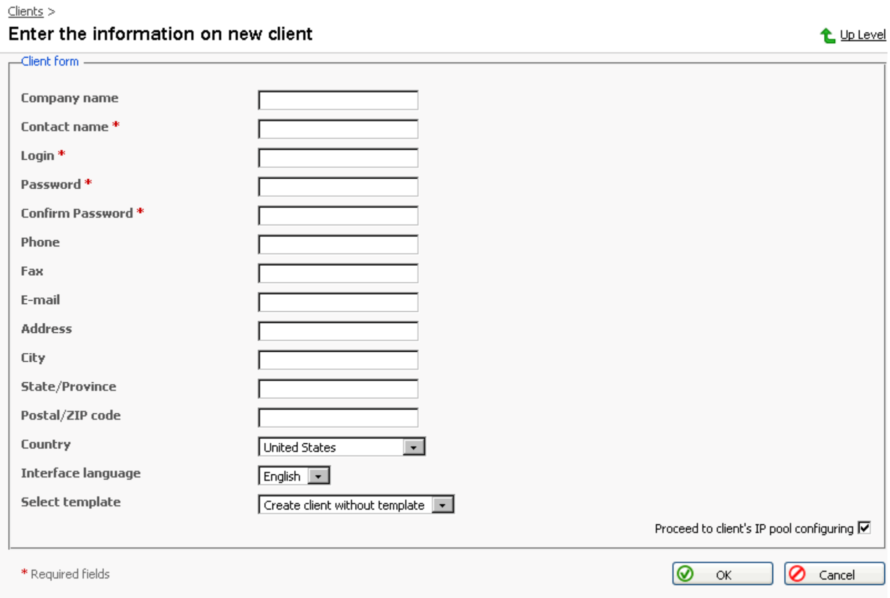
The client's status is represented by two icons:

Table 4.1. The client state/status icons.

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

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

2. Click New Client Account. The Client form appears prompting you to enter all the information required:



Clients >

Enter the information on new client

Client form

Company name	
Contact name *	
Login *	
Password *	
Confirm Password *	
Phone	
Fax	
E-mail	
Address	
City	
State/Province	
Postal/ZIP code	
Country	United States
Interface language	English
Select template	Create client without template

Proceed to client's IP pool configuring ☑

* Required fields

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

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

NOTE

Use only alphanumeric symbols in the login name.

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

NOTE

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

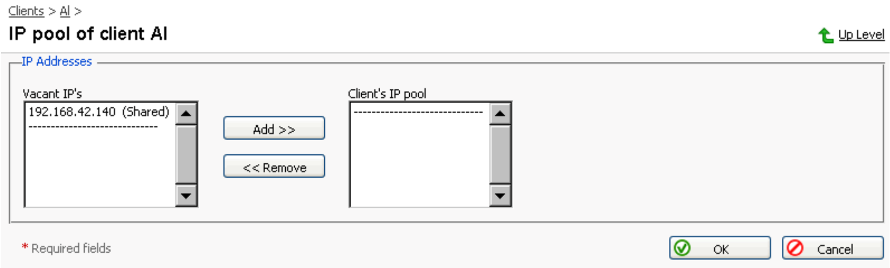
- Confirm password. In order to make sure that you have entered the password you wanted, re-enter it in this field.

4. Review the entered information. Edit data in any text box by clicking and editing the specific word or phrase.

5. Select a template from the drop-down box to create the client account by the template. This option may be unavailable if not supported by your license key.

6. To proceed directly to configuring the IP pool for the new client account, leave the Proceed to client's IP pool configuring checkbox selected.

7. When you are satisfied that the information is complete and correct, click OK. The client's IP pool opens:



Clients > Al >

IP pool of client Al

IP Addresses

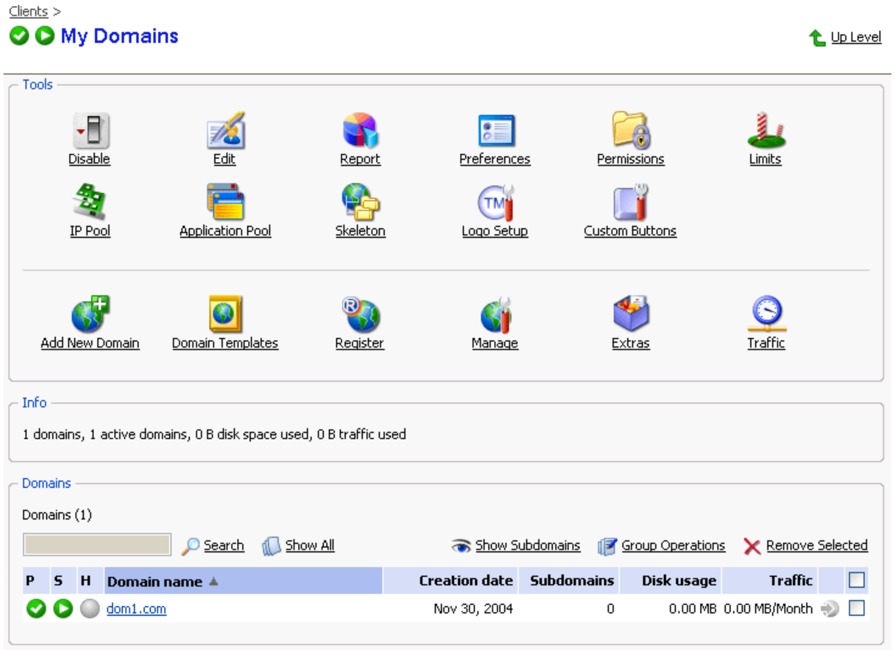
Vacant IP's: 192.168.42.140 (Shared)

Client's IP pool: -----------------------------

* Required fields

8. Select a desired IP address in the list of Vacant IPs, and click Add>> to add it to the pool.

9. Click OK. Now the client account is created, and the client is provided with the IP addresses necessary for creating domains. The Client Home page appears, providing you with client account management functions:



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

Domains (1)

P	S	H	Domain name ▲	Creation date	Subdomains	Disk usage	Traffic	□
✓	▶	●	dom1.com	Nov 30, 2004	0	0.00 MB	0.00 MB/Month	□

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

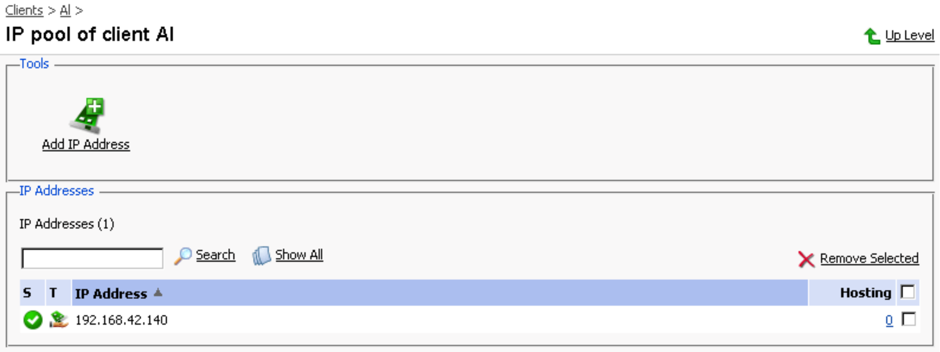
Note that if you skipped the IP allocation procedure during account creation, you can do this later using the Client's IP pool function, which is described in the following section. You should keep in mind that the client will not be able to create domains until he or she is granted an IP address.

Managing IP Pool

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

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

Click the IP Pool icon on the Client Home page to access the Client IP pool. It displays the list of IP addresses that were granted (exclusively or as shared) to this client:



Clients > Al >

IP pool of client Al

IP Addresses (1)

S	T	IP Address ▲	Hosting □
✓		192.168.42.140	0 □

Table 4.2. The IP state/type icons.

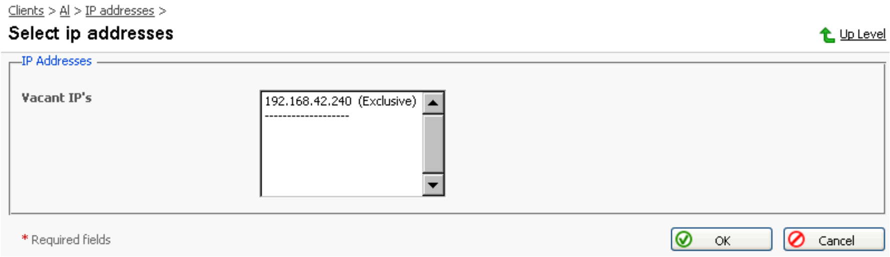
Icon	Meaning
The state icon indicates the system state of the IP address:	
✓	means that the IP address functions properly
❗	means that there is something wrong with the IP address.
The type icon indicates how the IP address was granted:	
👑	means that the IP address was granted exclusively
	means that the IP address was granted as shared

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

Adding IP address to the client's IP pool

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

1. At the Client IP pool page, click Add IP Address icon. IP selection dialog will open:



Clients > Al > IP addresses >

Select ip addresses

Vacant IP's: 192.168.42.240 (Exclusive)

* Required fields

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

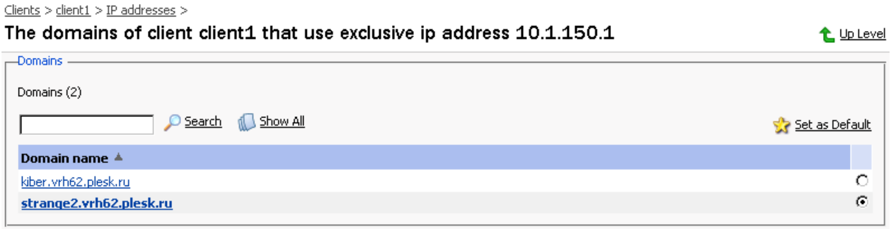
> **NOTE**
>
> You can select several IP addresses at a time.

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

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

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

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



The domains of client client1 that use exclusive ip address 10.1.150.1

Domains (2)

Domain name ▲	
kiber.vrh62.plesk.ru	○
strange2.vrh62.plesk.ru	●

2. To jump to a Domain administration page, simply click on the name of the domain.

3. To set a domain as default for the exclusive IP address, select the domain using the corresponding radio button and click ★ Set as Default. The default domain name will be displayed in bold.

4. Click Up Level to return to the Client IP pool page.

Assigning an SSL certificate for an exclusively granted IP address

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

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

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

Removing an IP address from the client's IP pool

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

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

To remove an IP address(-es):

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

Setting the Permissions for Operations

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

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

2. In order to allow (forbid) the client to perform a specific operation, select (deselect) the corresponding checkbox.

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

3. When you are done editing, click OK.

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

Setting the Resource Usage Limits

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

1. Click the Limits icon on the Client Home page. The Client limits page will appear listing the resource types.
2. To set a limit value for a specific resource, deselect the corresponding "Unlimited" checkbox and enter the value into the corresponding input box.

   Mailbox quota defines the amount of disk space that a given client is allowed to have per mail box on a single domain.

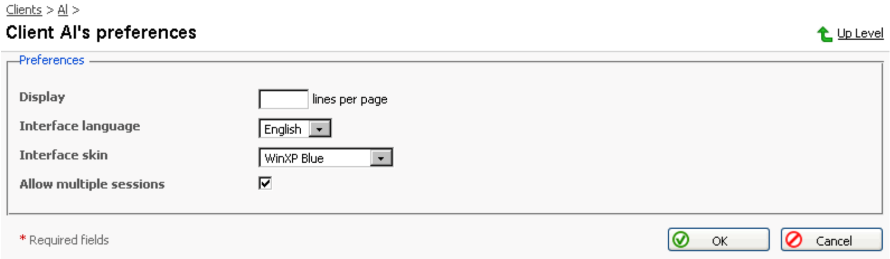
   Note, that you can impose the tighter limit on the mailbox size from the Domain Limits page and in the mailbox properties.
3. At this page you can also set validity period for the given client account. To this effect, deselect the corresponding "Unlimited" checkbox, and define the desired account expiration date in the Validity period input fields.
4. When you are done editing, click OK.

Setting the Interface Preferences

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

To change the interface preferences, follow these steps:

1. Click the Preferences icon at the Client home page. The client preferences page opens:



Clients > Al >

Client Al's preferences

Preferences

Display: lines per page

Interface language: English

Interface skin: WinXP Blue

Allow multiple sessions: ☑

* Required fields

2. To define the number of list entries that will be shown per page, click into the Display ... lines per page input box and type in the desired number.

3. If you have several language packs installed for Plesk, you can select the client’s interface language. Select the desired language from the Interface language drop-down box.

4. To set a skin to be used for client's sessions, select one from the Interface skin drop-down box.

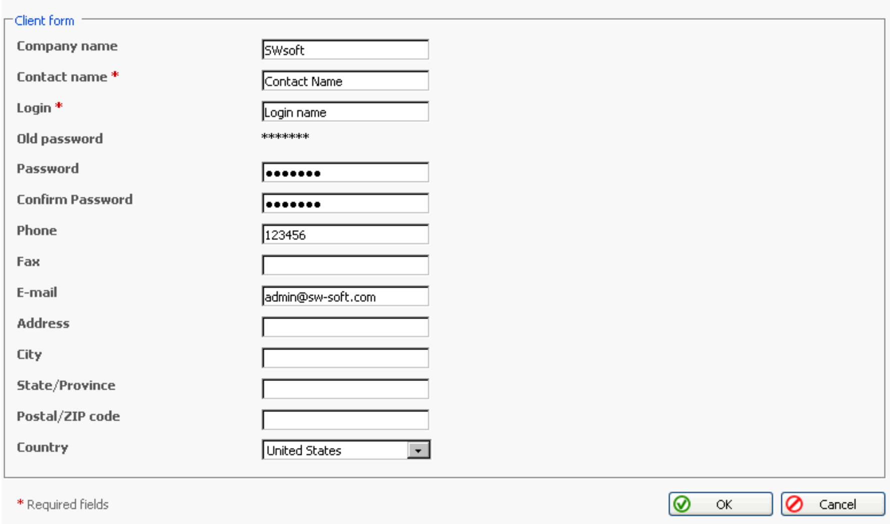
5. To allow multiple simultaneous sessions under client's login name, select the Allow multiple sessions checkbox.

6. When you are done editing, click OK.

Editing Client Information

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

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



Client form

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

* Required fields

2. To modify an item in the client's data, click in a specific text box to enter data, or use the Tab key to move from one text box to the next. The following data fields are required:

   - Contact Name - This is the name that appears in the Clients list. The contact name must be unique in order to work with it in the Plesk system.

   - Login - By assigning a login name to a client, you grant that user access to Plesk for independent account administration. Each client's Plesk Control Panel login name must be unique in the system.

NOTE

Use only alphanumeric symbols in the login name.

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

NOTE

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

   - Confirm password. In order to make sure that you have entered the password you wanted, re-enter it in this field.

3. Review the entered information. Edit data in any text box by clicking and editing the specific word or phrase.

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

IMPORTANT

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

Viewing the Client Report and Statistics

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

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

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

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

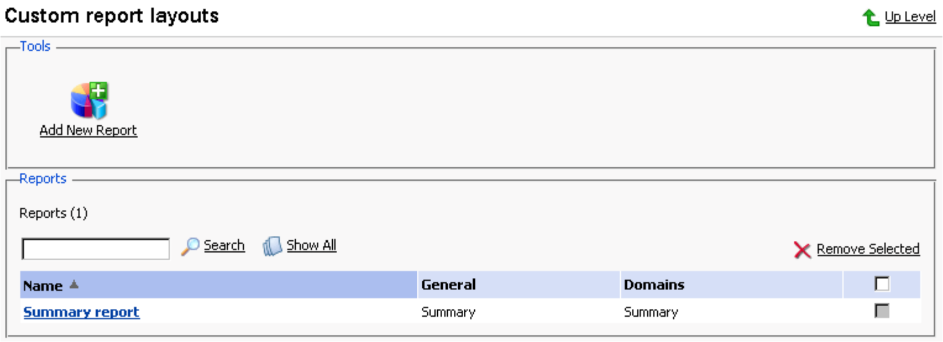
Viewing traffic history

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

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

Customizing a report layout

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



Custom report layouts

Up Level

Tools

Add New Report

Reports

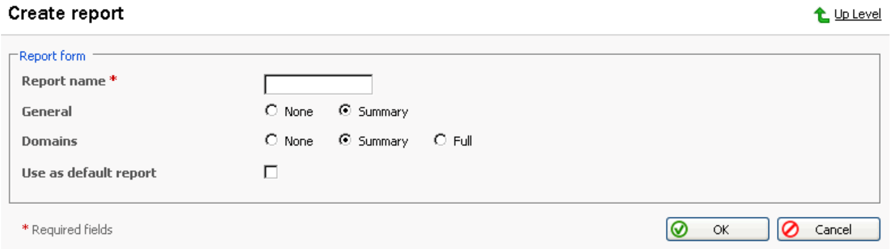
Reports (1)

Search Show All Remove Selected

Name ▲	General	Domains	☐
Summary report	Summary	Summary	☐

To add a new custom layout, follow these steps:

1. Click the Add New Report icon. The page appears:



Create report

Up Level

Report form

Report name *	
General	○ None ● Summary
Domains	○ None ● Summary ○ Full
Use as default report	☐

* Required fields

OK Cancel

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

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

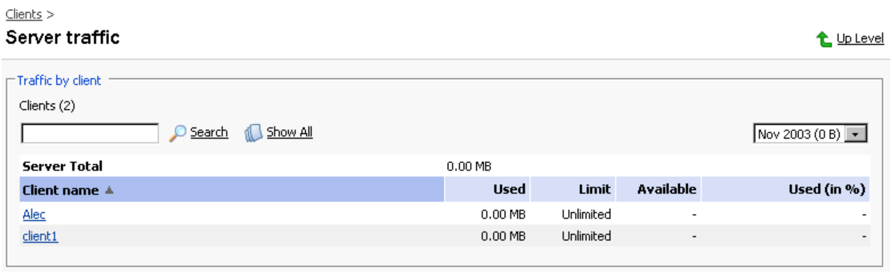
To edit a custom layout, select its title in the list.

Viewing Traffic Statistics by Clients

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

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

statistics:



Clients >

Server traffic

Clients (2)

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

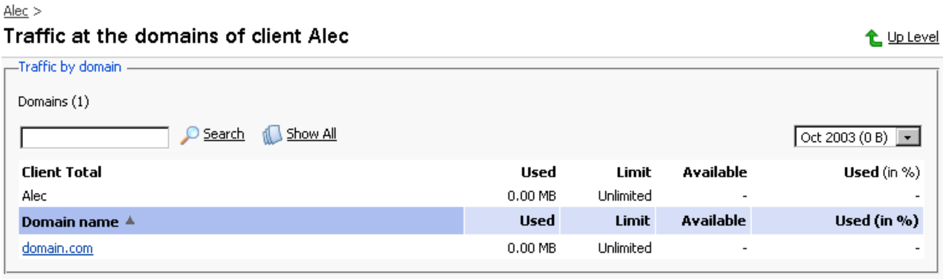
Presented in the table are the data on amounts of traffic used by clients.

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

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

Viewing Traffic Statistics by Client's Domains

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



Alec >

Traffic at the domains of client Alec

Domains (1)

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

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

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

To view the traffic statistics at the domain and the data on traffic used by domain services, click on a domain name.

Deactivating/Activating a Client Account

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

To deactivate a client's account:

1. On the Client Home page of the selected client, click Disable. The confirmation will appear querying whether you actually wish to change the status of the selected client's account.
2. Click OK.

To activate an account, follow these steps:

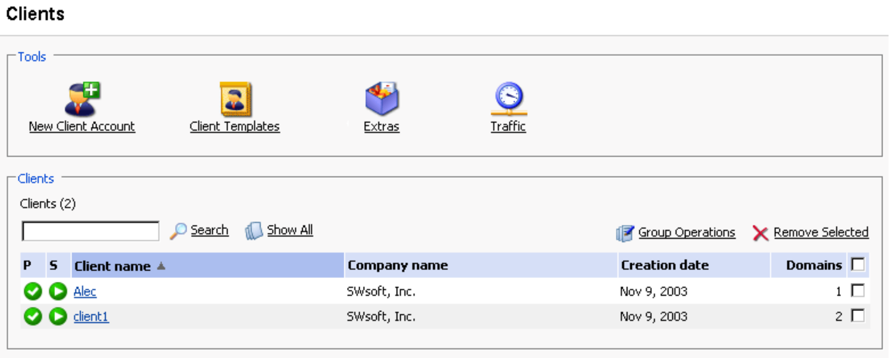
1. On the Client Home page of the selected client, whose account is deactivated, click Enable. The confirmation will appear querying whether you actually wish to change the status of the selected client's account.
2. Click OK.

Performing Group Operations on Accounts

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

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

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



Clients

Tools

Clients

Clients (2)

P	S	Client name ▲	Company name	Creation date	Domains ☐
✓	▶	Alec	SWsoft, Inc.	Nov 9, 2003	1 ☐
✓	▶	client1	SWsoft, Inc.	Nov 9, 2003	2 ☐

2. Select the clients, whose accounts you wish to modify by checking the corresponding checkboxes.

3. Click the Group Operations icon. The Group Operations page will appear, divided into three groups:
   - The Permissions group is used for setting permissions for various operations
   - The Limits group is used for modifying limits for granted resources
   - The Modified accounts area lists the client accounts selected for modification.

4. To set permissions, select the **`Do not change`**, **`Enable`** or **`Disable`** radio button for the corresponding type of operation.

5. To edit limit settings for a particular resource type:

   5.1. First, select the desired action from the drop-down box:
   - Leave the **`Do not change`** option selected, if you do not wish to make a change
   - Select **`Unlimited`** if you wish not to limit the resource usage
   - Select the **`Value`** option in order to specify a new value for the resource limit
   - Select **`Increase (+)`**, to specify the value by which to increment the presently set resource limit value
   - Select **`Decrease (-)`**, to specify the value by which to decrement the presently set resource limit value

   5.2. Then, specify the value of the new resource limit in the corresponding input field.

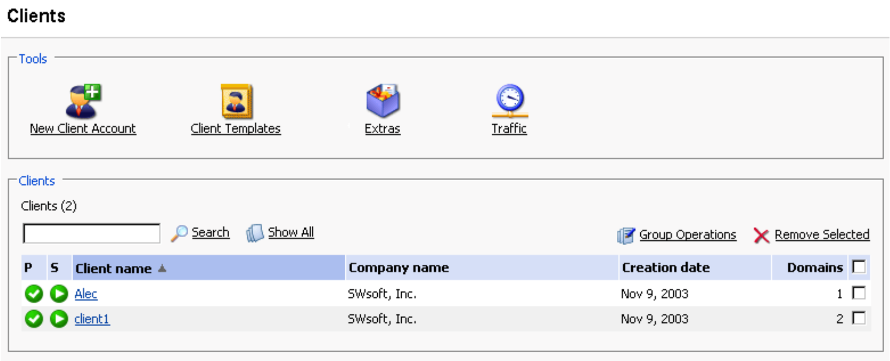
   5.3. If you chose to increase/decrease the presently set limit value, use the drop-down box to select **`units`** if you wish to modify the limit value by a quantity of commonly used units or **`%`** if you wish to modify the limit value by a particular percentage.

6. Click OK to apply the new settings to the selected client accounts.

Removing Client Accounts

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

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

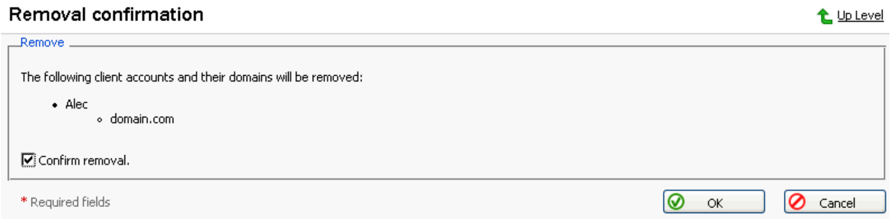


Clients (2)

P	S	Client name ▲	Company name	Creation date	Domains □
✓	▶	Alec	SWsoft, Inc.	Nov 9, 2003	1 □
✓	▶	client1	SWsoft, Inc.	Nov 9, 2003	2 □

2. Select the clients, whose accounts you wish to remove by checking the corresponding checkboxes.

3. Click Remove Selected. The Removal confirmation page appears:



The following client accounts and their domains will be removed:

- Alec
  - domain.com

☑ Confirm removal.

* Required fields

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

Chapter 5. Administering Domains

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

Creating a Domain

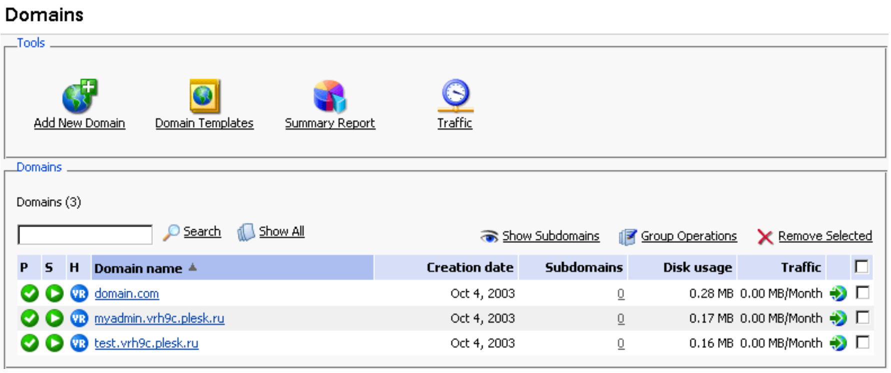
A domain is a virtual address on the Internet for any organization or entity. Technically, a domain is defined as a group of networked computers (servers) that represent an organization and provide network services; however, several domains could reside on one server, in dedicated space provided by a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

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

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

To create a new domain, follow these steps:

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



Domains

Domains (3)

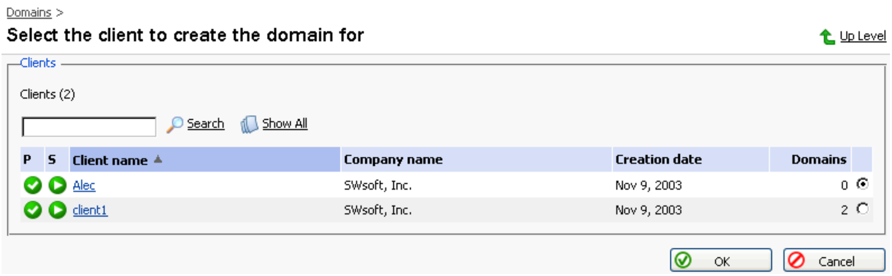
P	S	H	Domain name ▲	Creation date	Subdomains	Disk usage	Traffic		□
✓	▶	VR	domain.com	Oct 4, 2003	0	0.28 MB	0.00 MB/Month	➔	□
✓	▶	VR	myadmin.vrh9c.plesk.ru	Oct 4, 2003	0	0.17 MB	0.00 MB/Month	➔	□
✓	▶	VR	test.vrh9c.plesk.ru	Oct 4, 2003	0	0.16 MB	0.00 MB/Month	➔	□

Each domain name is accompanied by the following icons:

Table 5.1.

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

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



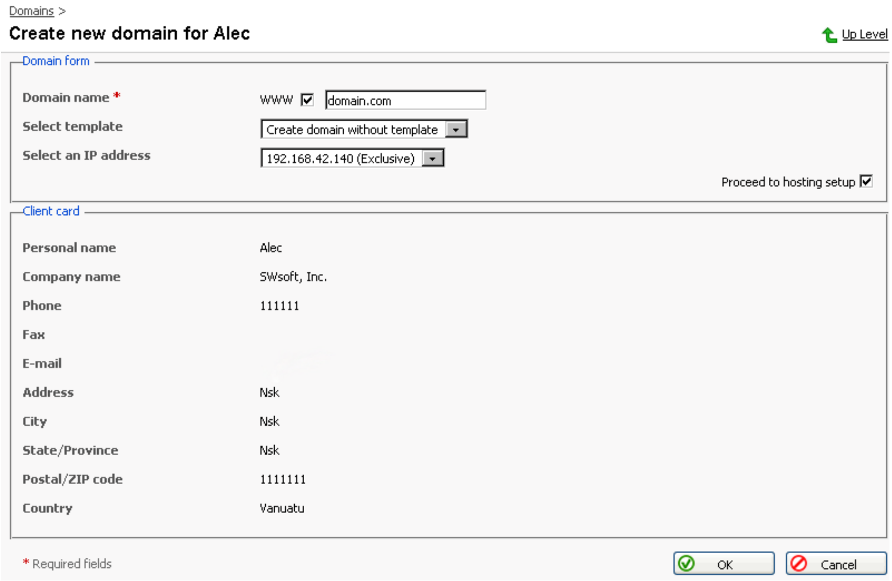
Domains >

Select the client to create the domain for

Clients (2)

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

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



Domains >

Create new domain for Alec

Domain form

Domain name *	WWW ☑ domain.com
Select template	Create domain without template
Select an IP address	192.168.42.140 (Exclusive)

Proceed to hosting setup ☑

Client card

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

* Required fields

NOTE

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

4. 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.

5. Select a template to be applied from the drop-down list, if you wish this domain to be created by a template.

6. Select the IP address to be used for hosting from the drop-down list.

7. 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.

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

IMPORTANT

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

Managing Hosting

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

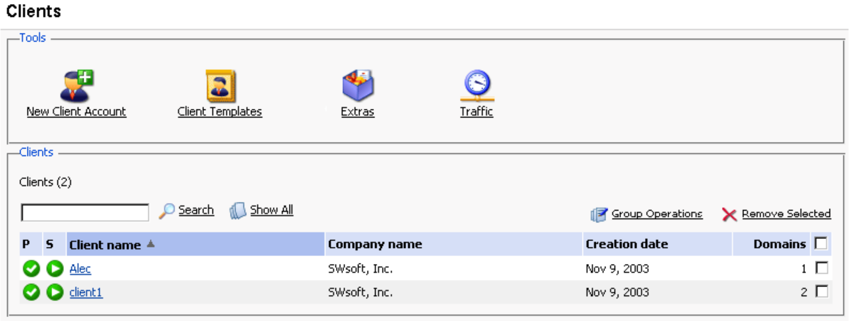
- Physical hosting: the most common type of hosting service, creating a virtual host (disk space on the local server) for the client. The client controls and publishes his own web site without having to purchase a server and dedicated communication lines.
- Standard forwarding: with this type of forwarding,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

Accessing the Hosting Setup Wizard

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

•

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

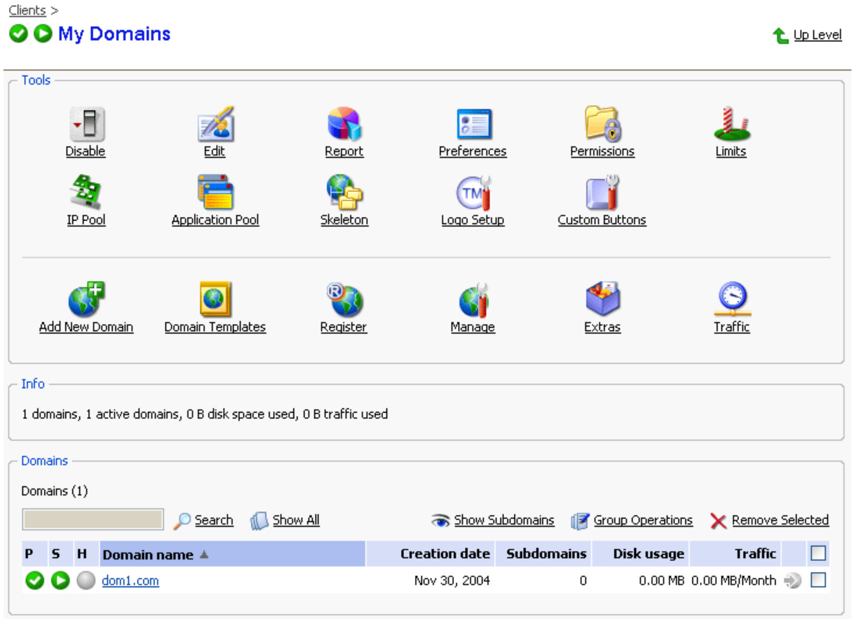


Clients

Clients (2)

P	S	Client name ▲	Company name	Creation date	Domains □
✓	▶	Alec	SWsoft, Inc.	Nov 9, 2003	1 □
✓	▶	client1	SWsoft, Inc.	Nov 9, 2003	2 □

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



Clients >

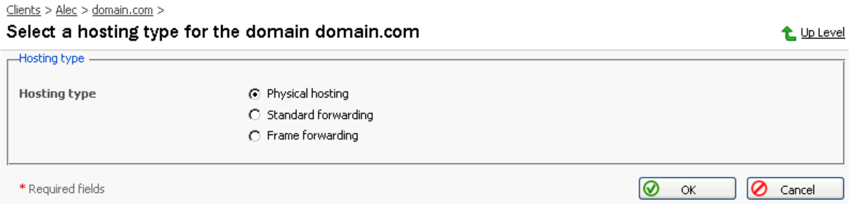
My Domains

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

Domains (1)

P	S	H	Domain name ▲	Creation date	Subdomains	Disk usage	Traffic	□
✓	▶	●	dom1.com	Nov 30, 2004	0	0.00 MB	0.00 MB/Month	□

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



Clients > Alec > domain.com >

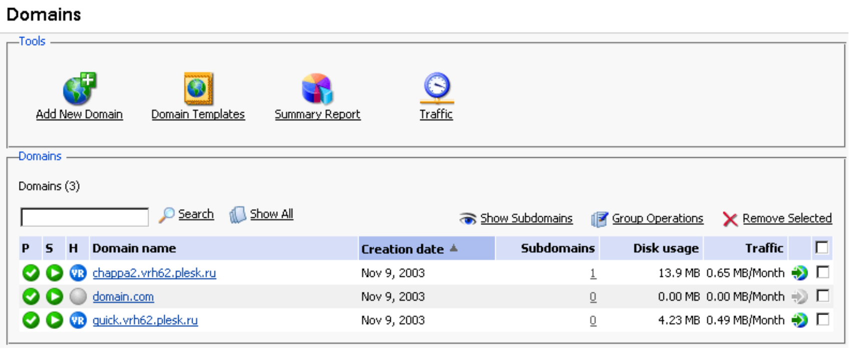
Select a hosting type for the domain domain.com

Hosting type ● Physical hosting
○ Standard forwarding
○ Frame forwarding

* Required fields

•

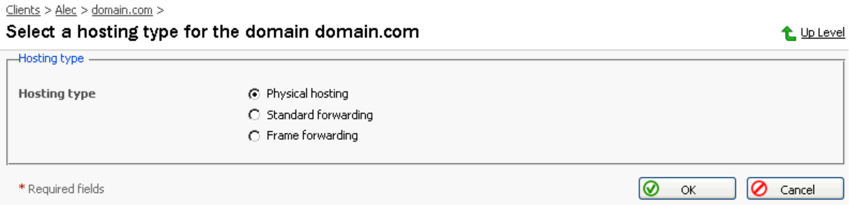
1. Select the Domains shortcut in the navigation pane. The Domains list page will open:



Domains (3)

P	S	H	Domain name	Creation date ▲	Subdomains	Disk usage	Traffic	□
✓	▶	VR	chappa2.vrh62.plesk.ru	Nov 9, 2003	1	13.9 MB	0.65 MB/Month	□
✓	▶	●	domain.com	Nov 9, 2003	0	0.00 MB	0.00 MB/Month	□
✓	▶	VR	quick.vrh62.plesk.ru	Nov 9, 2003	0	4.23 MB	0.49 MB/Month	□

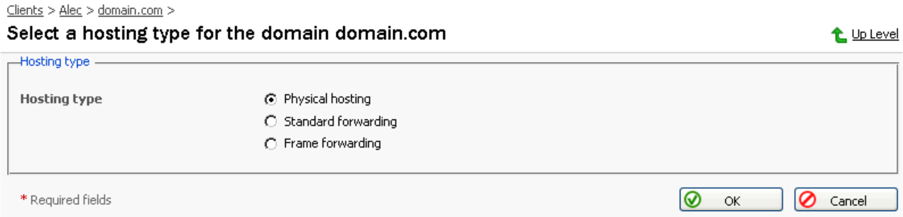
2. Click on the ● icon to the left of the domain name. The hosting type selection page opens:



Select a hosting type for the domain domain.com

Hosting type: ● Physical hosting ○ Standard forwarding ○ Frame forwarding

- When on the Domain Administration page click the Setup icon. The Hosting Type Selection page appears:



Select a hosting type for the domain domain.com

Hosting type: ● Physical hosting ○ Standard forwarding ○ Frame forwarding

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 an IP address from the drop-down list displaying available IP addresses in a client's IP pool.

NOTE

When editing physical hosting account, if you change IP type to shared, the certificate previously assigned to the IP will be changed to the default one.

3. 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 provides https protocol, as a result, users access the domain with the command `https://newdomain.com`. If you want to grant permission to your client to implement an SSL certificate, make sure a check mark appears in the SSL support box.

4. You should set an FTP/Microsoft FrontPage 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, and allow access to Microsoft FrontPage, click in the FTP/Microsoft FrontPage Login box, enter or edit a login name to be used for accessing FTP file transfer services on the domain and Microsoft FrontPage interface.

5. Click in the FTP/Microsoft FrontPage Password box and enter or edit the password.

6. 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.

7. Hard disk quota field allows you to set the limit for the maximum disk space amount available for use by this domain.

8. In the System access drop-down list, select the system access availability.

NOTE

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

9. To allow the use of Microsoft FrontPage Server Extensions, select 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 Microsoft FrontPage support box.

NOTE

Plesk creates a special user group for your site called FPSE_<sitenumber>, where <sitenumber> is the IIS identifier site to overcome possible problems outlined at http://www.microsoft.com/resources/documentation/sts/2001/all/proddocs/en-us/admindoc/ows

10. Tab to the Authoring enabled option. You can authorize or disable remote editing of the web site using Microsoft FrontPage. This setting is changeable by the Admin, Client, and Domain User logins to the control panel. For security purposes the main server administrator should notify their Clients and Domain Users that Microsoft FrontPage authoring should be disabled whenever not in use. To activate Microsoft FrontPage authoring, make sure this option is selected. If you want to turn off Microsoft FrontPage authoring, select the Authoring disabled option.

11. If FrontPage authoring is selected, then the FrontPage Admin Login, FrontPage Admin Password, and Confirm Password fields must be entered. 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.

12. Tab to the Microsoft ASP support checkbox. It enables the development of dynamic web applications with embedded code.

13. Tab to the Microsoft ASP.NET support checkbox. It enables the development of .NET dynamic web applications.

14. Tab to the SSI support check box. SSI stands for 'server-side includes', a type of HTML comment that directs the web server to dynamically generate data for the Web page whenever information is requested. SSI can also be used to execute programs and insert the results; therefore they represent a powerful tool for web developers. If your client wants to support SSI, make sure a check mark appears in the SSI box.

15. Tab to the PHP support check box. PHP is a server-based HTML embedded scripting language used to create dynamic Web pages. If your client wants to support PHP scripting in HTML documents, make sure a check mark appears in the PHP box. The run as ISAPI extension checkbox controls the way the PHP interpreter is called. When it is unchecked, the PHP interpreter is called through the CGI interface. When it is set, the ISAPI version of PHP is used, which is tighter connected to the web server therefore use of this option will give a performance boost.

16. Tab to the CGI support check box. CGI is a set of rules describing how a web server communicates with another piece of software on the same

machine, and how the other piece of software (based on the CGI program) communicates back to the web server. If your client wants to support CGI, make sure a check mark appears in the CGI box.

17. Tab to the Perl support check box. Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use it for a vast number of automation tasks. Many CGI programs are written in Perl. If your client wants to support Perl, make sure a check mark appears in the Perl support checkbox.
18. Tab to the Python support checkbox. Python is an interpreted, interactive, object-oriented, high-level programming language. Python is good for many system administration type tasks and for CGI programming and is also extensively used as a graphical user interface development aide. If your client wants to support Python, make sure a check mark appears in the Python support checkbox.
19. Tab to the ColdFusion support checkbox. This enables the ColdFusion scripting.

> **NOTE**
>
> ColdFusion should be installed on the server with Default Web Site chosen on the Web Server Selection step of installation. Otherwise, ColdFusion support will always be activated for all domains with enabled Physical hosting, regardless to the corresponding checkbox status. If you do not know or remember the way ColdFusion was installed, reinstall it respectively. For more details see Installing Plesk 7.5 for Windows chapter in the Installation Guide.

20. 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.
21. In the Web statistics drop-down box, select the web statistics software to be used for this domain. This package is accessible via the Plesk interface within the given domain's Report page or via the Internet using the URL `http://'domainname'/webstat`.
22. The section IIS Application Pool provides the Use dedicated checkbox. When it is checked, IIS creates a separate application pool for every web application it runs. This way, if one of them crashes, it does not take others with it, they continue to work normally. You may want to leave this option disabled for backward compatibility with some applications utilizing IIS functionality which works only in the common pool mode.
23. When you are sure that you have fully defined the hosting services for this domain, click OK.

Configuring Forwarding Hosting

Configuring Standard Forwarding

To set up standard forwarding, follow these steps:

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

Configuring Frame Forwarding

Follow these steps to configure frame forwarding:

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

Deleting Hosting Configuration

You can change hosting type for a domain only after you delete the current hosting configuration. To delete the current hosting configuration, use the Delete icon, located at the Domain administration page, Hosting group.

Setting Domain Level Limits

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

1. Click the Limits icon on the Domain administration page. The Domain limits page will appear containing the list of resource limits. At this page you can set the limits on the following resources:
   - Number of subdomains
   - Amount of disk space
   - Amount of traffic
   - Number of web users
   - Number of MS SQL databases
   - Number of MySQL 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.

Mailbox quota is the amount of disk space that a single mail user in this domain is allowed to have.

Note, that you can impose the tighter limit on the mailbox size in the mailbox properties.

3. To set the validity period for the domain, define the required domain expiration date in the Validity period field.

4. When you are done with editing, click OK.

Editing Domain Preferences

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

1. Click the Preferences icon at the Domain administration page. The Domain preferences page will open.

2. Check or uncheck the WWW prefix checkbox to determine whether the given domain will allow the www prefix to be used to access the domain. If the box is checked, Internet users will be able to access a domain (i.e. domain.com) by specifying either the domain name itself or the domain with the "www" prefix. If the box is unchecked it will not be accessible with the "www" prefix (i.e. www.domain.com).

3. To change the domain name, click in the Domain name field, displaying the given domain name and edit it as desired.

IMPORTANT

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

4. To set the traffic statistics retention period, select the Retain traffic statistics for [__] Months checkbox, and type the number in the input field provided.

5. Click OK to submit the changes and return to the Domain administration page.

Customizing DNS Settings

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

> ℹ **NOTE**
>
> Improper setup of DNS results in improper functioning of web, mail and FTP services.

Types of DNS Records

There are five types of accessible DNS records:

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

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

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

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

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

Changing DNS Settings

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

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

- If you wish to turn DNS on or off for the domain, click the Enable or Disable icon respectively.
- Turning the DNS zone off will refresh the page, so that only a list of nameservers remains.
- If you are running remote DNS, and therefore want to turn DNS off for the domain, you should first create the appropriate NS entries for the domain and remove any inappropriate NS entries possibly created by the default DNS template created in the Server DNS section. At that point, turn DNS off. You see that the name server(s) for the domain remains listed as a link.
- You can perform a test on these name servers by selecting any of them. Selecting any name server will perform an NSLookup to check for the DNS records for your specific domain on that specific name server. NSLookup is used to verify the A record for the domain, the CNAME record for www, and the MX record to ensure that these basic records are resolved properly on the remote name server. The results are interpreted and presented through the user interface.

3. In order to add a DNS entry, select the type of record you wish to create and click Add. Each record type has its own different setup. When creating DNS entries within a specific DNS zone the name of the zone must be present for all entries. Plesk sets the screen up with certain unchangeable fields in order to prevent possible errors within the zone.

   - For an A record you will need to enter the domain name for which you wish to create an A record. If you are simply defining an A record for your main domain, then you should leave the available field empty. If you are defining an A record for a name server then you will need to input the appropriate entry for the given name server (ie. ns1). Then, you need to enter the appropriate IP address to which to associate the domain name. Then select OK to submit your entry.
   - For a NS record, you will need to enter the domain name for which you wish to create the NS record. If you are defining an NS record for your main domain, then you will leave the available field blank. Then enter the appropriate name server name in the field provided. You will need to enter the complete name (i.e. ns1.mynameserver.com). Then select OK to submit your entry.
   - For a MX record, you will need to enter the domain for which you are creating the MX record. For the main domain, you would simply leave

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

- For a CNAME record, you will need to first enter the alias domain name for which you wish to create the CNAME record. You then need to enter the domain name within which you want the alias to reside. Any domain name can be entered. It does not need to reside on the same server. Select OK to submit your entry.
- For a PTR record you will first enter the IP address/mask for which you wish to define the pointer. Then enter the appropriate domain name for this IP to be translated to. Select OK to submit your entry.

4. To remove a DNS record, select it using a corresponding checkbox, and click Remove Selected. Before anything is processed you will be asked to confirm the deletion.

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

To switch the DNS zone, follow these steps:

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

To switch the DNS zone type back to master, click the 🔄 Switch icon again. You will return to the DNS Settings page.

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

Managing Mail

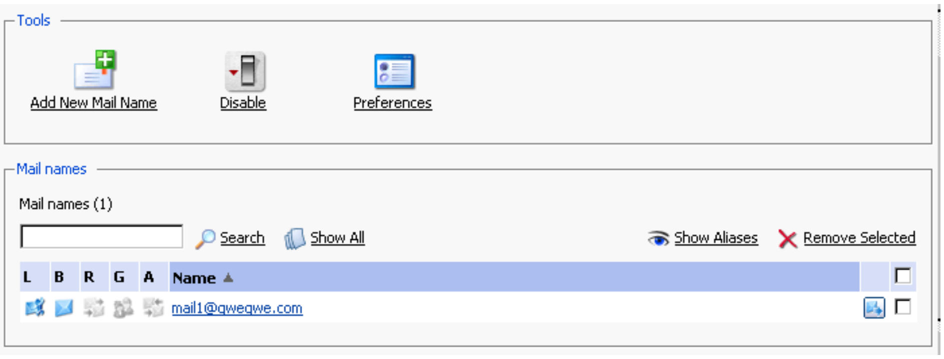
Using Plesk, you can create and manage email boxes for individuals within a domain, or your client can manage the e-mail accounts via domain self-administration. As an administrator, you can use the following e-mail administration functions:

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

Managing Mail Names

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

Domain administration page to access the Mail Names Management functions:



L	B	R	G	A	Name ▲		□
					mail1@qweqwe.com		□

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

You can allow the use of web-based e-mail for the domain through webmail.'domain name' and set up a strategy used to handle mail that is received for nonexistent users at this domain.

1. Click Preferences

2. Select a strategy of handling mail to nonexistent user:

   - To utilize a mail bounce message, select the radio button for Bounce with phrase and enter the appropriate text. With this option selected, mail messages that are recieved for nonexistent user at the domain are sent back with the specified phrase. If your mail server does not support custom mail bounce messages, the corresponding input field is hidden and the mail server bounces the mail with its default phrase.

   - To utilize a catch-all e-mail address, select the radio button for Catch to address and enter the appropriate e-mail address. With this option selected, all mail messages addressed to nonexistent user at the domain are forwarded to the specified e-mail.

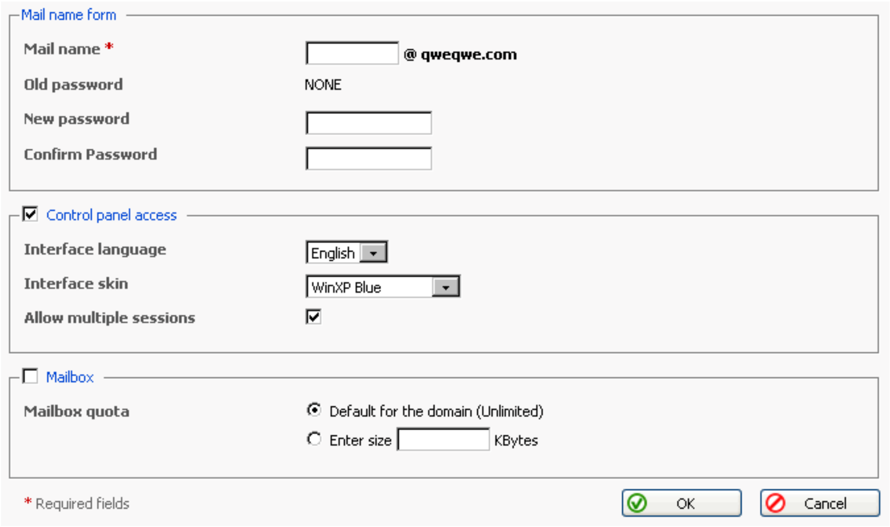
   - If you wish mail to nonexistent user to be silently discarded, select the Discard radio button.

3. Check or uncheck the WebMail checkbox to allow or disallow the use of web-based e-mail for the given domain through webmail.'domain name'.

4. Click OK to submit the changes.

To create a new mail name, follow these steps:

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



Mail name form

Mail name *	@ qweqwe.com
Old password	NONE
New password	
Confirm Password	

☑ Control panel access

Interface language	English
Interface skin	WinXP Blue
Allow multiple sessions	☑

☐ Mailbox

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

* 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 from the drop-down boxes. Check the Allow multiple sessions checkbox to allow multiple sessions under the same mail user's login.

4. To create a mailbox, select the Mailbox checkbox, and specify the mailbox quota if desired.

5. Click OK to submit all changes.

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

- indicates permission to use the control panel,
- represents a mailbox,
- represents a mail redirect
- represents a mail group
- represents a mail autoresponder

These icons are displayed in gray when they 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 send an e-mail message to the mail user, click the corresponding icon.

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.

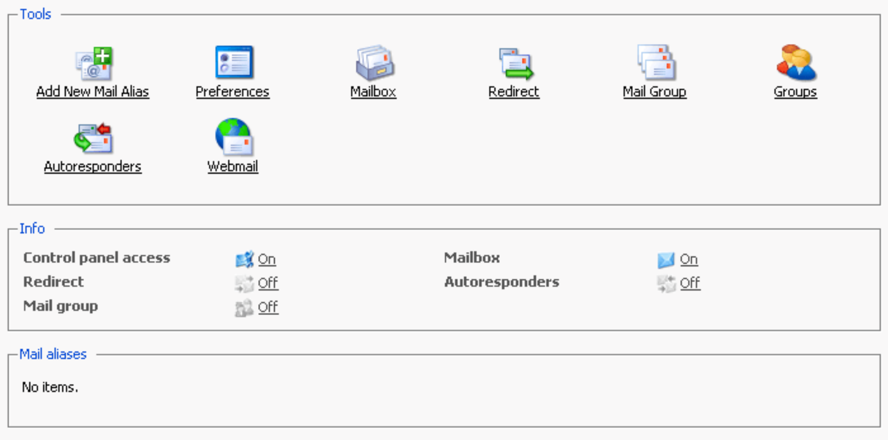
To remove one or several mail names, select the checkboxes in the mail names list, corresponding to the mail names you wish to remove and click Remove Selected.

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, and Autoresponder.

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:



Control panel access	On	Mailbox	On
Redirect	Off	Autoresponders	Off
Mail group	Off		

No items.

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

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

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

4. To edit properties of the mail name, such as interface language and skin, change password, allow multiple sessions, click Preferences.

5. To edit mailbox quota, click Mailbox.

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

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

8.

Groups.

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

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

Mailbox

Using this function, you can enable/disable the mailbox and set up mailbox quota:

1. When on the mail name properties page, click on the Mailbox icon

2. To enable/disable the mailbox, select/deselect 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. Click OK to submit your changes.

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

Managing Mail Redirects

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

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

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

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

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

Managing Mail Groups

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

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

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

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

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

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

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

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

NOTE

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

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

Managing Mail Autoresponders

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

Attachment files repository

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

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

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

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

1. On the mail name properties page, click the Autoresponders icon. Autoresponders management page will open.
2. Click Add New Autoresponder. The autoresponder creation/editing page will open.
3. Enter the name into the Autoresponder name field.
4. Below the Request text input box, you can determine whether an autoresponder responds to specific text or set of characters found within either the subject line or body of the incoming email, or if it responds to all incoming requests. Type the phrase or a set of characters in the Request text input box, and select the appropriate radio button to enable checking **`in the subject`** or **`in the body`**.
5. To set up the autoresponder to always respond, regardless of the contained text, click the bottom radio button for always respond.
6. You can select a specific subject to appear in your automatic reply using the Answer with subject option. To simply respond with the same subject as was received from the incoming request select the radio button for the default setting. To specify a certain subject line select the radio button beside the text box and enter the desired text.
7. In the Return address field, you can specify the return address that will be set up in the autoresponder message. This is done for the messages not to be directed to the autoresponder itself, when users use the "Reply to the message" function in their mail client software.
8. You can enter text to be included into the autoresponder in the Reply with text field.
9. Using the Add New Attachment button, you can attach files to be included in the autoresponder. These files must be uploaded into the Repository on the Mail Names Properties page. Select the uploaded file from the Attach files list, and use the Add New Attachment button to attach the file to the autoresponder. To remove an attached file, select the corresponding checkbox, and click Remove Selected.
10. You can limit the frequency at which the autoresponder responds to the same unique address, after receiving multiple emails from it. In the Reply to the unique email address not more than [ ] times a day input field, you can set the autoresponder to respond no more than a specified number of times per day. The default setting is to respond not more than 10 times in one day to unique mail addresses.

11. You can define the number of unique addresses that the autoresponder will remember. Enter the desired number in the Store up to: field. This memory enables the system to control response frequency. In the event of extremely high mail volume, to protect server performance, you can limit the address memory of the system database.

12. To specify an email address to which incoming requests are forwarded, enter the new e-mail in the Forward request to e-mail field. Email requests meeting the requirements established on this page will be forwarded to this alternate e-mail address.

13. Click OK to submit all changes.

14. Click the Enable buton to enable the autoresponder service.

Managing Mailing Lists

You can create and manage mailing lists via Plesk. Click the ✉ Mailing lists icon on the Domain administration page to access the Mailing Lists Management functions: activating/deactivating the Mailing List service, adding and removing mailing lists, enabling/disabling mailing lists.

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

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

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

Activating/deactivating the Mailing lists service

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

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

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

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

To activate/deactivate the mailing list service:

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

Creating a new mailing list

To create a new mailing list, follow these steps:

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

After the mailing list is created, you are taken to the page where you can add to and remove users from the mailing list.

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

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

Removing mailing lists

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

1. At the Mailing lists management page, select the checkboxes corresponding to the mailing lists you wish to remove.

2. Click Remove Selected. The Mailing lists removal page appears.

3. Confirm removal, and click OK.

Enabling/disabling mailing lists

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

1. At the Mailing lists management page, check the checkboxes corresponding to the mailing lists you wish to change state.

2. Click the On/Off icon. The confirmation page appears.

3. Click OK. The state of the selected mailing lists will be changed.

Setting Up a Domain User Account

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

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

To set up the domain user account:

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

   The Domain User Properties page appears.

2. To allow access to the control panel for the domain user select the checkbox Allow domain user access.

3. Enter the password in the Password text box, and then re-enter it in the Confirm Password text box. Select the domain user language and skin using the drop-down lists. Supply the personal and contact information in the fields provided.

4. Select the Allow multiple sessions checkbox to allow several simultaneous domain user sessions under the same login name and password.

5. If you wish to allow domain user to manage scheduler and use the backup/restore functions, select the respective checkboxes.

6. Click OK to complete creation.

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)

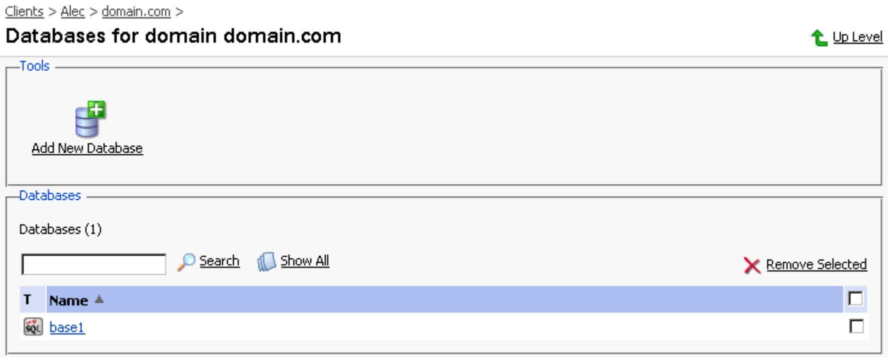
From the Plesk control panel, you can access external services, such as third party solutions provided through My.Plesk.com. To do that, click the Extras icon on the Domain Administration page. You will be taken to the MyPlesk.com login page, where you will need to enter your login and password. You 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:

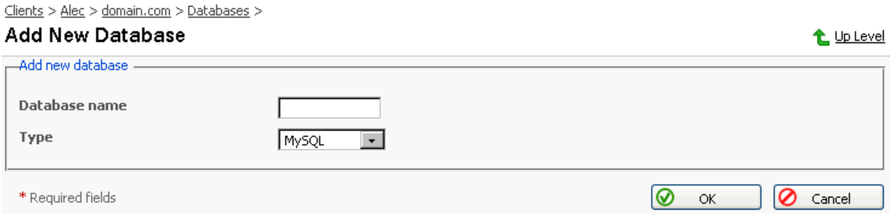


Databases for domain domain.com

Databases (1)

T	Name ▲	□
	base1	□

2. Click Add New Database. The page appears:



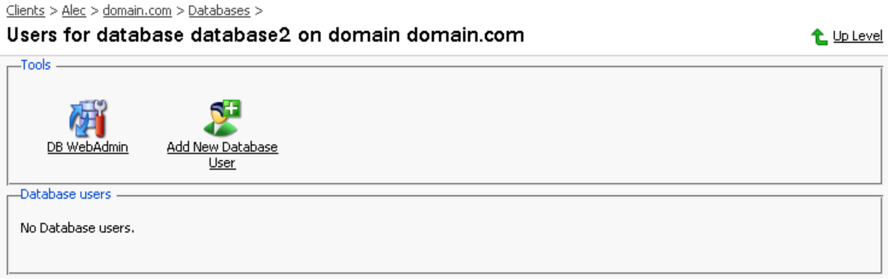
Add New Database

Database name

Type: MySQL

* Required fields

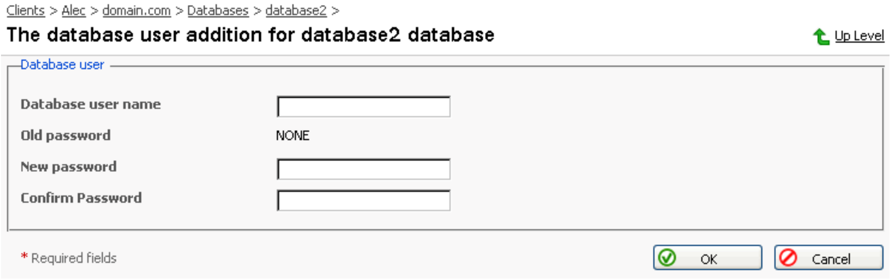
3. Enter the desired name for the database, select the database type and click OK. The Database Users page appears:



Users for database database2 on domain domain.com

No Database users.

4. To add database users to the newly created database, click Add New Database User. The Database user addition page appears:



Clients > Alec > domain.com > Databases > database2 >

The database user addition for database2 database

Database user

Database user name	
Old password	NONE
New password	
Confirm Password	

* Required fields

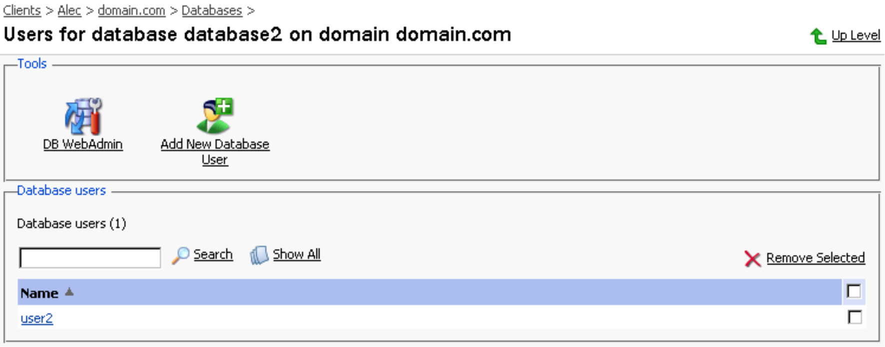
5. Enter the user name into Database user name text box, specify a password in the New Password text box, and then enter it again in the Confirm Password text box. Select OK to complete the creation of new user.

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:



Clients > Alec > domain.com > Databases >

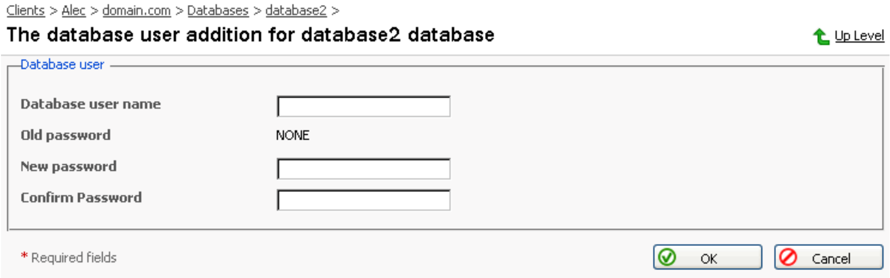
Users for database database2 on domain domain.com

Database users

Database users (1)

Name ▲	□
user2	□

2. To add database users to the selected database, click Add New Database User. The Database user addition page appears:



Clients > Alec > domain.com > Databases > database2 >

The database user addition for database2 database

Database user

Database user name	
Old password	NONE
New password	
Confirm Password	

* Required fields

3. Specify user name, enter new password in the New Password text box, and then re-enter it into the Confirm Password text box. Select OK to complete creation of the new user. Selecting Up Level will ignore all entries and return to the Database Editing page making no changes.

4. To edit the password of an existing database user, select the user from the database user list.

5. To delete existing database users select the users that you wish to delete using the corresponding checkboxes, and click Remove Selected.

6. To access and/or edit database content use the DB WebAdmin function.

7. Once you are finished with editing the database and its users, click Up Level to return to the Database Management page.

8. To delete databases from the system, select the databases that you wish to delete using the checkboxes and click Remove Selected.

9. To edit further databases, follow the steps outlined above. To return to the Domain Administration page, click Up Level.

Domain SSL Certificates Repository Management

Plesk enables you to upload a Secure Socket Layer (SSL) Certificate, generate a Certificate Signing Request (CSR), and/or generate a Self-signed Certificate. Each certificate represents a set of rules used when exchanging encrypted information between two computers. Certificates ensure secure communications; this is especially important when handling e-commerce transactions and other private transmittals. Only authorized users can access and read an encrypted data stream. If your client intends to implement SSL support for a virtual host domain, you can grant permission for SSL capabilities to the domain. Or, your client can implement the SSL certificate by self-administering his/her domain.

Notes on Certificates:

- You can acquire SSL certificates from various sources. We recommend using the CSR option within Plesk. You can also purchase the certificate through the My.Plesk.com (MPC) web site.
- If using a SSL certificate issued by a certificate authority other than Thawte or Verisign, a rootchain certificate is required to appropriately identify and authenticate the certificate authority that has issued your SSL certificate.
- Once you have obtained a SSL certificate or a certificate part, you can upload it through Plesk using the instructions, which follow in this section.

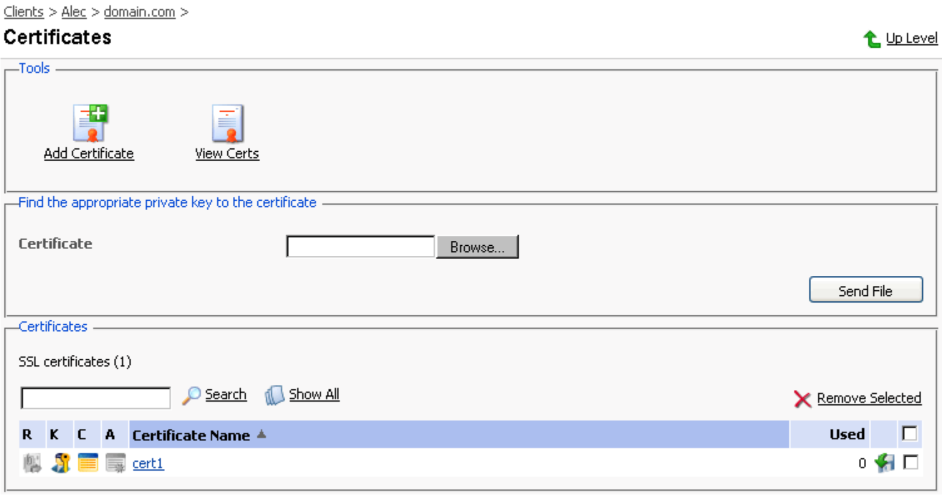
IMPORTANT

When you add a certificate, it is not installed automatically onto the domain or assigned to an IP address, but only added to the Certificate repository.

You can assign a certificate to an IP address at the Client's IP pool, at the server IP addresses management page, and during hosting creation on an exclusively granted IP.

Accessing the Domain SSL Certificates Repository

To access the Domain certificates repository page, click the Certificates icon at the Domain administration page. The certificates repository page will open displaying the list of available certificates:



R	K	C	A	Certificate Name ▲	Used	□
				cert1	0	□

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

Uploading a certificate file with finding the appropriate private key

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

Changing a certificate name

To change a certificate name follow these steps:

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

Viewing purchased certificates

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

Downloading a certificate to the local machine

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

Removing a certificate from repository

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

Adding a certificate to the repository

To add a certificate to repository, click the Add Certificate icon at the Domain certificate repository page. The SSL certificate creation page will open. On this page you can generate a self-signed certificate, certificate-signing request, purchase a SSL certificate, and add the certificate parts to an existing certificate.

Generating a self-signed certificate

To generate a self-signed certificate follow these steps:

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

Generating a Certificate Signing Request

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

1. Specify the certificate name.
2. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop-down list.
3. Select a country from the drop-down list.

4. Specify the state or province, location (city).
5. Enter the appropriate organization name and department/division in the field provided.
6. Enter the Domain Name for which you wish to generate the certificate signing request.
7. Specify the E-mail address.
8. Click the Request button. A certificate signing request will be generated and added to the repository. You will be able to add the other certificate parts later on.

Purchasing a Certificate

To purchase a new certificate follow these steps:

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

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

Uploading certificate parts

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

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

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

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

You can upload an existing certificate in two ways:

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

Uploading a CA certificate

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

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

You can upload an existing certificate in two ways:

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

Generating a CSR using an existing private key

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

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

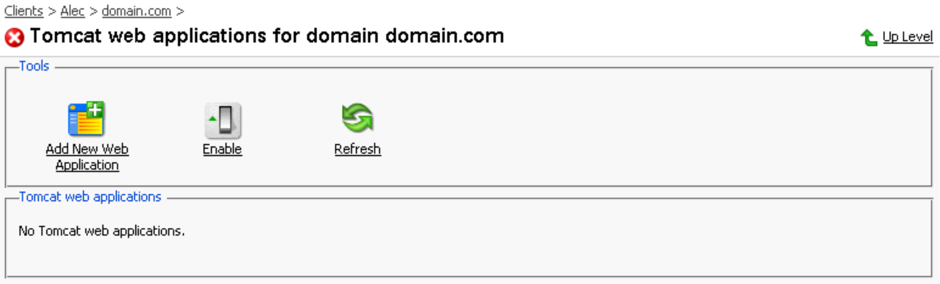
Removing a certificate part

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

1. At the certificate repository page, select a certificate from the list. You will be taken to the SSL certificate properties page.
2. Click on the Remove button located next to the CA certificate field.

Managing Tomcat Web Applications

Plesk supports deploying and managing Tomcat web application in order to enable users to set up hosting with JSP support. Click the Tomcat icon on the Domain Administration page, to access the Tomcat Web Applications Management functions:



Tomcat web applications for domain domain.com

No Tomcat web applications.

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

IMPORTANT

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

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

Table 5.3. The Tomcat service/web applications status icons

Icon	Meaning
The Tomcat service status	
▶	means that the Tomcat service is activated
✖	means that the Tomcat service for the domain is presently deactivated.
The Tomcat web application status	
▶	means that the web application is activated
✖	means that this web application is presently deactivated and inaccessible.
❗	means that web application is inaccessible.

Activating/deactivating the Tomcat service

In order to disable the support of Tomcat web applications the Tomcat service can be deactivated. When the Tomcat service is deactivated, all active Tomcat web applications also change their status to 'inaccessible' while all inactive web applications remain unchanged.

Activation of the Tomcat service enables access to active web applications.

> **NOTE**
>
> When the Tomcat service is activated, the status icon will change to ▶, and so will the status icons of the Tomcat web applications at this domain that were active before deactivating the Tomcat service.

To activate/deactivate the Tomcat service:

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 Tomcat web application archive files

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

1. Click Add New Web Application.

2. Select the web application archive file. Use the Browse button to locate the desired file.

> **NOTE**
>
> Only .war format (Web-application archive) files can be uploaded. The application file cannot be named as manager.war

3. Click OK. The new web application will be uploaded and added to the Tomcat web applications list.

Restarting the web applications

You can restart the Tomcat web applications directly from the control panel. In order to stop, start or restart a web application follow these steps:

1. Select the web application at the Tomcat web applications list on the Tomcat Web Applications Management page.

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

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

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

The current web application state will be marked by an icon: ▶ (ON) for the web application running, and ✖ (OFF) for the web application stopped.

Accessing the Tomcat web applications

A Tomcat web application can be accessed simply by clicking on its name in the Tomcat web applications list. The selected application will be opened in a new browser window.

> **NOTE**
>
> If a web application is disabled, it cannot be accessed, and therefore, the link to it is also disabled.

Removing web applications

You can remove one or several web applications at the same time. To remove a web application(s):

1. Check the checkboxes in the Tomcat web applications list corresponding to the web applications you wish to remove.
2. Click Remove Selected. The Web Application Removal page appears.
3. Confirm the removal, and click OK.

Managing Web Users

A web user is a user account within web server. It is used to define locations for personalized web pages with individual FTP access. The result of creating a web user is a subdirectory within your domain (e.g. `domain.com/~webuser`).

Creating a web user account

To create a new web user account:

1. Click the Web Users icon on the Domain administration page. The Web Users page appears.
2. Click the Preferences icon to configure web user access format and enable scripting capabilities. The Preferences page opens.
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.
5. 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).

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.

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

6. Once you have completed all entries click OK.

As you create web users, the user names appear listed on the Web Users page.

NOTE

New web users can access the directory using FTP software by entering the domain name under which the web user account was created and using the appropriate web user name and password.

Editing the web user account properties

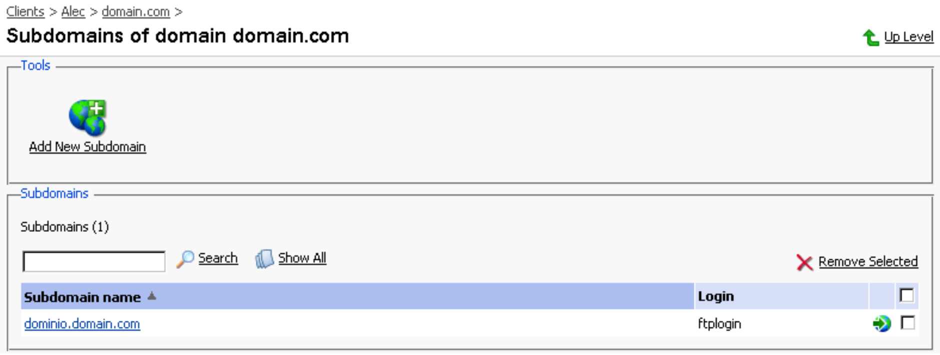
To change web user passwords or edit scripting options, click on the user name in the web user list. This takes you to the Web User Configuration page. Follow the same procedure as described above.

Deleting a web user account

To delete existing web users select the users that you wish to delete using the checkboxes, and click Remove Selected. You will be asked for confirmation prior to deleting the selected web users.

Managing Subdomains

You can create and manage subdomains from the control panel. Access the subdomains management functions, selecting the Subdomains icon on the Domain Administration page. The subdomains management page opens, listing the subdomains existing under the domain and corresponding FTP account names used for managing them:



Clients > Alec > domain.com >

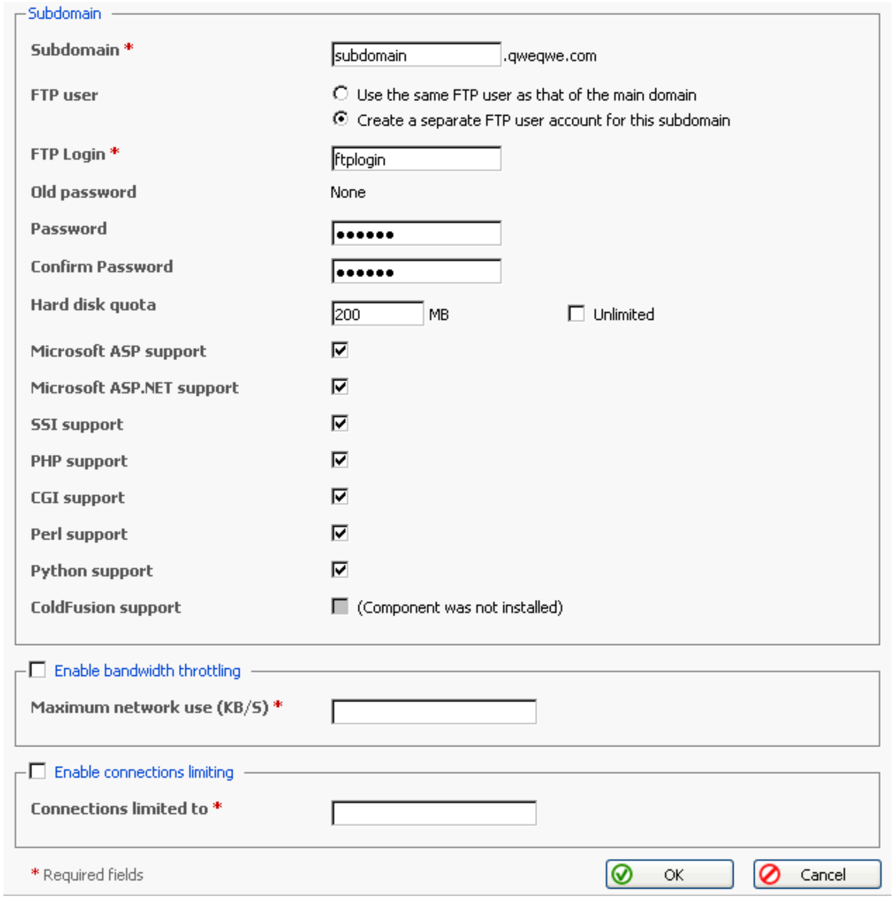
Subdomains of domain domain.com

Subdomains (1)

Subdomain name ▲	Login	□
dominio.domain.com	ftplogin	□

To create a subdomain, follow these steps:

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



Subdomain *	subdomain .qweqwe.com
FTP user	○ Use the same FTP user as that of the main domain ● Create a separate FTP user account for this subdomain
FTP Login *	ftplogin
Old password	None
Password	••••••
Confirm Password	••••••
Hard disk quota	200 MB □ Unlimited
Microsoft ASP support	☑
Microsoft ASP.NET support	☑
SSI support	☑
PHP support	☑
CGI support	☑
Perl support	☑
Python support	☑
ColdFusion support	□ (Component was not installed)

□ Enable bandwidth throttling

Maximum network use (KB/S) *

□ Enable connections limiting

Connections limited to *

* 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. To limit the bandwidth for this subdomain, select the Enable bandwidth throttling checkbox and enter the required value in the input box.

7. To restrict the number of simultaneous connections to a given Web site, select the Enable connections limiting checkbox, and specify the number of connections. If the number of connections reaches the maximum allotted, all subsequent connection attempts are returned with an error, and then disconnected.

8. Click OK.

To open the subdomain URL in browser, in the list of subdomains click .

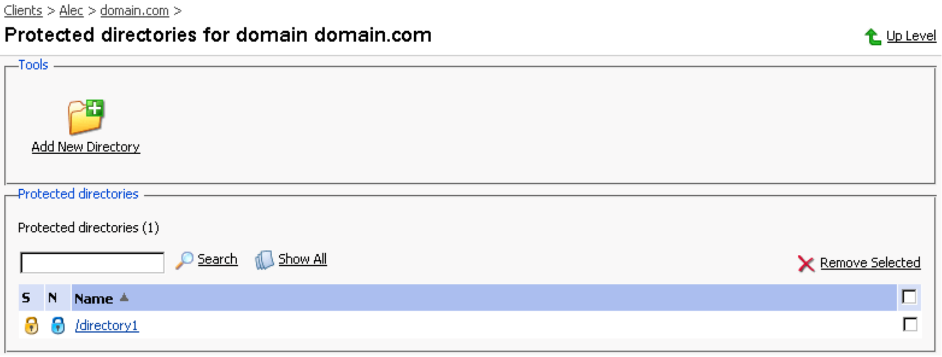
To edit hosting account of a subdomain, select the required subdomain name in the list.

To remove one or several subdomains, select them using the corresponding checkboxes, and click Remove Selected.

Managing Protected Directories

This feature is active if virtual hosting has been configured for the domain. It creates and provides password-protected access to the directories where the secure documents reside in the virtual domain. It is possible to create directories under either the standard virtual host accessible via http protocol, or if applicable for the given domain, under the SSL virtual host accessible via https protocol.

To access the protected directories management functions, use the Directories icon on the Domain Administration page. The page will open listing all protected directories of this domain:



Protected directories for domain domain.com

Protected directories (1)

S	N	Name ▲	□
🔒	🔒	/directory1	□

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.

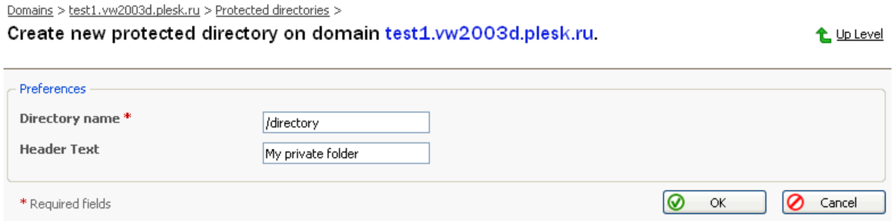
NOTE

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:



Domains > test1.vw2003d.plesk.ru > Protected directories >

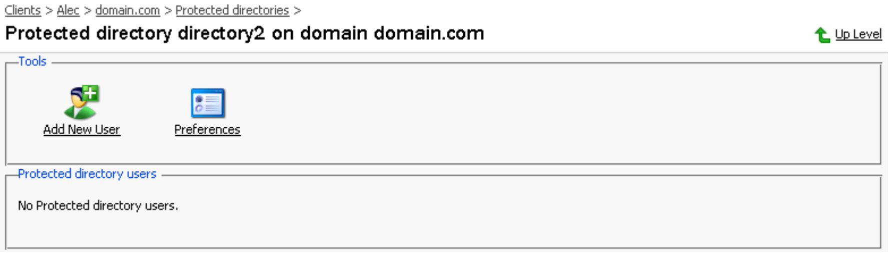
Create new protected directory on domain test1.vw2003d.plesk.ru.

Directory name *	/directory
Header Text	My private folder

2. Enter the name of the protected directory you wish to create in the Directory name field.

3. If desired, enter the text displayed when users are prompted to enter their login and password into the Realm access text field.

4. Click OK to complete creation. You will be taken to the list of protected directory users:

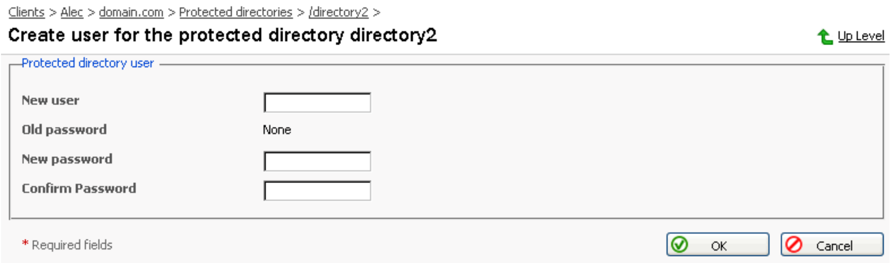


Clients > Alec > domain.com > Protected directories >

Protected directory directory2 on domain domain.com

No Protected directory users.

5. To add a new user, click the Add New User icon. You are taken to the new directory user creation page:



Clients > Alec > domain.com > Protected directories > /directory2 >

Create user for the protected directory directory2

Protected directory user

New user

Old password None

New password

Confirm Password

* Required fields

6. Specify the user name, password and confirm password.

7. Click OK to submit. You will return to the Protected Directory Management page. The new user record will appear in the list of users.

8. 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.

9. To access a directory user record in order to edit the user password, click on the user name in the list.

10. 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:

1. On the Protected directories page, click on a title of the directory that you wish to edit. You will be taken to the Protected Directory Management page.

2. Edit the directory properties by following the same steps outlined above, in the Creating a protected directory section.

3. Click OK to submit all changes to the system and to return to the Protected Directories page.

Removing a Protected Directory

To remove one or more directories, follow these steps:

1. Select the checkboxes in the list of protected directories.

2. Click Remove Selected. The Protected Directory Removal page appears.

3. Confirm removal, and click OK.

> **NOTE**
>
> Removing a protected directory in Plesk does not delete the directory off the server, it simply removes the protection. Meaning that the directory and its contents will now be reachable via the Internet without the need for login and password.

Managing Virtual Directories

A virtual directory is an alias for a physical directory on your server hard drive that resides in the domain's home directory. Because an alias is usually shorter than the path of the physical directory, it is more convenient for users to type. The use of aliases is also secure because users do not know where your files are physically located on the server and therefore cannot use that information to modify your files. Aliases also make it easier for you to move directories in your site. Rather than changing the URL for the directory, you change the mapping between the alias and the physical location of the directory.

To manage virtual directories, use the 📁 Virtual Directories icon on the Domain Administration page.

Creating a Virtual Directory

To create a virtual directory, follow these steps:

1. Click Add New Virtual Directory.

2. In the Name box, type a name for the virtual directory. This is the name the user types, and should be short and easy to type.

3. In the Path box, choose the name of the physical directory in which the virtual directory resides. The path should be relative to the domain's home directory.

4. Select the Read checkbox to allow users to read or download files or directories and their associated properties.

5. Select the Write checkbox to allow users to upload files and their associated properties to the enabled directory on your server or to change

content in a Write-enabled file. Write access is allowed only when a browser that supports the PUT feature of the HTTP 1.1 protocol standard is used.

6. Select the Script source access to allow users to access source code if either Read or Write permissions are set. Source code includes scripts in ASP applications.

7. Select the Directory browsing box to allow users to see a hypertext listing of the files and subdirectories in this virtual directory. Because virtual directories do not appear in directory listings, users must know a virtual directory's alias. If Directory browsing is disabled and the user does not specify a file name, the Web server displays an “Access Forbidden” error message in the user's Web browser.

8. The Execute permissions option determines the program execution level allowed for this site's resources.

   Set permissions to None to restrict access only to static files such as HTML or image files.

   Set permissions to Scripts only to allow only scripts to run, not executables.

   Set permissions to Scripts and Executables to remove all restrictions so that all file types can be accessed or executed.

9. Click OK.

NOTE

While creating a virtual directory, you configure its basic settings. Advanced configuration of a virtual directory is available afterwards, when editing the properties of an existing directory.

Once added, a virtual directory is displayed in the list, accompanied by the status icons that indicate the types of permissions set for the directory. The columns are:

- R - read permissions,
- W - write permissions,
- S - script source access,
- B - directory browsing.

To set or revoke a specific permission, click the appropriate icon.

To remove a virtual directory, select the corresponding checkbox and click Remove Selected.

Editing Virtual Directories Properties

To adjust a virtual directory settings, click on its name or path in the list of virtual directories.

When you are on the page of a virtual directory properties, you can change its basic configuration described in the Creating a Virtual Directory section. You can also specify the advanced settings:

- Select the Log visits checkbox if you want the information about visiting the current directory to be logged.
- Select the Enable parent paths checkbox to allow using double period in the pathname when refering to a folder above the current virtual directory. This makes possible for users moving up the folder tree without knowing the folder name or the whereabouts in the hierarchy.
- Select the Enable to run in MTA checkbox to allow the application execution in multi-threaded apartment (MTA) mode, that may provide a slight performance boost. If the checkbox is left deselected, the application runs in single-threaded apartment.
- The Enable default content page checkbox is needed for allowing a default document for the current virtual directory. The default document is sent to a client's browser of user who accesses the directory through the Web without a specific file name (e.g. using http://www.sw-soft.com, not http://www.sw-soft.com/index.php).

  If this checkbox is deselected and Directory browsing is enabled, the Web server returns a folder listing. If it is deselected and Directory browsing is disabled, the Web server returns an "Access Forbidden" error message.
- Specify the names of files that can be used as default documents (e.g. index.html, default.html, index.php etc) in the Default documents in a search order text input field. IIS searches for the default documents in the order you defined when listed the file names, and then operates the first available file it finds. If no match is found, IIS behaves as in the cases when the default content page is disabled.
- Select the Enable anonymous access checkbox if you want to make the directory public, so that web users could access it without authentication.
- Select the Require SSL checkbox/ to enable SSL-only access to the directory.

Managing MIME Types

Multipurpose Internet Mail Exchange (MIME) types instruct a Web browser or mail application how to handle files received from a server. For example, when a Web browser requests an item on a server, it also requests the MIME type of the object. Some MIME types, like graphics, can be displayed inside the browser. Others, such as word processing documents, require an external helper application to be displayed.

When IIS delivers a mail message to a mail application, or a Web page to a client Web browser, it also sends the MIME type of the data it is sending. If there is an attached or embedded file in a specific format, IIS also tells the client application the MIME type of the embedded or attached file. The client application then knows how to process or display the data being received from IIS.

To manage MIME types, use the MIME Types icon on the Domain Administration page.

Defining a new mime type

To define a MIME type, follow these steps:

1. Click Add New MIME Type.
2. In the Extension box, type the file name extension beginning with a dot (.), or use a wildcard (*) to serve all files regardless of file name extension.
3. In the Content box, determine the file content type. You can select the appropriate value from the list or define a new content type. To do this, select Custom... and specify the content type in the input box.
4. Click OK.

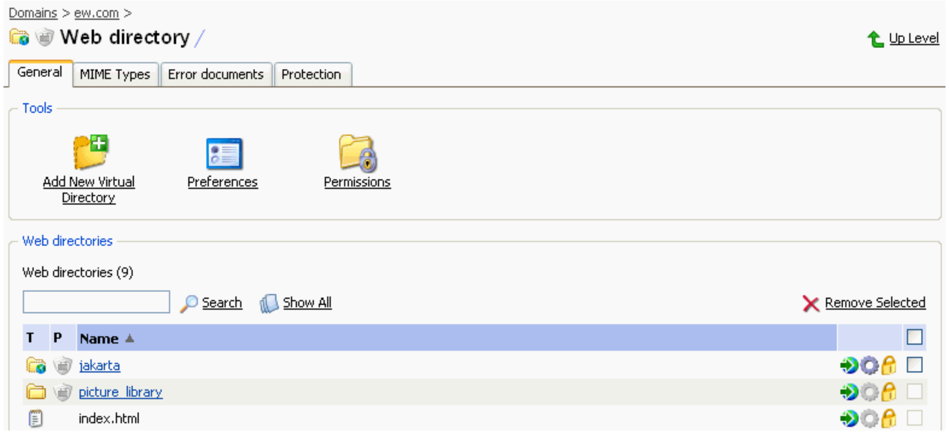
Once added, all MIME types are presented in the list.

To redefine a MIME type, click the required extension or content type.

To remove a MIME type, select the corresponding checkbox and click Remove Selected.

Managing Web Directories

Plesk allows you to see the directories of your domain the way they are seen from the web and manage their protection and settings. Generally, there are two types of directories, physical and virtual ones. Physical directories are the actual directories present on the server's hard drive while virtual ones are only abstraction, a kind of links to the existing physical directories. Therefore, virtual directories are not visible in regular file manager but you can see and manage them on the Web Directories screen at the Domain Administration page.



Domains > ew.com >

Web directory /

Up Level

General | MIME Types | Error documents | Protection

Tools

Add New Virtual Directory

Preferences

Permissions

Web directories

Web directories (9)

Search | Show All | Remove Selected

T	P	Name ▲		□
		jakarta		□
		picture_library		□
		index.html		□

Further, directories may be protected and unprotected. Everybody can access unprotected directories, while only privileged users can access directories with protection.

While working with the Web Directories screen, there is a notion of current directory. It is written in the title text of the page (by default, it is "Web directory /"). All the actions accessible on the screen affect the current directory. To change the directory, click on the desired name in the Web directories list. The title text will be updated to reflect the change.

Each entry in the directories list has three icons at the right side. First one allows you to open the corresponding directory in browser. The next one allows changing preferences of the directory. It is accessible only for virtual directories. The last one allows editing permissions.

If the current directory is virtual, four tabs are shown at the top of the page:

- General. This is the tab where you can change the current directory and change its properties.
- MIME Types. Here you can define what types of files the web server can handle in the current directory.
- Error documents. Allows you to change custom error documents for the web

server errors. For using this feature, you should allow this on the domain setup page (the Custom Error Documents checkbox).

- Protection. Used for managing protected directories.

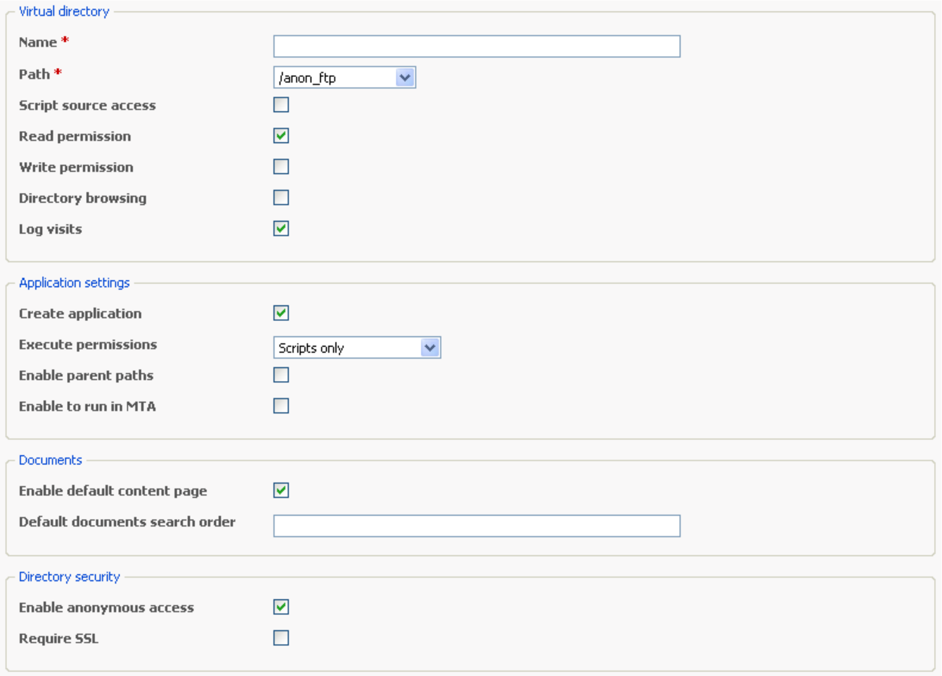
If the current directory is physical, only General and Protection tabs are shown.

Preferences on each of them affect the current web directory. There are three available buttons on the General tab:

- Add New Virtual Directory. Press it to add a new virtual directory in the current directory.
- Preferences. Manages the properties of the current directory. Available only for virtual directories.
- Permissions. Allows you to define what types of actions different user types can carry out with the current directory.

Managing Directory Preferences

To change properties of the current directory, press the Preferences button on the General tab. The following page will appear:



Virtual directory

Name *

Path * /anon_ftp

Script source access □

Read permission ☑

Write permission □

Directory browsing □

Log visits ☑

Application settings

Create application ☑

Execute permissions Scripts only

Enable parent paths □

Enable to run in MTA □

Documents

Enable default content page ☑

Default documents search order

Directory security

Enable anonymous access ☑

Require SSL □

At this page you can change the properties of the given virtual directory, and add and remove nested virtual directories.

The Name field contains the name of the current virtual directory. You can rename the directory by entering the new name in this field.

In the Path drop-down list, select the path to the physical directory where the virtual directory resides.

Select the Script source access to allow users to access source code if either Read or Write permissions are set. Source code includes scripts in ASP applications.

Select the Read permission checkbox to allow users to read files or directories and their associated properties.

Select the Write permission checkbox to allow users to upload files and their associated properties to the current virutal directory or to change content in a write-enabled file. Write access is allowed only when a browser that supports the PUT feature of the HTTP 1.1 protocol is used.

Select the Directory browsing box to allow users to see a hypertext listing of the files and subdirectories in this virtual directory. Because virtual directories do not appear in directory listings, users must know a virtual directory's alias. If Directory browsing is disabled, user does not specify a file name and the default content page (see below) is disabled, the Web server displays an "Access Forbidden" error message in the user's Web browser.

Select the Log visits checkbox if you want to store the information on visiting the current directory.

The Create Application checkbox makes the virtual directory an IIS Application. The directory becomes logically independent from the rest of the web-site.

The Execute permissions option determines the program execution level allowed for this site's resources.

Set permissions to None to allow access only to static files such as HTML or image files.

Set permissions to Scripts only to allow running scripts only, not executables.

Set permissions to Scripts and Executables to remove all restrictions so that all file types can be executed.

Select the Enable parent paths checkbox to allow using double period in the pathname when referring to a folder above the current virtual directory. This makes users able to move up the folder tree without knowing the folder name or the whereabouts in the hierarchy. If the option is selected, parent paths should not have the Execute permission so that applications do not have the ability of unauthorized running of programs in the parent paths.

Select the Enable to run in MTA checkbox to allow the application execution in multi-threaded apartment (MTA) mode. Otherwise, the application runs in single-threaded apartment (STA) mode. Using STA, each application pool is executed in a dedicated process. With MTA, several concurrent application pools are executed in one thread which can increase performance in some cases.

The Enable default content page checkbox allows use of a default document for the current virtual directory. The default document is sent when users access the directory on the Web without a specific file name (e.g. using http://www.sw-soft.com as opposed to http://www.sw-soft.com/index.html). If this checkbox is deselected and the Directory browsing checkbox is enabled, the Web server returns a folder listing. If it is deselected and theDirectory browsing checkbox is disabled, the Web server returns an "Access Forbidden" error message.

IIS searches for the default documents in the order specified in the Default documents search order field and sends user the first available file it finds. If no match is found, IIS behaves as in the cases when the default content page is disabled.

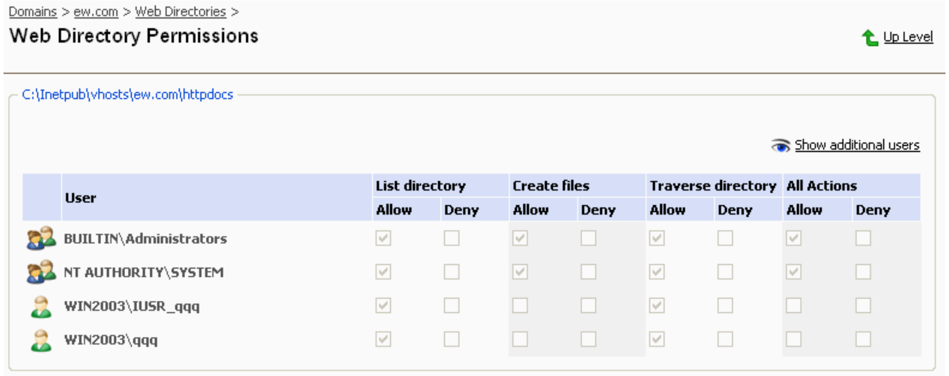
Select the Enable anonymous access checkbox if you want to make the directory public so that web users could access it without authentication.

Select the Require SSL checkbox to enable SSL-only access to the folder.

Click OK to submit your changes.

Managing Web Directory Permissions

Plesk allows setting up permissions for a web directory; this way you control what types of actions different uses can perform with the directory. To manage permissions of the current web directory, click the Permissions button on the General tab. The following page will open:



Domains > ew.com > Web Directories >

Web Directory Permissions

C:\Inetpub\vhosts\ew.com\httpdocs

User	List directory		Create files		Traverse directory		All Actions	
	Allow	Deny	Allow	Deny	Allow	Deny	Allow	Deny
BUILTIN\Administrators	☑	□	☑	□	☑	□	☑	□
NT AUTHORITY\SYSTEM	☑	□	☑	□	☑	□	☑	□
WIN2003\IUSR_qqq	☑	□	□	□	☑	□	□	□
WIN2003\qqq	☑	□	□	□	☑	□	□	□

- When setting permissions for folders: using the appropriate checkboxes, allow or disallow users to view the folder and its contents, to create files within the directory, and to traverse the directory. You can also select appropriate checkboxes in All Actions column if you want to allow or deny all operations for the given user/user group.

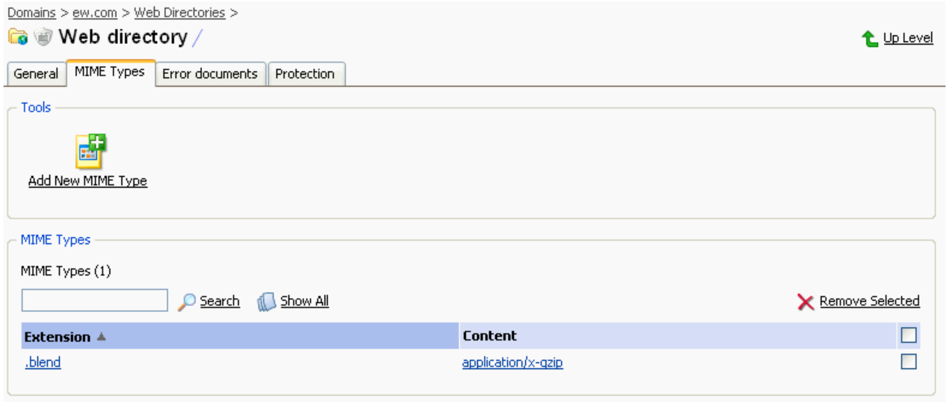
- When setting permissions for files: using the checkboxes, allow or disallow users to read and write to the file, and define permissions for file execution. You can also select appropriate checkboxes in All Actions column if you want to allow or deny all operations for the given user/user group.

Select the Show additional users checkbox for users with non-defined access rights to be shown in the list, so that you could grant them appropriate rights.

Click OK to submit your changes or click Cancel to discard all changes and return to the previous page.

Managing MIME Types

To set up MIME types for the current web directory, go to the MIME Types tab. The following screen will appear:



Extension ▲	Content	□
.blend	application/x-gzip	□

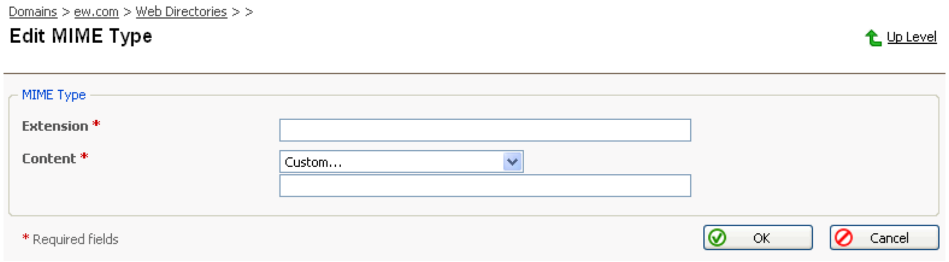
Multipurpose Internet Mail Exchange (MIME) types instruct a Web browser or mail application how to handle files received from a server. For example, when a Web browser requests an item on a server, it also requests the MIME type of the object. Some MIME types, like graphics, can be displayed inside the browser. Others, such as word processing documents, require an external helper application to be displayed.

When a web server delivers a Web page to a client Web browser, it also sends the MIME type of the data it is sending. If there is an attached or embedded file in a specific format, IIS also tells the client application the MIME type of the embedded or attached file. The client application then knows how to process or display the data being received from IIS.

IIS can only operate files of registered MIME types. These types could be defined both on the global IIS level and on the domain or virtual directory level. Note that globally defined MIME types are inherited by all the domains and virtual directories while ones defined on the domain or virtual directory level are used only for the area where they are defined. Otherwise, if the web server receives request for a file with unregistered MIME type, it returns the 404.3 (Not

Found) error.

To add a new MIME type, click on the corresponding icon. To edit an existing type, click on its name in the list at the bottom of page. The following screen will appear:



Domains > ew.com > Web Directories > >

Edit MIME Type

MIME Type

Extension *

Content * Custom...

* Required fields

In the Extension box, type the file name extension beginning with a dot (.), or use a wildcard (*) to serve all files regardless of file name extension.

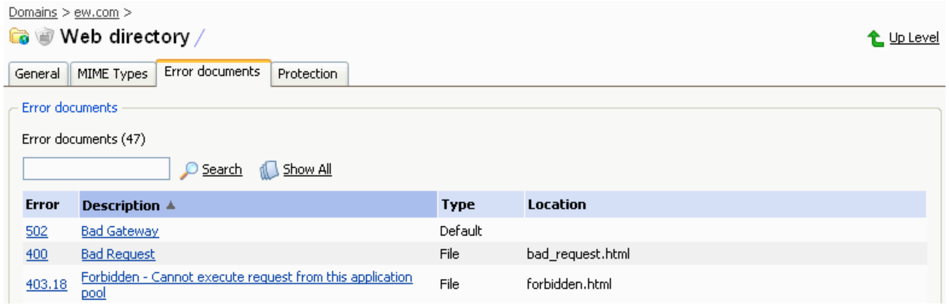
Specify the file content type in the Content box. You can either select the appropriate value from the list or define a new content type. To do this, select Custom... and enter the content type in the input box provided.

Click OK to submit your choice.

Managing Custom Error Documents

Plesk allows managing error documents sent to clients in cases of web server errors. The error codes are standardized in the HTTP protocol. For each error type you can either leave the default error document or replace it with the custom one.

To set up custom error documents, go to the Error Docs tab. The following screen appears:



Domains > ew.com >

Web directory /

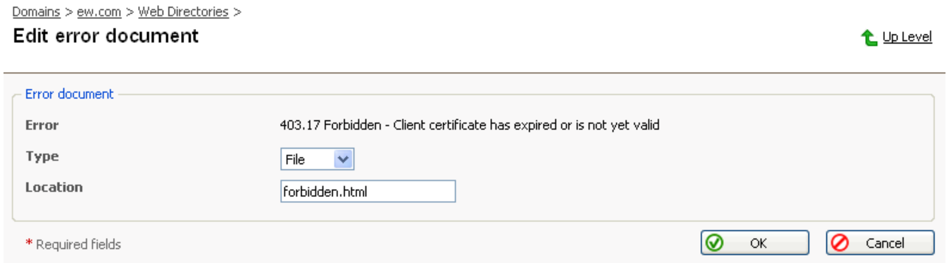
Error documents

Error documents (47)

Error	Description ▲	Type	Location
502	Bad Gateway	Default	
400	Bad Request	File	bad_request.html
403.18	Forbidden - Cannot execute request from this application pool	File	forbidden.html

The changes made on this screen affect only the current directory and all of its subdirectories.

All HTTP errors for which you can change the error page are listed in the Error docs list. To view the current settings for an error or change them, click on the error's name or number. The Edit Error Document page will open where you can change the default error document for the chosen type of error to your own one.



Domains > ew.com > Web Directories >

Edit error document

Error document

Error	403.17 Forbidden - Client certificate has expired or is not yet valid
Type	File
Location	forbidden.html

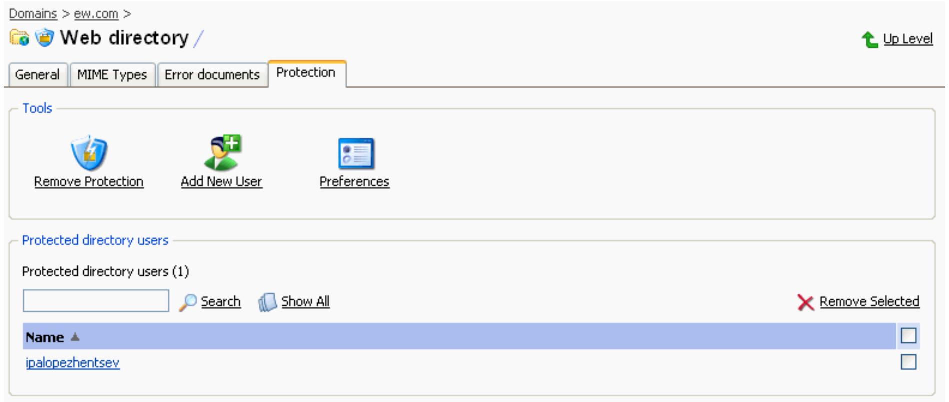
* Required fields

The Error label contains the standard error number along with its description.

The Type drop-down list contains two items: Default and File. When it is set to Default, the default IIS documents are used and the Location field below is inactive. To force server to show your page instead of the default one for the selected error type, select the File option in the Type drop-down field and type the name of the desired HTML document in the corresponding field. The error documents should lie in the errordocs directory and the Location field should only contain the name of document, e.g. 404.html.

Managing Protected Directories

Plesk allows setting protection on a web directory, which means the directory will be accessible only by users allowed to do so. You can protect both physical and virtual folders. To manage protection of the current directory, go to the Protection tab. The following screen will appear:



Domains > ew.com >

Web directory /

Protected directory users

Protected directory users (1)

Name ▲	□
ipalopezhentsev	□

To protect the current directory, press the Protect button. Now you can start adding users which will have access to it. To do this, press the Add New User button. A new screen will open where you will have to specify new user's name and password. When the user tries to access the protected directory via browser, a window opens where user should enter his/her name and password.

Click the Preferences button to set up the current protected directory's settings.

The list at the bottom of page shows all users which have permission to access the directory. You can click on user's name to change its password.

If you want to disable protection for the current directory, press the Remove protection button.

Adjusting Domain Performance Settings

You can limit the bandwidth use, the number of client Web connections, and CPU load for each domain hosted on Plesk server. By configuring network bandwidth on a given site, you can better control the amount of traffic allowed to that site. For example, by restricting bandwidth and/or the number of connections on a low-priority Web site, you allow other, higher-priority sites to handle larger traffic loads. Settings are site-specific and can be adjusted as network traffic and usage changes.

Bandwidth Throttling

If the network or Internet connection used by your Web server is also used by other services such as e-mail or news, you may want to limit the bandwidth used by your Web server so that bandwidth is available for those other services.

Limiting Connections

Connection limits restrict the number of simultaneous connections to a given Web site and your Web server. If the number of connections reaches the maximum allotted, all subsequent connection attempts are returned with an error, and then disconnected.

Limiting connections is a way to conserve bandwidth for other uses, such as e-mail servers, news servers, or another Web site running on the same installation. Limiting connections also conserves memory and protects against malicious attacks designed to overload your Web server with thousands of client requests.

Not limiting connections allows as many simultaneous connections as your network's bandwidth and processor can support. Be aware that allowing an unlimited number of simultaneous connections to your Web server exposes all sites on the server to the threat of a malicious attack where thousands of clients are instructed to connect to the server and delay subsequent service by consuming memory and bandwidth resources.

CPU Monitoring

CPU monitoring is a tool that monitors and automatically shuts down worker processes that consume large amounts of CPU resources. CPU monitoring is enabled for individual application pools.

To set any of these properties:

1. Click the Performance icon on the Domain administration page.
2. To enable bandwidth throttling, connection limiting, and/or CPU monitoring, select the corresponding checkboxes and supply the required values.
3. Click OK to submit your settings.

Managing Anonymous FTP Access

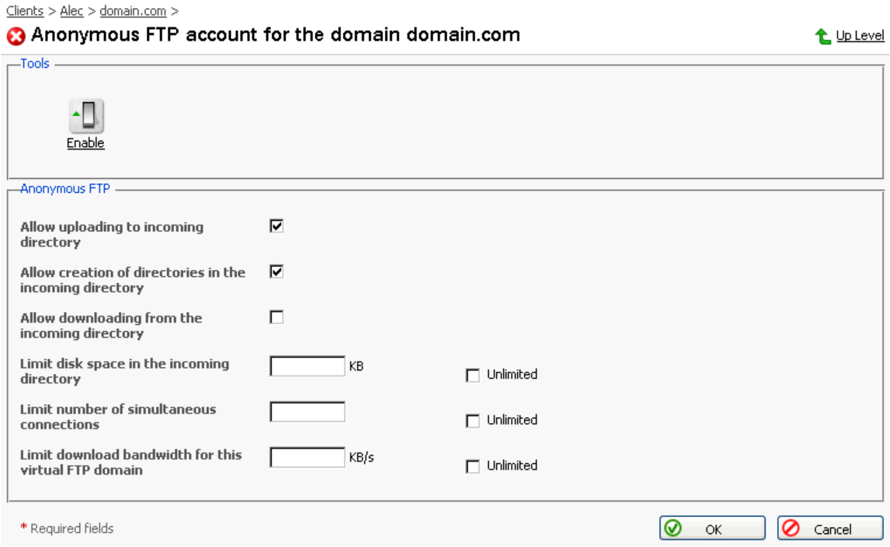
Within Plesk the Administrator, or Client given domain creation capabilities, can set up Anonymous FTP capabilities for a given virtual host. Anonymous FTP is used to allow an open, yet controlled, environment for visitors to the domain to download and/or upload files to and from the domain account. Users will be able to log into ftp.'domain name' with the standard anonymous user name and any password. Plesk allows the setup and limitation of incoming file space, number of connected users, and bandwidth usage throttling. Administrators should take care when allowing the use of anonymous FTP and be sure to use all the limitation capabilities within the interface wisely. If set up with excessive limits, it could lead to problems with server resources as well as excessive bandwidth usage.

NOTE

You can set up anonymous FTP only for domains that have physical hosting configured on exclusive IP.

To set up Anonymous FTP:

1. Click the Anonymous FTP icon on the Domain Administration page. The Anonymous FTP Account Management page appears:



Clients > Alec > domain.com >

Anonymous FTP account for the domain domain.com

Anonymous FTP

Allow uploading to incoming directory	☑	
Allow creation of directories in the incoming directory	☑	
Allow downloading from the incoming directory	□	
Limit disk space in the incoming directory	KB	□ Unlimited
Limit number of simultaneous connections		□ Unlimited
Limit download bandwidth for this virtual FTP domain	KB/s	□ Unlimited

* Required fields

2. By default anonymous FTP capabilities are disabled. To activate anonymous FTP select the Enable icon.

3. 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.

4. To allow users to create nested directories in the /incoming directory, select the Allow creation of directories in the incoming directory checkbox.

5. To allow downloading from the /incoming directory, select the Allow downloading from the incoming directory checkbox.

6. 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.

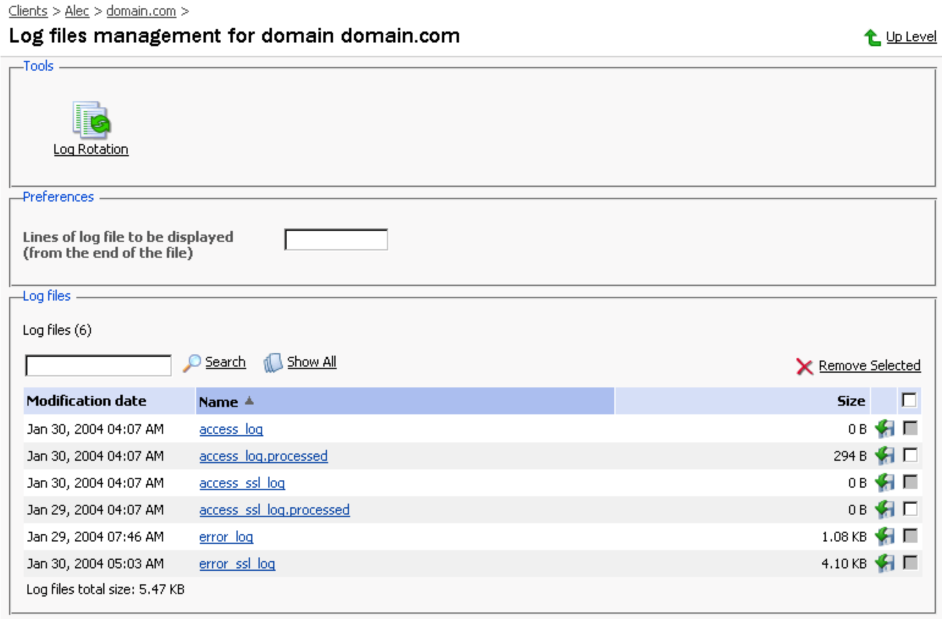
7. Deselect the Unlimited checkbox in the Limit number of simultaneous connections field to set limits on the number of users who can be simultaneously connected to the anonymous FTP site. Then enter the number of connections allowed.

8. 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.

9. 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:



Clients > Alec > domain.com >

Log files management for domain domain.com

Lines of log file to be displayed (from the end of the file)

Log files (6)

Modification date	Name ▲	Size	☐
Jan 30, 2004 04:07 AM	access_log	0 B	☐
Jan 30, 2004 04:07 AM	access_log.processed	294 B	☐
Jan 30, 2004 04:07 AM	access_ssl_log	0 B	☐
Jan 29, 2004 04:07 AM	access_ssl_log.processed	0 B	☐
Jan 29, 2004 07:46 AM	error_log	1.08 KB	☐
Jan 30, 2004 05:03 AM	error_ssl_log	4.10 KB	☐

Log files total size: 5.47 KB

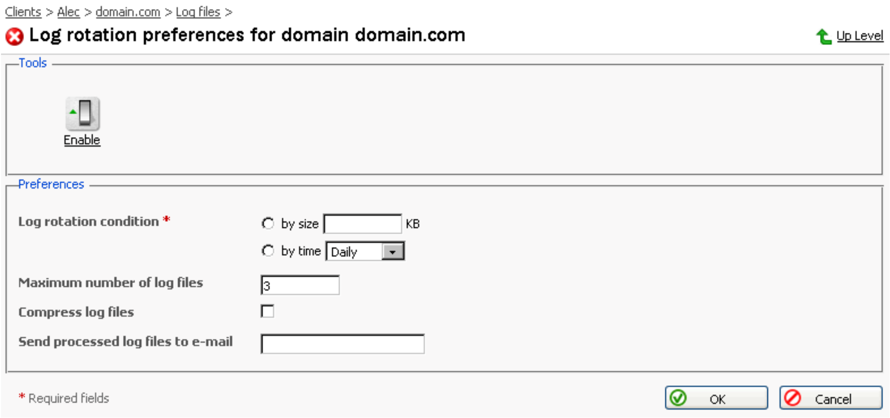
At this page, you can perform the following operations:

- Define the number of log file's lines to be displayed at once. To do that, type in the number of lines in the Lines of log file to be displayed input field prior to selecting a log file for viewing.
- View a log file. To this effect, click on a log file's name in the list. The log file contents will be displayed in a separate Log File Viewer window.
- Save a log file on your local machine. To do that, click on the appropriate icon. After that you will need to specify the location on your local machine and the file name for the downloaded log file to be saved, and then click Save.
- Delete log files. To this effect, select the corresponding checkboxes, and click Remove Selected.

To configure the log rotation preferences, follow these steps:

1. Click the Log Rotation icon on the Log Files Management page.

   The Log Rotation Preferences page will open:



Clients > Alec > domain.com > Log files >

Log rotation preferences for domain domain.com

Tools

Preferences

Log rotation condition *	○ by size ___ KB ○ by time Daily
Maximum number of log files	3
Compress log files	□
Send processed log files to e-mail	

* Required fields

2. Click the Enable or Disable icon respectively to enable/disable log rotation.

3. Select the log rotation condition:
   - log file size - enter the size in kilobytes in the appropriate field
   - time - select from the drop-down list. It can be set to **`Daily`**, **`Weekly`**, and **`Monthly`**.

4. Specify the maximum number of log files in the appropriate input field, if desired. The maximum number is the number of processed files to be kept for each log file.

5. Select the Compress log files checkbox to enable compression.

6. If desired, in the Send processed log files to e-mail input field, enter the e-mail address, for the processed log files to be delivered to.

7. Click OK to submit changes.

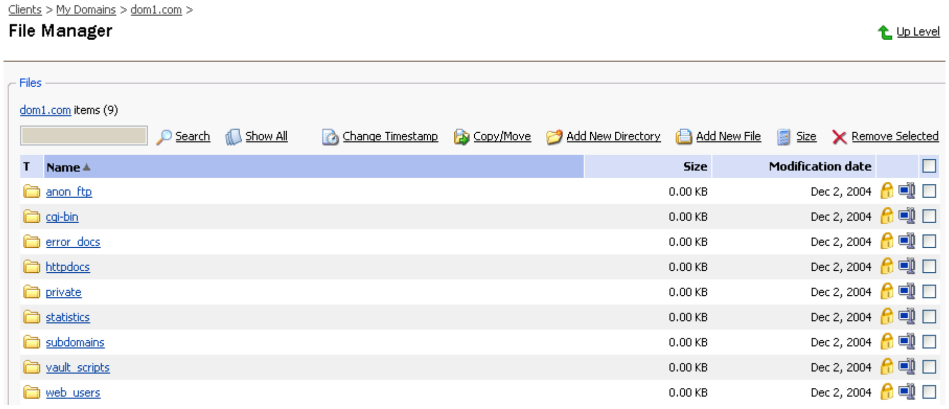
Using File Manager

The File Manager functions become available after you have configured physical hosting for a domain. File Manager is designed for working with files (e.g. web pages, text files, images etc) on a domain and its subdomains. Using File Manager, you can easily upload, create and delete files as well as organize them in folders and change file timestamps and permissions. File manager also allows to edit uploaded text and HTML files in text or WYSIWYG mode.

NOTE

On the top level of domain directories, deleting, moving, renaming folders, changing file timestamps and permissions, and creating new files and folders are not allowed.

To access the file manager functions, click the File Manager icon on the Domain Administration page. The file manager page will open displaying a domain directory structure and contents:



Clients > My Domains > dom1.com >

File Manager

dom1.com items (9)

T	Name ▲	Size	Modification date		□
	anon_ftp	0.00 KB	Dec 2, 2004		□
	cgi-bin	0.00 KB	Dec 2, 2004		□
	error_docs	0.00 KB	Dec 2, 2004		□
	httpdocs	0.00 KB	Dec 2, 2004		□
	private	0.00 KB	Dec 2, 2004		□
	statistics	0.00 KB	Dec 2, 2004		□
	subdomains	0.00 KB	Dec 2, 2004		□
	vault_scripts	0.00 KB	Dec 2, 2004		□
	web_users	0.00 KB	Dec 2, 2004		□

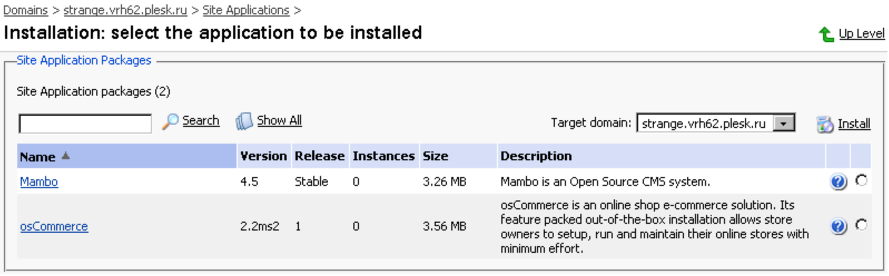
- To browse a directory, click the icon or directory name.
- To view or change permissions for a directory or a file, click the icon. The permissions settings page will open, allowing you to set the required permissions. Select the desired settings using the checkboxes, then click OK to submit.
- To rename a directory or a 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, a directory or a group of files and/or directories to another location, select the corresponding checkbox(es) and click Copy/Move. You will then need to specify the destination for the file or directory to be copied or moved to. Then click Copy to copy, or Move to move it.
- To change a timestamp for a directory, a file or a group of files and/or directories, select the corresponding checkbox(es) and click on the Change Timestamp icon. The timestamp(s) will be updated with the current local time.
- To remove a file, a directory or a group of files and/or directories, select the coresponding checkbox(es), and click Remove Selected.
- To upload a file to the current directory, click Add New File, then specify its location. Click OK.
- To create a file, click Add New 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 Add New Directory, then type in the directory name in the Directory name field, and click OK.
- To calculate disk space occupied by some files or directories, select them using the corresponding checkboxes and click the button.
- To edit a file in text mode, click the corresponding icon. The File Manager's editor window will open, allowing you to edit the file source. After you are done with editing, click Save to save the file, Save and Exit to save the file and quit the file editing mode, Cancel to cancel editing mode and return to the File Manager panel, or Reset to discard the alterations made.
- To edit a file in the WYSIWYG editor, click the corresponding icon.

Using the Domain Application Vault

The domain application vault function enables you to install various applications on domain and view the properties of the already installed applications.

Installing application on domain

1. Select a domain with configured physical hosting and click the Application Vault icon on the Domain Administration page.
2. Click the Add Application icon. The application installation wizard will open:



Domains > strange.vrh62.plesk.ru > Site Applications >

Installation: select the application to be installed

Up Level

Site Application Packages

Site Application packages (2)

Search Show All Target domain: strange.vrh62.plesk.ru Install

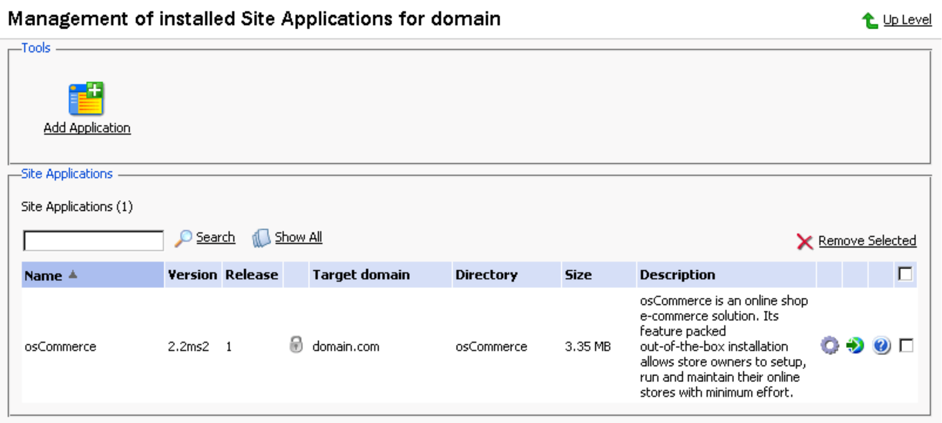
Name ▲	Version	Release	Instances	Size	Description		
Mambo	4.5	Stable	0	3.26 MB	Mambo is an Open Source CMS system.	?	○
osCommerce	2.2ms2	1	0	3.56 MB	osCommerce is an online shop e-commerce solution. Its feature packed out-of-the-box installation allows store owners to setup, run and maintain their online stores with minimum effort.	?	○

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

   You can view information on available application packages by clicking on the application package name in the list. If there is a documentation available for the application, it will be accessible through the icon .
4. Click Install.
5. Some applications require that certain parameters be entered before executing the installation. Click Finish once you are done editing the required parameters.

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:



Management of installed Site Applications for domain

Tools

Site Applications

Site Applications (1)

Name ▲	Version	Release	Target domain	Directory	Size	Description				□
osCommerce	2.2ms2	1	domain.com	osCommerce	3.35 MB	osCommerce is an online shop e-commerce solution. Its feature packed out-of-the-box installation allows store owners to setup, run and maintain their online stores with minimum effort.	⚙	➔	?	□

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

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

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

Accessing Site Builder

Plesk is shipped with Mambo site builder software intended to simplify the process of creating and deploying web sites. In order to use the site builder, you need to have the PHP support enabled for the domain set-up on physical hosting. You can set it up to work via HTTP or HTTPS protocol. The application can be installed on the domain and configured either via Domain Application Vault or using the installation procedure invoked when you click on the Site Builder icon for the first time. After the application is installed and configured, use the Site Builder icon on the Domain administration page to access it.

Accessing Microsoft FrontPage Web Administrator

You can access the Microsoft FrontPage Web Administrator directly from the Control Panel, using the FP Webadmin icon, or FP-SSL Webadmin if you wish to access it over secure SSL connection. These icons are located at the bottom of the Domain Administration page, provided that hosting is set up for the domain, and Microsoft FrontPage is available. Note, that the FrontPage Web Admin software should be installed and configured properly for this function to work, and the FrontPage and FrontPage over SSL support should be enabled within Plesk.

NOTE

Frontpage users created by Plesk are not allowed to create new Frontpage users outside of Plesk Control Panel for security reasons.

IMPORTANT

Some browsers (such as Netscape and Mozilla versions before 1.4b) do not support NTLM authorization, required to login to FP Webadmin. Therefore, to allow the clients who use non-Windows platforms to access Microsoft FrontPage, you will need to do the following:

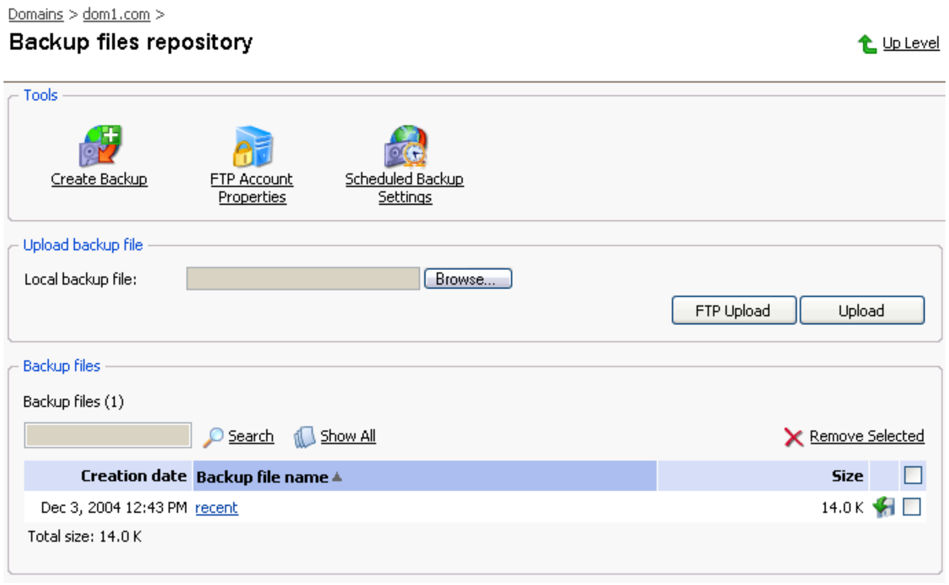
1. Run IIS Manager (Start -> Programs -> Administrative Tools -> Internet Information Services).
2. Right click on the domain virtual directory and select Properties in the context menu (Web Sites -> <domain IP address> -> <domain name_non_ssl|domain name_ssl>).
3. Select the Directory Security tab.
4. In the "Authentication and access control" section, click the Edit button.
5. Select the "Basic authentication (password is sent as clear text)" checkbox in the "Authenticated access" section.
6. Click OK.

Note that enabling basic authentication renders the connections to FrontPage insecure.

Backing Up and Restoring Domains

You can back up and restore domain data by the control panel means, provided that the backup utilities are installed on your server, and the backup/restore functions are supported by the product license key.

To access the backup/restore functions, on the Domain administration page of the selected domain, click the Backup icon. The Backup files repository page opens displaying the stored domain backup files and their properties:



Domains > dom1.com >

Backup files repository

Up Level

Tools

Upload backup file

Local backup file: Browse...

FTP Upload | Upload

Backup files

Backup files (1)

Search | Show All | Remove Selected

Creation date	Backup file name ▲	Size	□
Dec 3, 2004 12:43 PM	recent	14.0 K	□

Total size: 14.0 K

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 the data you input.

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. Note that if you want backup files to be stored on FTP server, you should first specify FTP account properties (see above).
4. Specify the maximum number of backup files that can be stored in the selected location.

NOTE

When the specified number is exceeded, the oldest backups are removed from the repository.

5. Enter the name the backup files should begin with.

6. Click OK to submit the data you input.

To back up the domain data, follow these steps:

1. Click the Create Backup icon on the Backup files repository page.

   The Backup file creation page appears.

2. Specify the backup file name.

3. Select the appropriate Backup method from the corresponding drop-down list:

   - if you choose to create backup file and store it in repository, the backup file created is saved on the server and is shown in the corresponding list;

   - if you choose not to store the backup file in repository, only to download it, the backup file created is saved only on your local machine;

   - if you choose to create the backup file and store it on FTP server, the backup file created is saved to the remote FTP server. To be able to use this option, you should specify a FTP server name and a FTP server directory name where you want the domain backup files to be stored, and the FTP server login and password in the corresponding text input fields. If the FTP account settings have been previously specified, the FTP server, Base directory on FTP server, FTP Login and FTP Password fields will be automatically filled. In cases when you wish to use FTP server or directory different from the default one, you can specify its properties for the current backup file creation.

4. Specify the backup file name and type in your comments in the respective text input fields.

5. Select the Notify by email checkbox and enter the e-mail address, if you wish to receive notifications of backup procedures start and completion.

6. Click Back Up.

7. In cases of backup file creation with downloading it to the local machine, the File Download dialog window opens. Click Save, specify the file

location and then click Save again. The file will be saved on your local machine.

To view the properties of backed up domain click the backup file's name.

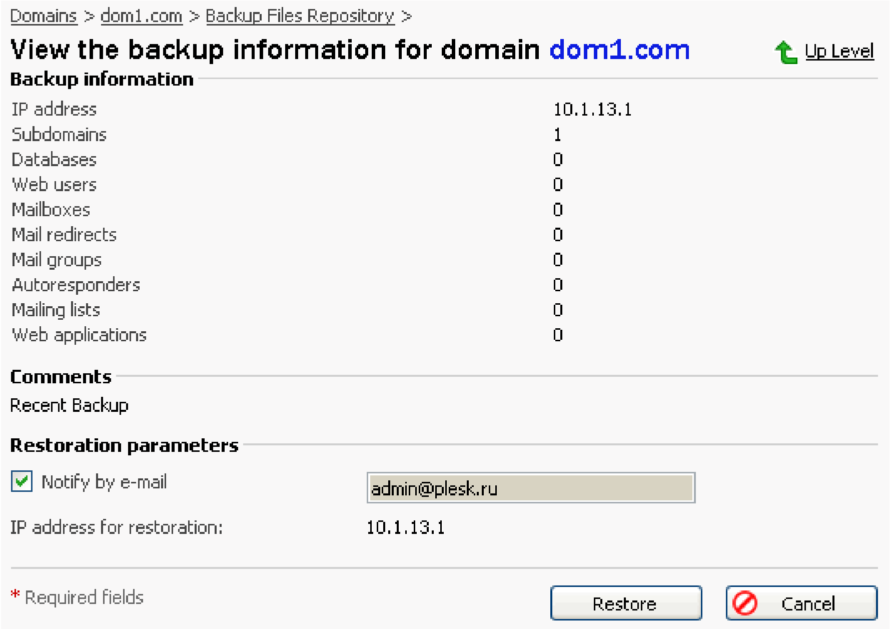
To save a backup file on your local machine, click the corresponding icon. After that you will need to specify the location on your machine and the file name for the downloaded backup file to be saved, and then click Save.

To delete one or several backup files from the repository, select the corresponding checkboxes and click Remove Selected.

To upload a backup file to the server, specify the file location using the Browse button, then click Upload.

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:



Domains > dom1.com > Backup Files Repository >

View the backup information for domain dom1.com

Backup information

IP address	10.1.13.1
Subdomains	1
Databases	0
Web users	0
Mailboxes	0
Mail redirects	0
Mail groups	0
Autoresponders	0
Mailing lists	0
Web applications	0

Comments

Recent Backup

Restoration parameters

☑ Notify by e-mail admin@plesk.ru

IP address for restoration: 10.1.13.1

* Required fields

3. If desired, enter an e-mail and select the checkbox to enable the notification.

   Select the IP address to be used for restoring the domain data.
4. Click Restore.

NOTE

During backup/restore processes, the domain is automatically switched off and all of its services are unavailable.

Deactivating/Activating a Domain

You can disable the domain operations by deactivating it. When a domain is deactivated, it cannot be accessed.

To deactivate a domain:

1. On the Domain administration page of the selected domain, click Disable. The confirmation will appear querying whether you actually wish to change the status of the selected domain.
2. Click OK.

To activate a domain, follow these steps:

1. On the Domain administration page of the selected domain, which is disabled, click Enable. The confirmation will appear querying whether you actually wish to change the status of the selected domain.
2. Click OK.

NOTE

When a domain is deactivated, the domain status icon will change to ✖.

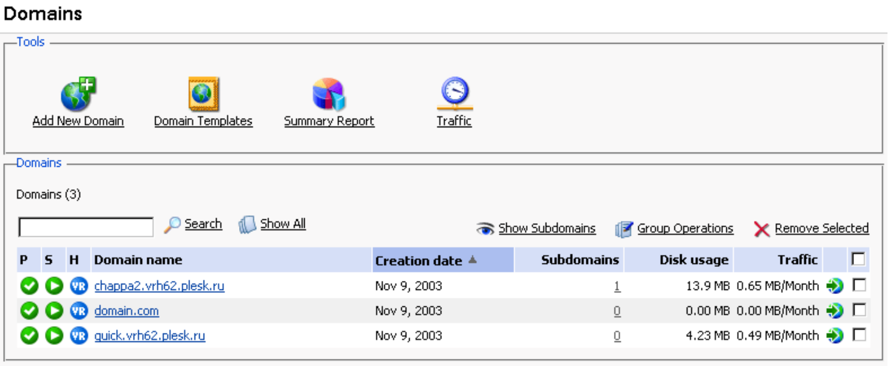
When a domain is activated, the domain status icon will change to ▶.

Performing Group Operations on Domains

In cases when you need to introduce certain similar changes to several domains, you can use the Group Operations function, made available to simplify administration of multiple domains. Using this feature you can, for instance, select a number of domains, enable all of them to support SSL and limit the total amount of available traffic to a specific figure - all that within a single operation, without having to select each domain independently and edit its settings.

To perform group operations on domains, follow these steps:

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



Domains

Tools

Domains

Domains (3)

P	S	H	Domain name	Creation date ▲	Subdomains	Disk usage	Traffic		☐
✓	▶	VR	chappa2.vrh62.plesk.ru	Nov 9, 2003	1	13.9 MB	0.65 MB/Month	➜	☐
✓	▶	VR	domain.com	Nov 9, 2003	0	0.00 MB	0.00 MB/Month	➜	☐
✓	▶	VR	quick.vrh62.plesk.ru	Nov 9, 2003	0	4.23 MB	0.49 MB/Month	➜	☐

2. Select the domains, whose settings or limits you wish to modify by checking the corresponding checkboxes.

3. Click the Group Operations icon. The Group Operations page will appear, divided into five sections:
   - The Limits group is used for modifying the limits for various resources
   - The Hosting group is used for editing various hosting-related settings
   - The Preferences group contains miscellaneous editable options for domains
   - The Services group is used for enabling/disabling the use of domain services
   - The Modified domains area lists the domains, whose settings you are going to modify.

4. To edit limit settings for a particular resource type:

   4.1. First, select the appropriate action from the drop-down box:
   - Leave the **`Do not change`** option selected, if you do not wish to make any changes
   - Select **`Unlimited`**, if you wish not to limit the resource usage
   - Select the **`Value`** option in order to specify a new value for the resource limit
   - Select **`Increase (+)`**, to specify the value by which to increment the presently set resource limit value
   - **`Select Decrease (-)`**, to specify the value by which to decrement the presently set resource limit value

   4.2. Then specify the value of the new resource limit in the corresponding input field.

   4.3. If you chose to increase/decrease the presently set limit value, use the drop-down box to select **units** if you wish to modify the limit value by a quantity of commonly used units or **%** if you wish to modify the limit value by a particular percentage.

5. To change the hosting-related settings, select **Do not change**, **Enable** or **Disable** radio button for the corresponding type of setting. You can manage the following:
   - SSL support
   - Web statistics
   - Custom Error Documents
   - Microsoft ASP and ASP.NET support
   - SSI support
   - PHP support
   - CGI support
   - Perl support
   - Python support
   - ColdFusion support (for information on possible problems see Configuring Physical Hosting section)

   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.

6. To change preferences, select **Do not change**, **Enable** or **Disable** radio button for the corresponding item. You can edit the following:
   - WWW prefix requirement
   - Web Mail
   - Allow the web users scripting
   - Traffic statistics retention settings
   - Mail to nonexistent user; if enabled, you can choose either to **Bounce** or **Catch to address**.

7. To enable/disable services, select **Do not change**, **Enable** or **Disable** radio button for the corresponding service. You can edit the following:
   - DNS Zone

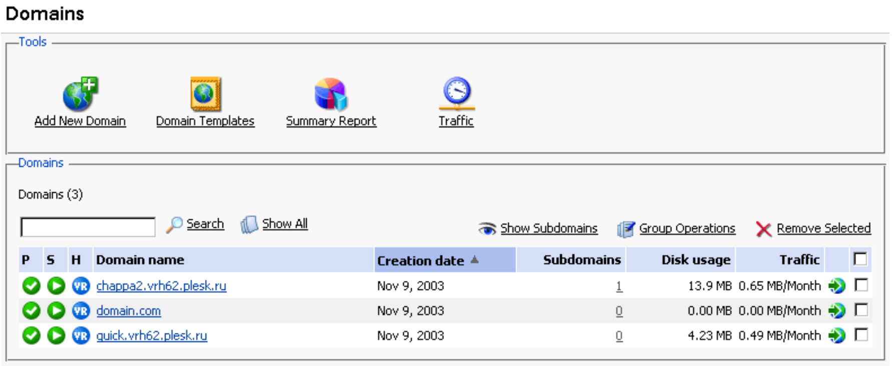
- Mail
- Mailing lists
- Tomcat
- Anonymous FTP

8. Click OK to apply the new settings to the selected domains.

Removing Domains

You can remove one or several domains at once. To remove domains:

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



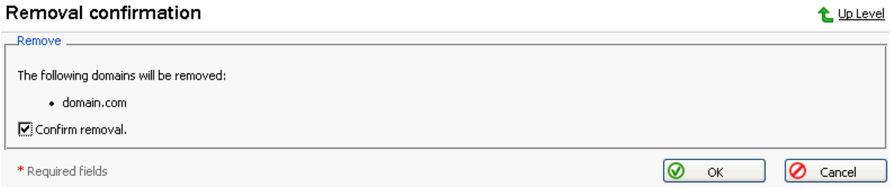
Domains

Domains (3)

P	S	H	Domain name	Creation date ▲	Subdomains	Disk usage	Traffic		☐
✓	▶	VR	chappa2.vrh62.plesk.ru	Nov 9, 2003	1	13.9 MB	0.65 MB/Month	➜	☐
✓	▶	VR	domain.com	Nov 9, 2003	0	0.00 MB	0.00 MB/Month	➜	☐
✓	▶	VR	quick.vrh62.plesk.ru	Nov 9, 2003	0	4.23 MB	0.49 MB/Month	➜	☐

2. Select the domains that you wish to remove by selecting the corresponding checkboxes.

3. Click Remove Selected. The Removal confirmation page appears:



Removal confirmation

The following domains will be removed:

- domain.com

☑ Confirm removal.

* Required fields

4. Select the checkbox to confirm removing, and click OK. If you decide not to delete these domains or wish to modify the list of domains selected for deletion, click Cancel.

Appendix A. Glossary of Terms

ASP

Short for Active Server Pages, a specification for a dynamically created Web page with a .ASP extension that utilizes ActiveX scripting - VB Script or Jscript code. When a browser requests an ASP, the Web server generates a page with HTML code and sends it back to the browser. ASPs are similar to CGI scripts, but they enable Visual Basic programmers to work with familiar tools.

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 Server, 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 network: neighborhood
- the organization type: com

Some top-level domain names:

- arpa: ARPAnet (a Defense Department communications system that established the Internet)
- com: Commercial, for-profit organizations and businesses
- edu: Educational institutions
- gov: Government organizations
- int: International organizations
- mil: U. S.-based military
- net: Internet access providers
- org: Non-profit organizations
- aero: Air-transport industry
- biz: Businesses
- coop: Cooperatives
- info: Information
- museum: Museums
- name: For registration by individuals
- pro: Accountants, lawyers, physicians, and other professionals
- 2-alphabetic characters: the country code top-level domains (ccTLDs), such as, for instance .uk for United Kingdom.

FTP

FTP, or File Transfer Protocol, is a method used to transfer files to (upload) and from (download) a remote server. You can use the FTP command to:

- Copy a file from the Internet to your PC

- Move a file from your PC up to the Internet
- Rename an existing file
- Delete a file
- Update an existing file with more recent data

GATEWAY

A gateway is a combination of hardware and software allowing dissimilar systems to communicate by filtering data through standardized protocols. Think of a gateway as a translator that allows your PC to talk with other computers on the network.

HOST

In a network, a host is usually a computer that stores software applications and data that may be accessed or retrieved by other users. But a host can be any addressable device on the network, not just a computer. The host provides services to other computers or users. An Internet Service Provider may also be referred to as a Web hosting company.

HTML

HTML, or HyperText Markup Language, is a standardized language for presenting information, graphics, and multimedia on the World Wide Web. HTML consists of hundreds of codes, tags, and symbols that define the type of information and how it should be displayed in a browser. HTML is universally understood on a wide variety of platforms.

HTTP

HTTP, or HyperText Transfer Protocol, is a standard for sharing World Wide Web files. HTTP lets you communicate across the Internet by carrying messages from your browser to a server.

IIS

Short for Internet Information Server, Microsoft's Web server that runs on Windows NT platforms.

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.

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.

MS FrontPage

Microsoft FrontPage is a software program that allows to create and manage Web pages.

MS SQL

Microsoft SQL Server is a database management system, which is optimized for the kernel of Windows NT.

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. My SQL 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.

.NET

A Microsoft server-side Web technology. ASP.NET takes an object-oriented programming approach to Web page execution. ASP.NET is used to create Web pages and Web services.

NETWORK

A network is a system of interconnected computers and peripheral devices (such as printers).

ODBC

ODBC is a programming interface that enables applications to access data in database management systems that use Structured Query Language (SQL) as a data access standard.

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

Short for Practical Extraction and Report Language, Perl is an interpretive programming language, especially designed for processing text. Because of its strong text processing abilities, Perl has become one of the most popular languages for writing CGI scripts.

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.

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

An interpreted, object-oriented programming language. Python is very portable since Python interpreters are available for most operating system platforms.

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. SSI can also be used to execute programs and insert the results; therefore they represent a powerful tool for web developers.

SSL

SSL stands for Secure Socket Layer, and is a set of rules used for exchanging information between two computer devices using a public encryption system. SSL establishes secure communications between servers and clients. SSL provides a safe and authenticated method of handling e-commerce transactions. Only authorized users can access and read an SSL-encrypted data stream. An alternative to SSL is Secure HTTP (S-HTTP), used to encrypt World Wide Web documents (rather than securing an entire session, as does SSL).

SSL CERTIFICATE

An SSL certificate is an electronic key that encrypts transmissions between two computers on a public network, providing privacy and security to the session. Think of an SSL certificate as an electronic ID card for an individual or a computer service. An SSL certificate confirms that a message that you receive actually did come from the person identified. The certificate key is issued by a third party. SSL certificates are used for secure e-commerce communications, protecting information such as credit card numbers and personal data. You can generate an SSL certificate with a utility such as SSLeay. Then, submit it to a certificate authority such as GeoTrust, Inc (www.geotrust.com).

TCP

TCP stands for Transmission Control Protocol, and is the primary data transport protocol on the Internet. TCP transmissions are fast, reliable, and full-duplexed.

TCP/IP

Transmission Control Protocol/Internet Protocol, commonly known as TCP/IP, is a data transmission protocol that was developed by ARPA, the Advanced Research Projects Agency. ARPA is the founding organization of the Internet.

TELNET

Telnet is a method of accessing another remote computer. You can only access the other computer if you have permission to do so. Telnet differs from other protocols that simply request information from a host computer, because it actually logs you on to the remote computer as a user.

TOMCAT

Tomcat is a server solution based on the Java Platform that supports the Servlet and JSP specifications. Managed by the Apache Jakarta Project, it is developed in an open and participatory environment.

URL

A URL is a Uniform Resource Locator used to identify an organization or domain on the Internet. URLs are standardized names that are typically found on the World Wide Web portion of the Internet. URL addresses identify domains on the network. Read about Domains for more detail.

USER

Simply put, a user is a client. In hardware terminology, a client is the PC that you use to access information from other computers (usually servers) on the Internet or network.

WEBMAIL

WebMail is a Web based interface to IMAP/POP3 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 web server 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.