Parallels® Plesk Control Panel

Parallels Plesk Control Panel 8.6 for Windows Administrator's Guide

|| Parallels™

Copyright Notice

Contents

Preface

In this section:

Who Should Read This Guide

This guide is intended for hosting resellers who manage their servers through Plesk and have access to server administrator's account in Plesk.

Typographical Conventions

Before you start using this guide, it is important to understand the documentation conventions used in it.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information	Example
Special Bold	Items you must select, such as menu options, command buttons, or items in a list.	Go to the **System** tab.
	Titles of chapters, sections, and subsections.	Read the **Basic Administration** chapter.
Italics	Used to emphasize the importance of a point, to introduce a term or to designate a command line placeholder, which is to be replaced with a real name or value.	The system supports the so called *wildcard character* search.
`Monospace`	The names of commands, files, and directories.	The license file is located in the `http://docs/common /licenses` directory.

`Preformatted`	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	`# ls -al /files` `total 14470`
`Preformatted Bold`	What you type, contrasted with on-screen computer output.	`# cd` `/root/rpms/php`
CAPITALS	Names of keys on the keyboard.	SHIFT, CTRL, ALT
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another.	CTRL+P, ALT+F4

Feedback

If you have found a mistake in this guide, or if you have suggestions or ideas on how to improve this guide, please send your feedback using the online form at http://www.parallels.com/en/support/usersdoc/. Please include in your report the guide's title, chapter and section titles, and the fragment of text in which you have found an error.

About Plesk

Plesk is a hosting automation solution that gives hosting providers full control over the managed Web hosting servers and simplifies setup and management of user accounts, Web sites, and e-mail accounts.

Plesk is stable, secure and reliable, and the main benefit of using Plesk is that it will save you and your technical staff much time and effort: all your customers (and customers of your resellers) will have personal isolated control panel environments and will be able to manage their sites and e-mail accounts on their own.

In this chapter:

Overview of Software Components Managed by Plesk

Plesk control panel works in cooperation with the following third-party software components and services:

- Microsoft IIS Web server or Apache Web Server *
- Microsoft FTP server
- Gene6 FTP Server 3.4.0.16 and Serv-U FTP Server **
- Bind DNS server
- Microsoft DNS server and Simple DNS Plus DNS server **
- MySQL, Microsoft Access and Microsoft SQL database servers ***
- Acronis True Image Enterprise Server backup system
- MailEnable mail server
- Merak, MDaemon, SmarterMail, hMailServer, CommuniGate Pro mail servers **
- Courier-IMAP IMAP/POP3 server
- SpamAssassin anti-spam software
- SiteBuilder
- Dr.Web and Kaspersky Antivirus antiviruses
- ClamAV and Merak Antivirus antiviruses **
- Webalizer and AWStats statistical packages
- Urchin and SmarterStats statistical packages **
- Microsoft FrontPage
- Horde IMP H3 web mail client
- MailEnable Web Client, IceWarp Web Mail 5, SmarterMail Web Client **
- Apache Tomcat

* - Plesk can work both with IIS and Apache web servers. Refer to Installation guide for more information.

** - Optional components supported by Plesk if they are installed in the system

*** - Plesk can host its own database on MySQL, Microsoft Access or Microsoft SQL database servers. Refer to Installation guide for more information.

Note: The web server (IIS or Apache) and Microsoft FTP server should be installed in the system before Plesk.

After installation of Plesk package, all essential services, such as DNS, Web, FTP and Mail are configured to run with the default optimal settings, so you can start serving your customers right away. However, we recommend that you review the default settings to make sure that they satisfy your needs, and create user account templates and domain templates, which will simplify further setup of hosting accounts.

Overview of Business Model, Users Accounts and Permissions

Plesk user accounts hierarchy is limited to four user levels:

- administrator account,
- client accounts,
- domain administrator accounts,
- e-mail user accounts.

For your customers who need to resell hosting services or host numerous domains/web sites, you will create client accounts.

Note: for the purpose of hosting your own sites, you should use a special service account which is created during Plesk setup. The account is registered with the control panel under the name **My Domains**.

Customers with access to client accounts can host on the server any number of sites you allow. They can host the sites of their own and/or resell hosting services to other users: for that purpose your resellers can create domain administrator accounts for their own customers.

Customers with access to domain administrator accounts cannot resell Web hosting services or host more than one site on their hosting accounts. They can only manage their own sites. In the current implementation of Plesk control panel, domain administrator accounts can be created only after the respective domains (web sites) are hosted on the server.

All site owners can set up e-mail accounts for themselves and provide other users with mail hosting services: for that purpose, they create e-mail user accounts and grant e-mail users with access to control panel.

Site owners can also host personal web pages or small sites for other users under their domains. However, the owners of such sites usually do not have their own domain names and cannot have a dedicated control panel environment.

All permissions for operations performed in the control panel you define for a reseller (client account) allow the reseller to further assign them to his or her customers. The resource allotments you define for a reseller can be further redistributed among reseller's customers. For a full list of permissions and resource usage limits you can define, refer to the Managing User Accounts (on page 114) section.

All quotas you define for a client or domain administrator's account are soft quotas: the control panel indicates resource overage by showing the respective icons in the control panel, sends notices by e-mail to the respective users, but it does not automatically suspend user accounts or Web sites.

The control panel does not have a built-in billing system, therefore, we recommend that you use a third-party solution of your choice, or use Plesk together with Parallels Business Automation solution.

What's New in This Version

Plesk Control Panel 8.6 offers you the following new features and enhancements:

Changing DNS zone SOA serial number format. The DNS zone SOA serial number format used by default in the Plesk Control Panel is Unix timestamp. You can change the format of the DNS zone SOA serial number to YYYYMMDDNN, which is recommended by IETF and RIPE and mandatory for many domains registered in some high-level DNS zones, mostly European ones.

Improved DNS zone update. Users can make multiple changes to a DNS zone without having to save every single change each time – all changes made to the DNS zone are now highlighted and visible to the user before saving them. The DNS zone is updated when the user saves the changes.

Permission for clients to select a target DB server. You can allow your customers to select a database server of each type for creating his or her databases, not only use the default database server.

Getting Started

This chapter describes the first actions you need to perform after installation of the Plesk Control Panel.

In this chapter:

Logging in to Plesk

> ➢ *To log in to your Plesk control panel:*

1 In the address bar of your web browser type the URL where your Plesk control panel is located and press ENTER. Plesk login screen will open.

   For example, type <u>https://your-domain.com:8443</u>, where `your-domain.com` is the domain name of your Web host.

2 Type the user name 'admin' and your password into the **Login** and **Password** boxes, respectively. If this is your first login to the freshly installed control panel, use the default password 'setup'.

3 If you log in for the first time, select the language for your control panel from the **Interface language** drop-down box. If you had previously specified the interface language and saved it in your interface preferences, leave the **User default** value selected.

4 Click **Login**.

   After your first login, you should accept the license agreement and then specify the host name and IP addresses to assign to the server.

5 In the **Full hostname** field, enter your server's host name. This should be a fully qualified host name but without a trailing dot (e.g. host.domain.tld).

6 Select the type of available IP addresses: exclusive or shared. By default, all available IP addresses are located in the **Exclusive IP addresses** field.

   ▪ To add an IP to the list of shared IP addresses, select the IP in the **Exclusive IP addresses** field and click **Add >>**.

   ▪ To remove an IP from the list of shared IP addresses, select the IP in the **Shared IP addresses** field and click **<< Remove**.

   Note: With Plesk you can mark all your IP addresses as shared or exclusive *before* you assign them to your customers. This allows the control panel to distinguish between them and not to let you assign a dedicated IP address to several customers at once. An exclusive IP address can be assigned to a single customer, while a shared IP address can be shared among several user accounts.

   You can skip this stage and define the type of IP addresses later (**Server** > **IP Addresses**).

7 In the **Administrator's preferences** section, change the default administrator password and click **OK**.

   Change the default administrator's password. Enter the new password and confirm it in the **New password** and **Confirm password** fields. The password can have up to 14 symbols. Note that the password is case sensitive.

Note: Do not forget to change the administrator's password from the default one to your own personalized password; otherwise, access to the control panel under the administrator account will be available with the default password 'setup', which is known to many users of Plesk.

---

8 On the next screen enter your contact information.

9 Select **I would like to receive periodic e-mails from Parallels announcing new products, discounts and more** check box to subscribe to the Parallels mailing list.

10 Select **I would like to create a default client account** if you want Plesk to create the default user account called **My Domains**. This account is typically used for hosting your own web sites.

11 Click **OK**.

In this section:

If You Forgot Your Password

xIf you forgot your password, you can retrieve it by using the password reminder feature in the control panel.

➢ *To use the password reminder:*

1 In your web browser's address bar, type the URL where your Plesk control panel is located (for example, https://your-domain.com:8443)

2 Press ENTER.

Plesk login screen will open.

3 Click the **Forgot your password?** link.

4 Specify your login name and e-mail address registered in the system.

5 Click **OK**.

6 Your password will be sent to your e-mail.

7 Once you received the e-mail from the password reminder, follow the provided instructions to create a new password.

Becoming Familiar with Plesk's Interface

When you log in to control panel, it can open in either a **standard view**, a simplified **desktop view**, or a combination of both. The standard view is a customary view of the control panel divided into two main areas: navigation pane on the left and the main screen where operations are performed on the right.
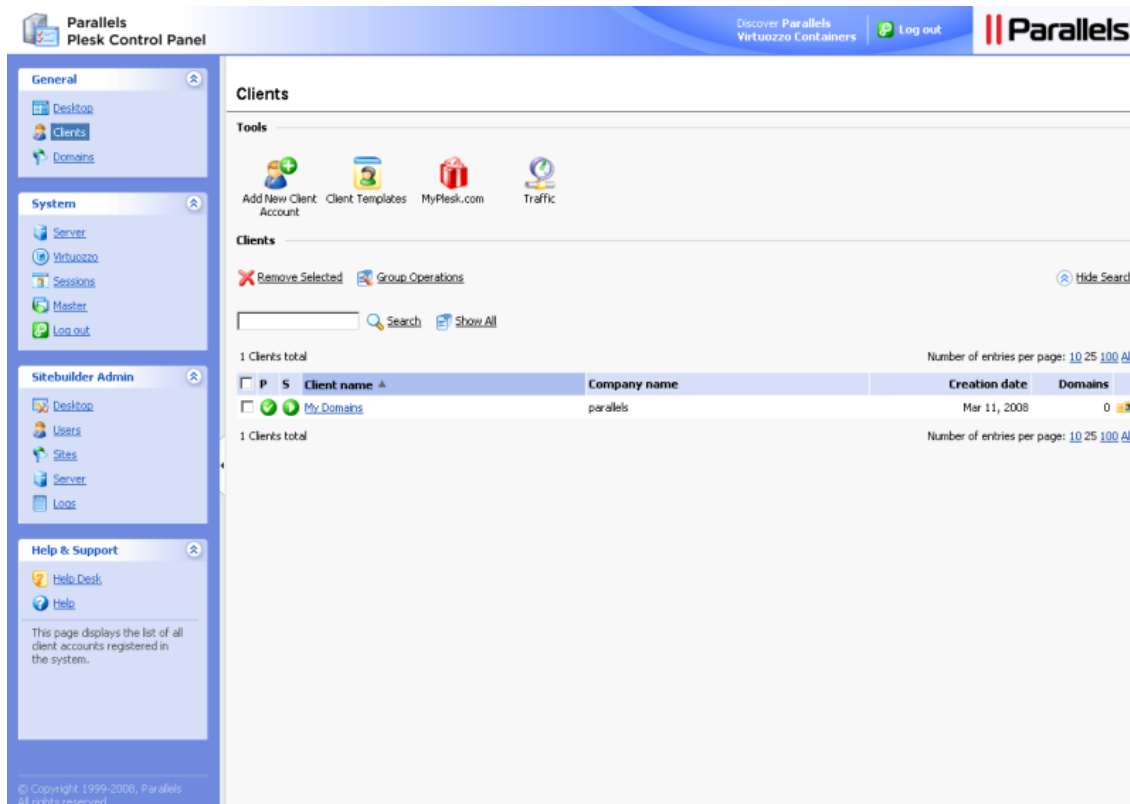
The desktop view can show server statistics and shortcuts to the operations you frequently perform—everything you may need can now be accessible from a single screen.
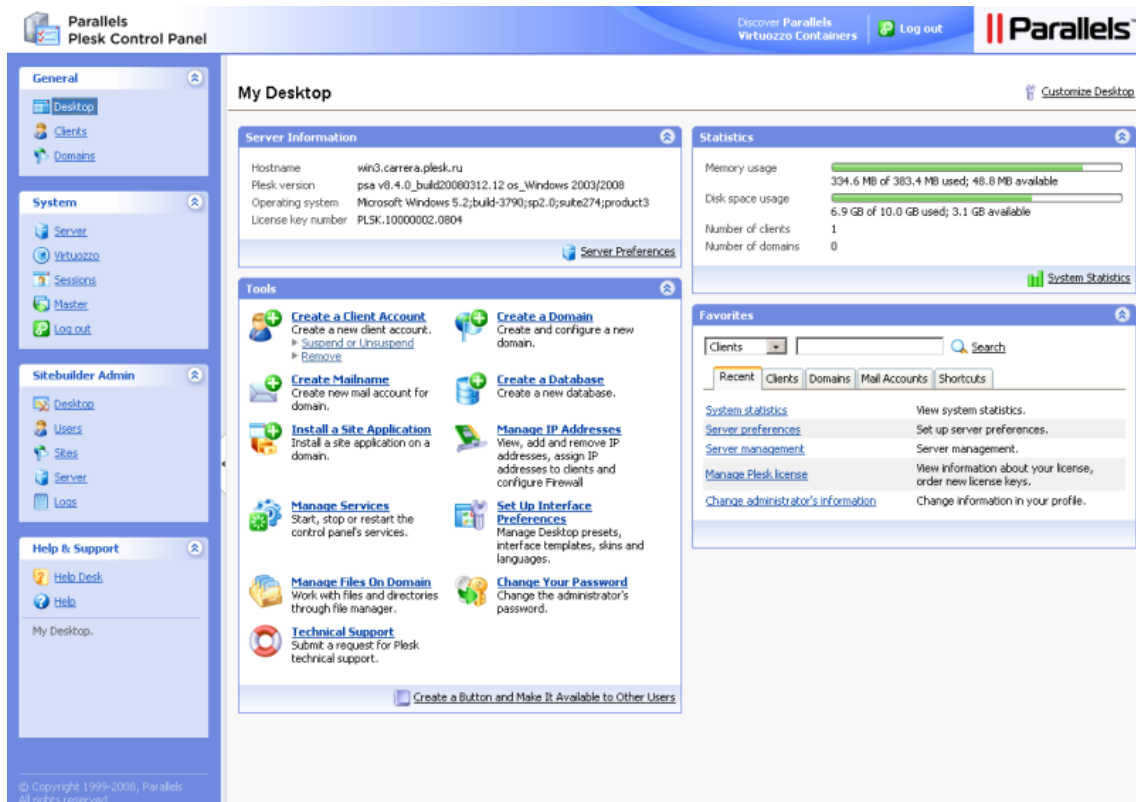
You can switch between the views (by installing the appropriate license key) or use a combination of them for your control panel. You can also specify what view should be shown to other control panel users. To customize your control panel, refer to the Customizing Your Control Panel chapter.

In this section:

Items in the Desktop View

The desktop view originally shows four sections:

- **Server Information**. This shows your hostname, control panel version, operating system and kernel versions, license key number, and system uptime.
- **Statistics**. This shows average processor load for the last minute, five minutes, and fifteen minutes, memory and disk space usage, number of served client accounts and hosted domains (Web sites). The client accounts include accounts of resellers and customers who have several sites—owners of a single domain are not counted.
- **Tools**. This group shows shortcuts to the operations that you can perform through the control panel. You can freely add and remove these shortcuts.
- **Favorites**. This group shows five types of shortcuts sorted by type and placed on the respective tabs. The **Clients** tab shows the shortcuts to administrative tools available for a selected user account, the **Domains** tab shows shortcuts to domain administration tools, the **Mail Accounts** tab shows shortcuts to the e-mail account administration tools. The **Shortcuts** tab shows all other types of shortcuts that do not relate to user accounts, domains and e-mail accounts. The **Recent** tab shows last ten control panel screens you have been on. The **Favorites** group also provides search tool for finding user accounts, web site hosting accounts, and e-mail accounts. To use the search tool, select the item type from the drop-down box, type the search criteria (this can be any combination of symbols, search is case insensitive) and click **Search**.

In this section:

Using Wizards

When you work with Plesk in the Desktop view, you accomplish the tasks you need through wizards. Each wizard is a series of consecutive screens. To accomplish a task using a wizard, follow the instructions displayed on the wizard screens. For information on individual options, refer to the respective sections of this guide.

Items in the Standard View

The navigation pane is located on the left. It gives you access to sets of administrative functions:

- **General** set.
  - **Clients.** This is where you manage your clients and all data related to their accounts.
  - **Domains.** This is where you manage Web sites and their respective e-mail services.
- **System** set.
  - **Server.** This shortcut gives you access to server administration functions.
  - **Sessions.** When clients, site and mailbox owners log in to control panel, or connect to the server via FTP protocol, they establish sessions that you can monitor and terminate.
  - **Global Account.** This shortcut appears in your Plesk Control Panel when the single sign-on capabilities are switched on the hosting server. Single sign-on technology allows you to log in to different Parallels products using a single global login name and password. This shortcut is used for changing the global login settings.
  - **Master.** This shortcut gives you access to centralized management of Plesk enabled servers.
  - **Log Out.** When finished working with control panel, click this icon to close your session.
- **SiteBuilder Admin** set.
  - **Desktop**. Opens up SiteBuilder Desktop, which is divided into two areas: **Tasks** and **Statistics**. In the **Tasks** area you can see an overview of main functionalities of the Administrator Panel. In the **Statistics** area you can see how many users, sites, are currently in the system.
  - **Users.** Click this shortcut to open the **Users** screen. On this screen you can see the list of available users. Here you can manage the user accounts.
  - **Sites.** On this screen you can see the list of available websites created in SiteBuilder and manage them.
  - **Server.** This page allows you access to the SiteBuilder's server administration functions.
  - **Logs.** Click **Logs** to view system and security logs of operations performed in SiteBuilder by your dependent users.
- **Help & Support** set.

- **Help Desk.** This is the help desk system integrated with your control panel. You can use it to view and solve the problems reported to you by your customers.
- **Help.** Provides context sensitive help.

Below the **Help** icon, there is a context help tip area. It provides a brief description of the current screen or available operations. When you place the mouse pointer over a system element or status icon, it displays additional information.

To navigate through Plesk, you can also use a path bar: a chain of links that appears in the right part of the screen, below the banner area. To return to a previous screen, use **Up Level** in the upper-right corner of the screen.

To find items in lengthy lists, use search boxes located above every list of items: type a search criterion into the input box, and click **Search**. A list will show the items matching the search criteria. To return back to viewing all items, click **Show All**. You can hide the search area by clicking **Hide Search**. To show the hidden search area, click **Show Search**.

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.

Changing Your Password and Contact Information

➢ *If you need to update your contact information*

1   Go to **Server** > **Edit**.

2   Update your information as required, and click **OK**.

➢ *If you need to change your password:*

1   Go to **Server** > **Change Password**.

2   Enter your old and new passwords, and click **OK**.

➢ *If you forgot your password:*

1   In your web browser's address bar, type the URL where your Plesk control panel is located (for example, https://your-domain.com:8443)

2   Press ENTER.

    Plesk login screen will open.

3   Click the **Forgot your password?** link.

4   Specify your login name and e-mail address registered in the system, and click **OK**.

5   Your password will be sent to your e-mail.

Once you received the e-mail from the password reminder, follow the provided instructions to create a new password.

Configuring Your Control Panel

This chapter discusses the configuration steps required to set up and manage your Plesk Control Panel.

In this chapter:

Upgrading License Key for Your Control Panel

Plesk comes with a trial license key, which is automatically installed to the control panel. This license key allows you to create one user account, host one Web site and one mail box. Therefore, to fully use the Plesk Control Panel as you need, you should obtain a license key from Parallels or one of its resellers and install it to the control panel.

Plesk license keys have a built-in expiration date. This has been implemented to help prevent fraud and theft. It requires the Plesk software to check with Parallels licensing server during a 10 day grace period (prior to the expiration date) to verify that the key has not been reported stolen and is being used in accordance with the End User License Agreement (that is, installed on only one server). Once this is verified, the expiration date is prolonged.

Plesk will attempt to connect over TCP/IP to the licensing server through port 5224. Please make sure that this is not blocked by a firewall. The update process runs automatically and the Plesk administrator does not need to do anything unless there is a problem. Should the Plesk key expire, check your firewall and then go to **Server** > **License Management** and click **Retrieve Keys**. If the key cannot be updated, contact your reseller or Parallels (if you purchased the license key directly from Parallels).

You can test the connection to the licensing server anytime by going to **Server** > **License Management** and clicking **Retrieve Keys**.

In this section:

Upgrading the Trial License Key

> ➢ *To upgrade the trial license key:*

1 Go to **Server** > **License Management** and click **Order New Key**.

2 The Parallels online store will open in a separate browser window. In this window, select the items and features you want to include into your Plesk license and click **Submit**. In the next steps, indicate the currency, number of license keys, provide contact details, billing address, and payment method, and submit the form. The new key will be sent to the specified e-mail address.

3 Save the new key to the hard drive on your local machine.

4 Open again the **License Management** screen in Plesk (**Server** > **License Management**) and click **Upload Key**.

5 Enter the path to the key file that you saved on your local machine or click **Browse** to locate it.

6 Select the **Replace the currently installed license key with the selected one** check box to confirm that you really want to replace the current license key with the new one.

If this check box is not selected, the new license key will not be installed and installation will be aborted.

7 If your new license key allows hosting fewer sites than you already host on the server, Plesk will stop working. However, to prevent the control panel from comparing the amount of the resources used and those covered by the new key, select the **Allow the resources usage override** check box.

This might be helpful if you want to temporarily install a license key that covers less resources and then upgrade it through the control panel interface.

8 Click **OK** to install the new key to the control panel.

Installing Additional License Keys

➢ *To order an additional license key from Parallels online store, and install it to control panel:*

1   Go to **Server** > **License Management**.

2   Click **Order New Key**.

3   The Parallels online store page listing available add-ons will open in a separate browser window. On this page, select the add-ons you want to order and click **Submit**.

4   Because you already have one license key, the Plesk Number Checking System page will open. Enter the number of your license key to which you add more license keys and click **Submit**.

5   In the next steps, indicate the currency, number of keys, provide contact details, billing address, and payment method, and submit the form. You will be notified by e-mail when your order is processed.

6   When you receive the e-mail notification, return to the **License Management** screen (**Server** > **License Management**), on the **Additional License Keys** tab click **Retrieve Keys** to retrieve the ordered license key. Plesk License Manager will retrieve the upgraded license key from the Parallels licensing server and automatically install it to your control panel.

➢ *If you uploaded an additional license key to the control panel, and after that installed the respective application on the server, follow these steps to install the license key:*

1   Go to **Server** > **License Management** > **Additional License Keys**.

2   Click the license key you want to install.

3   Click **Install Key**.

Upgrading Your License Key

If you are planning to expand your customer base and host more sites on the server than your current license allows, you need to upgrade your license key.

➢ *To upgrade the license key:*

1   Go to **Server** > **License Management**.

2   Click **Order New Key**.

3   On the Parallels online store page, select the desired upgrade option and click **Submit**.

4   In the next step, indicate purchase details and submit the form. You will be notified by e-mail when your order is processed.

5   After you receive the e-mail notification, return to the **License Management** screen (**Server > License Management**) and click **Retrieve Keys** to retrieve the ordered license key. Plesk License Manager will retrieve the purchased license key from the Parallels licensing server and automatically upload it to your control panel.

Rolling Back to Previously Used License Key

If you installed wrong license key for the control panel or a Plesk add-on, you can roll back to the previously used license key.

➢ *To roll back to previously used license key:*

1   Go to **Server** > **License Management**.

2   If you want to restore a license key for your control panel, go to the step 4 of this procedure. If you want to restore an additional license key for an application, click **Additional License Keys**.

3   Click **Roll Back Key**. You will be shown the list of properties for the key that you wish to roll back to.

4   Click **OK** to roll back to the previously used license key.

Note. Using the rollback function again will revert Plesk to the key you originally used before the previous rollback.

Securing Your Control Panel

In this section:

Restricting Administrative Access to Control Panel

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

➢ *To allow administrative access to control panel only from specific IP addresses or networks:*

1 Go to **Server** > **Access**.

2 Click **Add New Network** and specify the required IP addresses. Click **OK**.

To specify subnets, you can use wildcard symbols (*) and subnet masks.

3 Select the **Denied from the networks that are not listed** option, and click **Set**. When prompted to confirm the operation, click **OK**.

➢ *To prohibit administrative access from specific IP addresses or networks:*

1 Go to **Server** > **Access**.

2 Click **Add New Network** and specify an IP address. Click **OK**.

To specify subnets, you can use wildcard symbols (*) and subnet masks.

3 Select the **Allowed, excluding the networks in the list** option, and click **Set**. When prompted to confirm the operation, click **OK**.

By default Plesk allows multiple simultaneous sessions for several users logged into the control panel using the same login and password combination. This can be useful when delegating management functions to other users or in case if you accidentally close your browser without logging out, thus becoming unable to log in again until your session expires. You may want to switch off this capability, if you do not need it.

➢ *To disallow concurrent sessions for your administrative control panel:*

1 Go to **Server** > **Edit**.

2 Clear the **Allow multiple sessions under administrator's login** check box and click **OK**.

Securing Communication to Server with SSL Encryption

For security reasons, you can access your control panel only through a secure connection provided by Secure Sockets Layer-enabled hypertext transfer protocol. All data you exchange with the Plesk managed server are encrypted, thus preventing interception of sensitive information. The SSL certificate used in the data encryption process is automatically generated and installed on the server during installation of the control panel. This is the so-called self-signed certificate: it is not signed by a recognized certification authority (CA), therefore, upon attempt to connect to your control panel, you and your customers will see warning messages in Web browsers.

To gain customer confidence, you should purchase an SSL certificate from a reputable certification authority, and install it to the control panel.

You can either:

- use the facilities for purchasing SSL certificates from Comodo, GeoTrust, Inc. or GoDaddy provided by your control panel,

  OR

- create a certificate signing request (CSR) from the control panel and submit it to the certification authority of your choice, which will create an SSL certificate for you.

  Note: If you are going to use the control panel's facilities for purchasing a certificate through MyPlesk.com online store, you should not use command line tools for creating the certificate signing request.

> *To purchase an SSL certificate from Comodo, GeoTrust, Inc. or GoDaddy through MyPleskCom online store and secure your control panel:*

1 Go to **Server** > **Certificates**. A list of SSL certificates that you have in your repository will be displayed.

2 Click **Add New Certificate**.

3 Specify the certificate properties:

- Certificate name. This will help you identify this certificate in the repository.

- Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.

- Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.

- Specify the host name for which you wish to purchase an SSL certificate. For example: your-domain.com

- Enter your e-mail address.

4 Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.

5 Click **Buy Cert**.

Your private key and certificate signing request will be generated — do not delete them. MyPlesk.com login page will open in a new browser window.

6   Register or log in to an existing MyPlesk.com account and you will be taken step by step through the certificate purchase procedure.

7   Choose the type of certificate that you wish to purchase.

8   Click **Proceed to Buy** and order the certificate. In the Approver E-Mail drop-down box, please select the correct Approver e-mail.

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

9   Once your certificate request is processed, you will be sent a confirmation e-mail. After you confirm, the certificate will be sent to your e-mail.

10   When you receive your SSL certificate, save it on your local machine or network.

11   Return to the SSL Certificates repository (**Server** > **Certificates**).

12   Click **Browse** in the middle of the page and navigate to the location of the saved certificate. Select it, and then click **Send File**. This will upload the certificate to the repository.

13   Select the check box corresponding to the certificate you just added, and click 🔼 **Secure control panel**.

➢   *To secure your control panel with an SSL certificate from other certificate authorities:*

1   Go to **Server** > **Certificates**. A list of SSL certificates that you have in your repository will be displayed.

2   Click **Add New Certificate**.

3   Specify the certificate properties:

   ▪   Certificate name. This will help you identify this certificate in the repository.

   ▪   Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.

   ▪   Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.

   ▪   Specify the host name for which you wish to purchase an SSL certificate. For example: your-domain.com

   ▪   Enter your e-mail address.

4   Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.

5   Click **Request**. Your private key and certificate signing request will be generated and stored in the repository.

6   In the list of certificates, click the name of the certificate you need. A page showing the certificate properties opens.

7   Locate the **CSR section** on the page, and copy the text that starts with the line **-----BEGIN CERTIFICATE REQUEST-----** and ends with the line **-----END CERTIFICATE REQUEST-----** to the clipboard.

8 Visit the Web site of the certification authority from which you want to purchase an SSL certificate, and follow the links on their site to start a certificate ordering procedure. When you are prompted to specify CSR text, paste the data from the clipboard into the online form and click **Continue**. The certification authority will create an SSL certificate in accordance with the information you supplied.

9 When you receive your SSL certificate, save it on your local machine or network.

10 Return to the SSL Certificates repository (**Server** > **Certificates**).

11 Click **Browse** in the middle of the page and navigate to the location of the saved certificate. Select it, and then click **Send File**. This will upload the certificate to the repository.

12 Select the check box corresponding to the certificate you just added, and click 🔁 **Secure control panel**.

➤ *In case you need to generate a self-signed certificate, follow this procedure:*

1 Go to **Server** > **Certificates**. A list of SSL certificates that you have in your repository will be displayed.

2 Click **Add New Certificate**.

3 Specify the certificate properties:
  ▪ Certificate name. This will help you identify this certificate in the repository.

  ▪ Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.

  ▪ Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.

  ▪ Specify the host name for which you wish to purchase an SSL certificate. For example: your-domain.com

  ▪ Enter your e-mail address.

4 Click the **Self-Signed** button. Your certificate will be generated and stored in the repository.

Setting Up Global Account

Global Account is a single sign-on (SSO) technology feature that allows you to log in to different Parallels products using a single global login and password. If you have several accounts in Plesk Control Panel, you can connect them all to a global account and switch between these accounts without entering a password every time. You can also connect all your accounts in other Parallels products to your global account and switch between them without providing credentials.

➢ *To switch on support for single sign-on for your server, do the following:*

In Plesk Control Panel for Linux/Unix

1 Find out the IP address of the SSO server that you will be using. It can be provided by your hosting company, or you can set up the SSO server on any machine that is accessible over the Internet, including your Plesk Control Panel server. For installation instructions, refer to the Plesk Control Panel Installation Guide.

2 Register your server with the single sign-on server: issue the command `<plesk_installation_directory>/admin/sbin/sso -server https://idp-master.example.com:11443`.

3 Switch on single sign-on: issue the command `<plesk_installation_directory>/admin/sbin/sso -e`.

➢ *In Plesk Control Panel for Windows*

1 Find out the IP address of the SSO server that you will be using. It can be provided by your hosting company, or you can set up the SSO server on any machine that is accessible over the Internet, including your Plesk Control Panel server. For installation instructions, refer to the Plesk Control Panel Installation Guide.

2 Register your server with the single sign-on server: issue the command <plesk_installation_directory>\sso.exe -server https://idp-master.example.com:11443.

3 Switch on single sign-on: issue the command <plesk_installation_directory>\sso.exe -e.

In this section:

Creating A Global Account

After you create a global account and connect local accounts to it, you will be able to choose from any account connected to your global account when logging in under your global account.

➢ *To create a global account:*

1 Log in to Plesk, go to **Global Account** and click **Connect To Global Account**.

2 Select **Create new global account** and provide the login and password for your global account.

3 Click **OK**.

> Your global account is active now, so you can proceed with connecting other accounts to it. Refer to Connecting Local Accounts to Your Global Account (on page 33) section for more information.

Connecting Local Accounts To Your Global Account

➢ *To connect a local Plesk account to your global account:*

1 Log in to Plesk under the local account you want to connect.

2 Go to **Global Account** and click **Connect To Global Account**.

3 Make sure that **Use existing global account** option is selected and provide the login and password for the global account you want to connect to.

4 Click **OK**.

> Repeat steps 1-4 for other local accounts as necessary.

➢ *To connect an account in another product with SSO support to your global account:*

1 Log in to software product with SSO support under the account you want to connect.

2 Follow the instructions on connecting to a global account in respective software product documentation. Make sure that you provide the credentials for the existing global account when you are asked to.

Repeat steps 1-2 for other accounts or products as necessary.

Note. Different software products may use different names for the Global Account feature, such as Federated Identity or Global Login. Refer to respective software product documentation for more information.

After you have connected all required accounts to your global account, you can log in under your global account all the time in any product where you have a local account connected to your global account. You will be shown the list of local accounts connected to your global account every time you log in under it, so you can choose which account you would like to use now. You can switch to another account any time you want. Refer to Switching Between Accounts (on page 34) section for more information.

Switching Between Accounts

➢ *To switch to another account:*

1 Click **Switch User** in the upper right corner.

2 Select the account you want to switch to:

▪ Choose the required local account from the list of accounts connected to your global account

or

▪ Select **Specify credentials for another account** and provide login and password for a local account not connected to your global account or to another global account. You can also specify the language for your control panel from the **Interface language** menu. If you had previously specified the interface language for that account and saved it in its interface preferences, leave the **Default** value selected.

3 Click **OK**.

Changing Global Account Password

➢ *To change password of your global account:*

1 Log in to Plesk under your global account or any local account connected to it.

2 Go to **Global Account** and click **Change Password**.

3 Enter your old and new passwords, and click **OK**.

Disconnecting Local Accounts From Global Account

➤ *To disconnect a local account from your global account:*

1 Log in to Plesk under the local account you want to disconnect.

2 Go to **Global Account** and click **Disconnect From Global Account**.

3 Confirm the disconnection and click **OK**.

Repeat steps 1-3 for other local accounts as necessary.

Customizing Your Control Panel

The control panel's Desktop view and Standard view (as described in the chapter Becoming Familiar with Plesk's Interface (on page 16)) have different customization settings which are adjusted in different areas of the control panel.

To customize the Desktop view, refer to the section Customizing the Control Panel in the Desktop View (on page 46).

To customize the Standard view (that is, all areas and screens of the control panel except for Desktop), refer to the section Customizing the Control Panel in the Standard View (on page 36).

Note that you can choose to have in your control panel only Desktop view, only Standard view, or both views at once: to do this, you need to obtain and install a license key that supports the required interface view. However, you can specify what view should be shown to other control panel users regardless of your license key features.

This chapter explains how to accomplish the following tasks:

Change the interface language and theme (skin) for your control panel (on page 36)

Remove unwanted buttons from the control panel (on page 37)

Add custom hyperlink buttons to the control panel (on page 45)

Set a custom logo to the banner area of the control panel

Add support for more control panel languages

Add interface themes (skins)

Add to and remove items from the Desktop (on page 46)

In this section:

Changing Interface Language and Skin

> *To change the interface language and skin for your control panel:*

1 Go to **Server > Edit**.

2 Specify the following:

  a **Button label length.** To prevent lengthy button captions in languages other than English from overlapping in the control panel, you may want to specify a limit here. Any button caption longer than the defined limit will be shortened and ended with ellipsis (...).

  b **Administrator's interface language.** Select the language for your control panel.

  c **Administrator's interface skin.** Select the skin (theme) for your control panel.

  d **Desktop preset.** Once you customize the desktop and save the settings in a template as described in Using Desktop Presets (on page 48), you will be able to select your template here.

  e **Administrator's interface customization template.** Once you customize the control panel and save the settings in a template as described in Using Interface Customization Templates (on page 37), you will be able to select your template here.

  f **Allow multiple sessions under administrator's login.** By default Plesk allows multiple simultaneous sessions for several users logged into the control panel using the same login and password combination. This can be useful when delegating management functions to other users or in case if you accidentally close your browser without logging out, thus becoming unable to log in again until your session expires. You may want to switch off this capability, if you do not need it.

  g **Prevent users from working with the control panel until interface screens are completely loaded.** Leave this selected to avoid errors that might occur when users try to interact with control panel before is it ready.

3 Click **OK**.

Customizing the Control Panel in the Standard View

In this section:

Using Interface Customization Templates

Interface customization templates are sets of interface customization options assigned to Plesk users. You can configure custom settings for interface elements and save these settings in a template. Then, you assign the template to specific client accounts.

Default Customization Template is created automatically after Plesk installation. Initially, the default template allows user access to all interface elements of the control panel. The default template is automatically applied to all user accounts, including the administrator, if no other template is explicitly specified. The default template cannot be removed from the control panel. You can set another template as a default one. In the list of templates, the default template is displayed in bold.

Thus, to customize interface options for customers, you can either modify the default template or create own customization templates and assign them to user accounts.

Note that if you need to hide only buttons related to MyPlesk.com e-commerce portal and buttons related to currently unavailable features (such buttons are shown in the control panel as grayed out), you can do so without using interface customization templates. This is described in Hiding and Unhiding Sets of Buttons.

In this section:

Creating Templates

> *To create a template and specify custom rules for interface elements:*

1 Go to **Server** > **Interface Management** > **Interface Templates** tab and click **Add Interface Template**.

2 On the next page, enter the name for the new template. This field is required.

3 Select the **Default** check box to make this template default.

Remember that the default template is applied to all user accounts for which no other template is explicitly defined.

4 Click **Show Toolbar** to customize the rules for interface elements.

The toolbar serves to customize the appearance of buttons on Plesk screens for user accounts. The toolbar appears at the bottom of a Plesk screen. When the toolbar is on, you can navigate through Plesk interface screens and define rules for separate buttons.

5 Navigate to a Plesk screen on which you want to customize interface elements.

6 On the toolbar, click the **Customize** button to switch on the customization mode.

7 Click the transparent screen over a button you want to customize and select one of the following options in the drop-down menu:

- Hide – Hide this button from all users, including the administrator
- Admin Only – Hide this button from all users, but show for the administrator
- Show – Always show this button for all users
- Default – Reset previous customizations you have made for this button to the default settings.
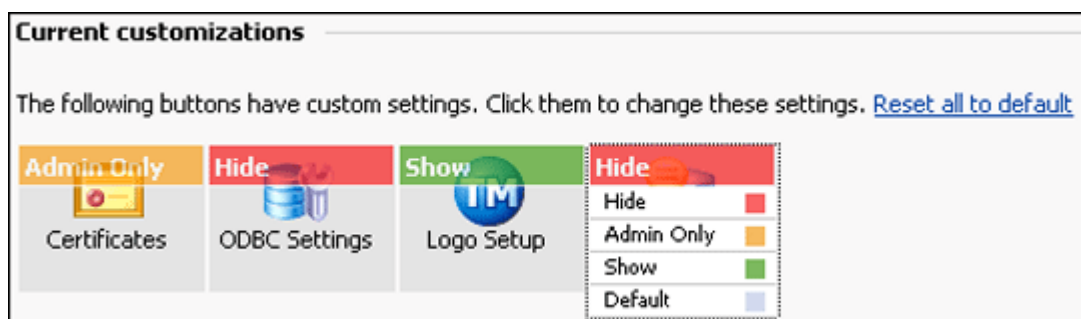
8 When you finish customizing buttons, click **OK** on the toolbar.

9 Click **Hide toolbar** to exit the customization mode.

10 Return to the list of interface customization templates (**Server** > **Interface Management** > **Interface templates**).

The template you have just created is added to the list of customization templates. You can now assign the template to user accounts.

Assigning Templates to User Accounts

> *To assign a template to your interface:*

1 Go to **Server** > **Edit**.

2 In the **Administrator's interface customization template** menu, select the customization template you need and click **OK**.

Note: In the list of templates, the template currently used for the administrator's interface is shown in italic. The default template name is displayed in bold. If you are using the default template, it is marked as bold italic.

> *To assign a template to a client account:*

1 Go to **Server** > **Interface Management** > **Interface Templates** tab.

2 In the list of templates, click the number in the **Usage** column.

This number shows the number of client accounts that currently use this template.

3 Click **Add New Client** to assign this template to another client account.

4 In the list of clients that do not use this template, select one or several client accounts and click **OK**.

The template will be assigned to the selected client accounts.

Note: You can also assign a template to a client when you are creating a new client account or editing client account preferences. To create a new account, click **Clients** in the navigation pane, then click **Add New Client Account**. To edit client account preferences, click **Clients** in the Navigation pane and then click the client name you need.

Removing Templates

> *To remove one template or several templates from the control panel:*

1 Go to **Server** > **Interface Management** > **Interface Templates** tab.

2 Select a template or several templates using the check boxes on the right.

3 Click ✕ **Remove Selected**.

4 Confirm the removal and click **OK**.

The specified templates are removed from the control panel and the default template is assigned to all users that previously used the removed templates.

Changing Default Template

> ➢ *To set another template as a default template:*

1   Go to **Server** > **Interface Management** > **Interface Templates** tab.

2   Select a check box corresponding to the template you need.

3   Click ☑ **Default**. The selected template will be used for all users for which no template is explicitly defined.

Exporting and Importing Templates

> ➢ *To import a template created on one Plesk server to another Plesk server:*

1   Go to **Server** > **Interface Management** > **Interface Templates** tab.

2   Click the 🖫 icon to save the template you want to export to a file.

3   In the **File Download** dialog box, click **Save** and specify the location on your hard drive where to save the file.

   The template settings will be saved as a template_name.xml file.

4   Transfer the template file to another Plesk server.

5   On another Plesk-enabled server, go to **Server** > **Interface Management** > **Interface templates** tab and click **Upload**.

6   Enter the name of the template to be imported or locate the template file on the hard drive.

   The file must be in .xml format.

7   Click **OK**. View the customization settings of this template. In this step, you can click **Show Toolbar** to edit the template.

8   When you finish editing, click **OK**. The new template will be uploaded to this machine.

9   Assign this template to client accounts (see the Assigning Templates to User Accounts section).

Hiding and Unhiding Sets of Buttons

You can easily hide predefined groups of buttons from the Plesk interface. In this case, users do not see the controls they are not allowed to operate or the features that are not supported (services not installed).

➢ *To hide groups of buttons:*

1 Go to **Server** > **Interface Management** > **Interface Templates** tab and click **Preferences**.

2 Select the check boxes to hide the following groups of controls:

▪ Buttons unavailable to users. Originally, unavailable (grayed out) icons in the control panel interface show services or components that are not installed and, hence, cannot be managed through the control panel. You can hide these buttons to prevent users from being disappointed that some services are unavailable. To hide all unavailable buttons, select the **Hide all unavailable buttons** check box.

▪ Limit management controls. To prevent users from viewing grayed out limit management controls they are not allowed to operate, select the **Hide all unavailable limits** check box.

▪ Permission management controls. To prevent users from viewing grayed out permission management controls they are not allowed to operate, select the **Hide all unavailable permissions** check box.

3 Under **Button groups**, select the check boxes to hide the following sets of buttons:

▪ Buttons related to services provided by MyPlesk.com online store. If you are reselling domain registration services and SSL certificates, select the check boxes **Hide buttons for domain registration**, **Hide buttons for certificate purchasing**, and **Hide buttons for extra services**. All buttons related to MyPlesk.com will be removed from the control panel at all user levels.

▪ Mail bounce controls. If you wish to prohibit your users from using their own mail bounce policies for e-mail addressed to nonexistent e-mail recipients within their domains, select the **Hide mail bouncing controls** check box.

4 Click **OK**.

➢ *To make groups of hidden buttons visible in the interface:*

1 Go to **Server** > **Interface Management** > **Interface Templates** tab and click **Preferences**.

2 Clear the corresponding check boxes to make the hidden groups of buttons again visible in the interface, then click **OK**.

Installing And Uninstalling Interface Languages

You can download new language packs from Parallels site and install them to the control panel. The number of languages you can use with your control panel depends on the license key you purchased. The control panel will alert you when you attempt to install more languages than allowed.

➢ *To view the interface languages installed in the control panel:*

1 Go to **Server** > **Interface Management**. The following information is displayed:

- **Language pack** contains the two-letter language code;

- **Language** shows the name of the language;

- **Used** displays the number of control panel users at all levels that use this language in their interface.

➢ *To select a new default language for the control panel:*

1 Go to **Server** > **Interface Management**.

2 Select the check box corresponding to the language you wish to set as default and click ☑ **Default**.

➢ *To install a new language pack:*

Download the required language pack file from Parallels web site and run it. The installation wizard will install the language pack in your system, enabling you and Plesk control panel users to choose the corresponding language during the login or on their personal settings page.

➢ *To uninstall a language pack from the control panel:*

1 Click **Start** on the OS taskbar and select **Control Panel** > **Add or Remove Programs** shortcut.

2 Select the language pack you want to remove and click **Change/Remove**.

3 Confirm the removal. The language pack you selected will be removed from the system.

If the language pack you have just removed is used by some other users, their interface language will be automatically set to the default language pack. The default language of the Plesk distribution package (en-US) cannot be removed.

Installing and Uninstalling Control Panel Themes (Skins)

You can develop and use custom skins for your control panel. Be aware that use of skins created by third parties can be dangerous, as the skin packages can contain malicious code. We strongly recommend that you use only the skins received from the trusted sources.

➢ *To view currently installed skins:*

1 Go to **Server** > **Interface Management**.

2 Click the **Skins** tab.

➢ *To set a new default skin:*

1 Go to **Server** > **Interface Management** > **Skins** tab.

2 Select the skin you wish to set as default:

- Click a skin you wish to set as default and click **Set Skin**

  or

- Select the corresponding check box and click ✅ **Default**.

➢ *To download a skin package to your local computer:*

1 Go to **Server** > **Interface Management** > **Skins** tab.

2 Click the appropriate 💾 icon, or click a skin title and then click **Download Skin**.

3 Select the type of archive you would like to have the skin files packed into, and click **OK**.

  Once the skin is prepared for downloading, a file download dialog window appears.

4 Click **Save**, specify the location and file name for the downloaded skin package file to be saved, and then click **Save**.

You can now prepare your own skin by modifying the contents of the downloaded archive file. To learn how to create custom skins for Plesk control panel, see the Creating And Installing Custom Plesk Skins guide. You can access this guide by clicking **Custom Plesk Skins** on the Skin Management page (**Server** > **Interface Management** > **Skins**)

➢ *To install a new skin to control panel:*

1 Go to **Server** > **Interface Management** > **Skins** tab.

2 Click **Add New Skin**. Specify the skin package file location and click **OK**.

➢ *To update the contents of an already installed skin:*

1 Go to **Server** > **Interface Management** > **Skins** tab.

2 Click a skin title and then click **Update Skin**. Specify the skin package file location and click **OK**.

➢ *To remove one or several skins from the repository:*

1 Go to **Server** > **Interface Management** > **Skins** tab.

2 Select the corresponding check box and click ✖ **Remove Selected**. Then, confirm removal and click **OK**.

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

Rebranding Your Control Panel

You can replace the default Plesk logo banner in the top frame with your own logo, and change the text that displays in the web browser's title bar. You can also make your logo a clickable hyperlink.

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

➢ *To change the control panel's logo image and text shown in web browser's title bar:*

1   Go to **Server** > **Branding**.

2   Clear the **Use default** check box and type your company name or any other text into the **Plesk title bar text** box.

You can use {product_name_version} and {plesk_key_id} variables to display product title (Plesk) with version number and key ID respectively.

3   To set your logo, specify the path to file in the **Choose new logo file** box, or click **Browse** to locate the file. Click **Open**.

4   To make the logo a clickable hyperlink that refers users to your corporate web site, type the desired URL into the **Enter new URL for logo** box.

5   Click **OK** to submit.

When you wish to restore the default Plesk logo, click **Default Logo**.

Adding and Removing Custom Hyperlink Buttons

> ➢ *To add a custom hyperlink button to your Plesk control panel and specify whether your customers will see it in their control panels:*

1 Go to **Server** > **Custom Buttons** and click **Add New Button**.

2 Specify properties of the button:

- Type the text that will show on your button in the **Button label** box.

- Choose the location for your button. To place it in the navigation pane, select the **Navigation pane** option from the **Location** drop-down box. To place it on each client's home page or desktop, select the **Client home page** option. To place it on each domain owner's home page or desktop (domain owners are your reseller's customers), select the **Domain administration page** option.

- Specify the priority of the button. Plesk will arrange your custom buttons on the control panel in accordance with the priority you define: the lower the number – the higher is priority. Buttons are placed in the left-to-right order.

- To use an image for a button background, type the path to its location or click **Browse** to browse for the desired file. It is recommended that you use a 16x16 pixels GIF or JPEG image for a button to be placed in the navigation pane, and 32x32 pixels GIF or JPEG image for buttons placed in the main frame or desktop.

- Type the hyperlink of your choice to be attached to the button into the **URL** box.

- Using the check boxes, specify whether to include the information, such as domain name, FTP login, FTP password and other data to be transferred within the URL. These data can be used for processing by external web applications.

- In the **Context help tip contents** input field, type in the help tip that will be displayed when you hover the mouse pointer over the button.

- Select the **Open URL in the Control Panel** check box if you wish the destination URL to be opened in the control panel's right frame, otherwise leave this check box unchecked to open the URL in a separate browser window.

- If you wish to make this button visible to your customers, your resellers and their customers with access to control panel, select the **Visible to all sub-logins** check box.

3 Click **OK** to complete creation.

> ➢ *To remove a hyperlink button from your Plesk control panel:*

1 Go to **Server** > **Custom Buttons**.

2 Select a check box corresponding to the button that you wish to remove and click ✖ **Remove Selected**.

Customizing the Control Panel in the Desktop View

➢ *To add or remove items from the desktop:*

1   Go to **Desktop** > 🔧 **Customize Desktop**.

2   Specify whether to show the **Server Information** group and what items to show there. Clearing check boxes will remove the respective items from the desktop.

3   Specify what tasks you would like to accomplish through the control panel. The appropriate shortcuts will be placed to the desktop. The **Selected tasks** list shows the tasks for which shortcuts are already placed on the desktop. The **Available tasks** list shows the tasks for which you do not yet have shortcuts on your desktop.

   ▪ To add a shortcut to the desktop, select the required tasks in the **Available tasks** list and click **Add >>**.

   ▪ To remove a shortcut from the desktop, select the task that you do not need in the **Selected tasks** list and click **<< Remove**.

4   To show your custom buttons on the desktop, under **Tools**, select the **Custom buttons** check box.

5   Specify whether to show the **Statistics** and **Favorites** group and what items to show there. Clearing check boxes will remove the respective items from the desktop.

   The **Favorites** group shows the links to items or control panel screens that you added to desktop by navigating to the respective control panel screens and clicking ⭐ **Add To Favorites** or 🔷 **Create Shortcut** icon.

6   Click **OK**.

➢ *To add items to the Favorites group of the desktop:*

1   Navigate to the control panel screen you need.

2   Click either the ⭐ **Add To Favorites** or 🔷 **Create Shortcut** icon in the upper right corner of the screen.

3   If you want to specify a custom label and description for the shortcut, clear the **Use default** check boxes and specify the desired label and description, then click **OK**.

➢ *To modify label or description for a shortcut in the Favorites group:*

1   On the desktop, click the shortcut that you wish to modify.

2   Click the 🖊 **Edit Favorite** or 🖊 **Edit Shortcut** icon in the upper right corner of the screen.

3   Modify the label and description as desired and click **OK**.

   OR

1 On the desktop, click the 🖊 icon corresponding to the shortcut that you wish to modify.

2 Modify the label and description as desired and click **OK**.

➢

➢ ***To remove items from the*** *Favorites* ***group of the desktop:***

1 On the desktop, click the shortcut that you wish to remove.

2 Click the 🖊 **Edit Favorite** or 🖊 **Edit Shortcut** icon in the upper right corner of the screen, then click **Remove**.

OR

1 On the desktop, click the 🖊 icon corresponding to the shortcut that you wish to remove, then click **Remove**.

In this section:

Using Desktop Presets

Alternately, you can modify items in the desktop view by modifying and applying desktop presets. The presets contain configurations of interface elements. You can have several presets for your interface and switch between them when needed. You can predefine the appearance of interface for your customers and customers of your resellers.

➢ *To customize your desktop by means of a template:*

1 Go to **Server** > **Interface Management** > **Desktop Presets** tab and click the **Default Administrator Desktop** shortcut in the list of desktop presets.

   If you wish to create a new preset based on an existing one, click the corresponding 🔧 icon.

2 Specify the configuration preset name.

3 Select the **Default** check box to apply this preset to the interface.

4 Specify whether to show the **Server Information** group and what items to show there. Clearing check boxes will remove the respective items from the desktop.

5 Specify what tasks you would like to accomplish through the control panel. The appropriate shortcuts will be placed to the desktop. The **Selected tasks** list shows the tasks for which shortcuts are already placed on the desktop. The **Available tasks** list shows the tasks for which you do not yet have shortcuts on your desktop.

   ▪ To add a shortcut to the desktop, select the required tasks in the **Available tasks** list and click **Add >>**.

   ▪ To remove a shortcut from the desktop, select the task that you do not need in the **Selected tasks** list and click **<< Remove**.

6 To show your custom buttons on the desktop, select the **Custom buttons** check box located above the list of **Available tasks**.

7 To show on the desktop a shortcut to functions for creating new custom hyperlink buttons, select the **Show the following buttons in the footer: Create a new custom button** check box below the **Available tasks** list.

8 Specify whether to show the **Statistics** and **Favorites** groups and what items to show there. Clearing check boxes will remove the respective items from the desktop. The **Favorites** group shows the links to items or control panel screens that you added to desktop by navigating to the respective control panel screens and clicking ⭐ **Add To Favorites** or 🔧 **Create Shortcut**.

9 Click **OK**.

➢ *To customize desktop for your resellers and customers who have several domains (client accounts):*

1   Go to **Server** > **Interface Management** > **Desktop Presets** tab and click the **Default Client Desktop** shortcut in the list of desktop presets.

If you wish to create a new preset based on an existing one, click the corresponding icon.

2   Specify the configuration preset name.

3   Select the **Default** check box to apply this preset to the interface.

4   Specify what tasks you would like your users to accomplish through the control panel. The appropriate shortcuts will be placed to the desktop. The **Selected tasks** list shows the tasks for which shortcuts are already placed on the desktop. The **Available tasks** list shows the tasks for which there are no shortcuts on the desktop.

  ▪   To add a shortcut to the desktop, select the required tasks in the **Available tasks** list and click **Add >>**.

  ▪   To remove a shortcut from the desktop, select the task that you do not need in the **Selected tasks** list and click **<< Remove**.

5   To show custom buttons on the desktop, select the **Custom buttons** check box located above the list of **Available tasks**.

6   To show on the desktop a shortcut to functions for creating new custom hyperlink buttons, select the **Show the following buttons in the footer: Create a new custom button** check box below the **Available tasks** list.

7   Specify whether to show the **Statistics and Favorites** group and what items to show there. Clearing check boxes will remove the respective items from the desktop.

The **Favorites** group shows the links to items or control panel screens that your users add to their desktops by navigating to the respective control panel screens and clicking the clicking ⭐ **Add To Favorites** or 🔷 **Create Shortcut**.

8   Click **OK**.

➢ *To customize desktop for your resellers' customers (domain owner accounts):*

1   Go to **Server** > **Interface Management** > **Desktop Presets** tab and click the **Default Domain Owner Desktop** shortcut in the list of desktop presets.

If you wish to create a new preset based on an existing one, click the corresponding icon.

2   Specify the configuration preset name.

3   Select the **Default** check box to apply this preset to the interface.

4   Specify what tasks you would like users to accomplish through the control panel. The appropriate shortcuts will be placed to the desktop. The **Selected tasks** list shows the tasks for which shortcuts are already placed on the desktop. The **Available tasks** list shows the tasks for which there are no shortcuts on the desktop.

  ▪   To add a shortcut to the desktop, select the required tasks in the **Available tasks** list and click **Add >>**.

- To remove a shortcut from the desktop, select the task that you do not need in the **Selected tasks** list and click **<< Remove**.

5 To show custom buttons on the desktop, select the **Custom buttons** check box located above the list of **Available tasks**.

6 To show on the desktop a shortcut to functions for creating new custom hyperlink buttons, select the **Show the following buttons in the footer: Create a new custom button** check box below the **Available tasks** list.

7 Specify whether to show the **Statistics and Favorites** group and what items to show there. Clearing check boxes will remove the respective items from the desktop.

The **Favorites** group shows the links to items or control panel screens that users add to their desktops by navigating to the respective control panel screens and clicking ⭐ **Add To Favorites** or 🔁 **Create Shortcut**.

8 Click **OK**.

➢ *To download a configuration preset in XML format:*

1 Go to **Server** > **Interface Management** > **Desktop Presets** tab.

2 Select the check boxes corresponding to the presets that you wish to download and click 💾 **Export selected to file**.

3 When prompted, specify file name and location where to save file and click **OK**.

➢ *To upload a configuration preset in XML format:*

1 Go to **Server** > **Interface Management** > **Desktop Presets** tab and click **Upload**.

2 Specify the path to preset file or click **Browse** to locate it.

3 Select the **Overwrite presets with the same name and type** check box if you wish to avoid errors on overwriting presets already registered in the control panel, then click **OK**.

4 To apply the preset, click its title, select the **Default** check box and click **OK**.

➢ *To remove a preset:*

1 Go to **Server** > **Interface Management** > **Desktop Presets** tab.

2 Select the check box corresponding to the preset that you wish to remove and click ❌ **Remove Selected**. Confirm removal and click **OK**.

Adjusting Session Preferences

You can adjust the allowed idle time for any session in Plesk as required.

➢ *To adjust session security parameters:*

1 Go to **Sessions** > **Preferences**.

2 Specify the required **Session idle time** in minutes in the appropriate field. Should a user session remain idle for the time period exceeding the one specified as the **Session idle time**, the Control Panel terminates this session.

3 Click **OK**.

➢ *To allow IP changes during one client session:*

1 Go to **Sessions** > **Preferences**.

2 Select the **Allow IP changes during one session** check box. This option will allow customers with dynamic IPs and unstable internet connection to work with Plesk at the cost of increasing the security risks.

3 Click **OK**.

➢ *To reset all parameters back to their default values:*

1 Go to **Sessions** > **Preferences** and click **Default**. The default session idle time will be set to 30 minutes.

2 Click **OK**.

Configuring and Maintaining Your Server

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

In this chapter:

Adding and Removing IP Addresses

After installation, Plesk reads all your IP addresses from the network configuration files and can then use these IP addresses for hosting DNS domains and Web sites.

When you obtain a new IP address that you would like to use on the server, you should add the address through the control panel, as Plesk might not recognize manual modifications you make to the network configuration files.

With Plesk you can mark all your IP addresses as shared or dedicated *before* you assign them to your customers. This allows the control panel to distinguish between them and not to let you assign a dedicated IP address to several customers at once. A dedicated IP address can be assigned to a single customer, while a shared IP address can be shared among several user accounts.

Note that SSL protection with authentic digital certificates and Anonymous FTP services are available only to dedicated hosting accounts on a dedicated IP address. Shared hosting accounts can also have SSL protection, but visitors to such protected sites will get error messages in their browsers.

Note: in this version of Plesk control panel, dedicated IP addresses are referred to as Exclusive IP addresses.

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

1 Go to **Server** > **IP Addresses**.

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

- An icon in the **S** (Status) column shows ✅ if your IP address is properly configured on the network interface. If your IP address was removed from the network interface, an icon will show 🛑.

- An icon in the **T** (Type) column shows 👑 if an address was allocated to a single customer as a dedicated IP address, and 🖥 if an address is shared among many customers.

- The **IP address**, **Subnet Mask** and **Interface** columns show which IP addresses are on which network interfaces.

- The **Clients** column shows the number of user accounts who you assigned a given IP address. To view the users by names, click the respective number in the **Clients** column.

- The **Hosting** column shows a number of web sites hosted on an IP address. To view the domain names of these web sites, click the respective number in the **Hosting** column.

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

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

1 Go to **Server** > **IP Addresses** and click **Add New IP Address**.

2 Select the network interface for the new IP from the **Interface** drop-down box. All network cards installed on your server are shown in this drop-down box.

3 Enter the IP address and subnet mask in the corresponding box (e.g., 123.123.123.123/16).

4 Select the type of the new IP address, shared or exclusive, using the **IP type** radio button.

5 From the drop-down box, select the SSL certificate for the new IP address. You can select the following certificates:

   ▪ **Default certificate** - the certificate that comes with the Plesk distribution package. However, this certificate is not recognized by web browsers as it is not signed by a Certificate Authority (a warning message appears). The default certificate is used to provide access to the control panel via the https protocol (https://<Plesk Server name or IP>:8443/).

   ▪ **Other certificates** - the certificates (self-signed or signed by a Certificate Authority) that you added to the repository of SSL certificates (about adding certificates, see the Securing Sites with SSL encryption section).

6 Select the **FTP over SSL** check box if you want to enable the ability to use secure FTP connection (FTP over SSL) for the domain on an exclusive IP address.

Note. To enable secure FTP connection, the FTP server installed on your Plesk server must support FTP over SSL.Currently, only Gene6 and Serv-U FTP servers support FTP over SSL.

---

7 Click **OK**.

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

1 Go to **Server** > **IP Addresses**.

2 Select the respective check box and click ✖ **Remove Selected**, confirm removal and click **OK**.

➢ *To assign an IP address to a user:*

1 Go to **Server** > **IP Addresses** and click the respective number in the **Clients** column, then click **Add New Client**.

2 Select the user account you need and click **OK**.

➢ *To revoke an IP address from a user:*

1 Go to **Server** > **IP Addresses** and click the respective number in the **Clients** column.

2 Select the respective check box and click ✖ **Remove Selected**.

3 Confirm removal and click **OK**.

➢ *To specify what web site will open when users refer to the web resource on your server by an IP address:*

1 Go to **Server** > **IP Addresses** and click the respective number in the **Hosting** column. All sites hosted on this IP will be listed.

2 Select the site you need and click ⭐ **Set as Default**.

➢ *To change an IP address allocation type (shared, exclusive) or assign another SSL certificate to an IP address:*

1 Go to **Server** > **IP Addresses** and click the IP address you need.

2 Select the IP address allocation type and SSL certificate you need, and click **OK**.

➢ *To switch on the ability to use secure FTP connection (FTP over SSL) for the domain:*

1 Go to **Server** > **IP Addresses** and click the required IP address you need.

2 Select the **Allow FTP over SSL** check box and click **OK**. It is recommended to use exclusive IP addresses for this feature to work properly.

Configuring Software Components Used by Plesk

Plesk supports a variety of third-party software components, from antiviruses to web mail servers. It is possible to choose what components should be used by Plesk.

➢ *To see the list of available components and to select the software components that should be used by Plesk:*

1 Go to **Server** > **Components Management**.

All available components are displayed in the list. The current state of a component is marked by an icon:

- means that Plesk is using this component, and the component is working.

- means that Plesk is not using this component (usually because a license key has expired or missing), but the component is working.

- means that Plesk is not using this component, because the component is stopped.

- means that Plesk is not using this component, but the component is installed in the system and available.

2 Click the component name (for example, **Mail Server**) and select the required component from the list of available components supported by Plesk.

3 Click **OK**. Plesk will start the selected component.

Some components (for example, Merak Mail Server) can be configured by clicking their name in the **Component version** table. Individual component settings depend on the component. After finishing the configuration of a component, click **OK**.

To refresh the list of available components, click **Refresh**.

Configuring DNS Services

Your control panel works in cooperation with a DNS server, which enables you to run DNS service on the same machine where you host Web sites.

Setup of DNS zones for newly added domains is automated: When you add a new domain name to control panel, a zone file is automatically generated for it in accordance with the server-wide DNS zone template and registered in the name server's database, and name server is instructed to act as a primary (master) DNS server for the zone.

You can:

- Add resource records to and remove from the template,

- Override the automatic zone configuration with custom settings on a per-domain basis,

- Select another DNS server (for example, switch to Microsoft DNS server from BIND DNS server),

- Switch off the domain name service on this machine altogether, if your provider or another organization is running centralized DNS service (for example, if your Plesk is using Plesk Expand DNS server).

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

1 Go to **Server** > **DNS Settings**. All resource record templates will be displayed.

The <ip> and <domain> templates are automatically replaced in the generated zone with real IP addresses and domain names.

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

1 Go to **Server** > **DNS Settings**.

2 Click **Add New DNS Record** in the **Tools** group.

3 Select the resource record type and specify the record properties as desired.

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

4 Click **OK**.

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

1 Go to **Server** > **DNS Settings**.

2 Select a check box corresponding to the record template you wish to remove, and click ✖ **Remove Selected**.

3 Confirm removal and click **OK**.

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

1 Go to **Server** > **DNS Settings**.

2 Click **Restore Defaults** in the **Tools** group

3 Confirm the restoration of the DNS template zone and click **OK**.

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

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

1 Go to **Server** > **DNS Settings**.

2 Click **SOA Records Template**.

3 Specify the desired values:

- **Refresh Interval**. This is how often the secondary name servers check with the primary name server to see if any changes have been made to the domain's zone file. Plesk sets the default value of three hours.

- **Retry Interval**. This is the time a secondary server waits before retrying a failed zone transfer. This time is typically less than the refresh interval. Plesk sets the default value of one hour.

- **Expire Interval**. This is the time before a secondary server stops responding to queries, after a lapsed refresh interval where the zone was not refreshed or updated. Plesk sets the default value of one week.

- **Minimum TTL**. This is the time a secondary server should cache a negative response. Plesk sets the default value of one day.

- **Default TTL**. This is the amount of time that other DNS servers should store the record in a cache. Plesk sets the default value of one day.

4 Click **OK**. The new SOA record parameters will be set for the newly created domains.

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

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

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

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

1 Go to **Server** > **DNS Settings**.

2 Click **SOA Records Template**.

3 Select the **Use serial number format recommended by IETF and RIPE** check box.

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

4 Click **OK**.

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

1 Go to **Server** > **DNS settings**.

2 Click **SOA Records Template**.

3 Clear the **Use serial number format recommended by IETF and RIPE** check box.

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

4 Click **OK**.

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

1 Go to **Server** > **DNS Settings**.

2 Select **Transfer Restrictions Template** tab. A screen will show all hosts to which DNS zone transfers for all zones are allowed.

▪ To add a network to ACL, specify the IP address and mask in the **IP address/mask** field and click **Add Network**.

▪ To delete a network from ACL, select the checkbox corresponding to the required network in the list, click ✖ **Remove Selected**, confirm the removal and click **OK**.

You can adjust the server-wide DNS recursion settings in Plesk.

1 Click the **Server** shortcut in the navigation pane.

2 Click **DNS Settings** in the **Services** group.

3 Select **DNS Recursion** tab.

▪ To allow recursion for all requests, select **Allow for all requests**.

▪ To allow recurson only for local requests, select **Allow for local requests only**. For example, the **Allow for local requests only** option can be helpful if you wish to avoid the usage of DNS server resources by spammers, this option is set by default in Plesk.

▪ Select **Deny** to switch off the recursion.

4 Click **OK**.

If you are using third-party DNS servers (for example, if your control panel is using Plesk Expand DNS server), and are not running your own DNS server, you should switch off your control panel's DNS server.

➢ *To switch off your control panel's DNS server:*

1 Go to **Server** > **DNS Settings**.

2   Click **DNS server**.

3   Select the **DNS server is switched off** option and click **OK**.

Configuring Plesk to Operate Behind a Firewall

This chapters describes how to configure Plesk for operating behind a standalone firewall you might use, or a firewall running on the Plesk server and manageable through the Plesk control panel.

In this section:

Configuring Plesk for Operating Behind a Standalone Firewall

If you want to run Plesk behind a standalone firewall, you might encounter certain problems with resolution of domain names served by Plesk: when you set up a new DNS domain in Plesk, its zone file includes a resource record that associates the domain name with the IP address your Plesk server is on, i.e. an internal network address like 192.168.1.1. As the 192.168.x.x IP addresses are reserved by the Internet Assigned Numbers Authority (IANA) for use by private networks, this domain name will not be accessible to the Internet users. To work around this, you would have to associate this domain name with the IP address of the firewall machine in the domain's zone file (**Domains** > **domain name** > **DNS**).

We recommend using the DNS zone template (**Server** > **DNS**) to automate association of the newly added domain names with appropriate IP addresses.

Let's consider setting up a Plesk server running on 192.168.1.1 in a private network protected by a firewall, which is running on 11.22.33.44:

1   Go to **Server** > **DNS Settings**.

2   Locate all resource records of A type. As you cannot edit any of these records, you should delete them and then create the new records: be sure to leave the values in the **Name** column unchanged for each A record, but replace the <ip> templates in the **Value** column with the IP address of your firewall host – 11.22.33.44.

3   Configure your firewall so as to ensure the proper address translation.

Setting Up Plesk's Firewall

Plesk control panel comes with a firewall, which you can use to protect your server from incoming network connections that could be used to compromise the server. The firewall comes with a set of predefined rules that allow connections to the services required for the proper functioning of a hosting server, such as Web, mail, and FTP. By default, the firewall is switched off.

Read this chapter to learn how to:

- Switch on the firewall
- View the currently allowed inbound connections
- Allow and block inbound connections
- Allow and block ICMP communications
- Restore the default configuration of the firewall
- Switch off the firewall

In this section:

Switching the Firewall On

> ➢ *To switch on the firewall:*

1 Go to **Server** > **IP Addresses** > **Firewall**.

2 Under **Tools**, click **Switch On**.

3 To switch on the firewall for a specific network interface, if you have a number of network interfaces, in the list of interfaces, click the interface name you need.

The list of applied filtering policies (rules) opens. The **S** (status) column shows the ⊗ icon if the firewall blocks the packets that match the rule, and the ✓ icon if the firewall allows the packets that match the rule to pass through.

Note. Configuring firewall for specific network interfaces is only available under Microsoft Windows Server 2003.

Viewing the Currently Allowed Inbound Connections

By default, all inbound connections that are not explicitly allowed are blocked.

> ➢ *To view the currently applied firewall rules for inbound connections:*

1 Go to **Server** > **IP Addresses** > **Firewall**.

2 Click the network interface you need.

All currently defined rules are listed. The **S** (status) column shows the ⊗ icon if the firewall blocks the packets that match the rule, and the ✓ icon if the firewall allows the packets that match the rule to pass through.

Note. Configuring firewall for specific network interfaces is only available under Microsoft Windows Server 2003. If you are using Microsoft Windows Server 2008, go to the **Firewall Rules** tab.

3 Do any of the following:

- To view or change the properties of a rule, click the respective rule's name. To save any changes you have made to the rule, click **OK**. To return to the previous screen without saving any changes, click **Cancel** or click **Up Level**.

- To allow connections to a service, click **Add Firewall Rule**, specify the rule name for future reference, specify the port and the protocol for which incoming connections must be allowed. Leave the **Switch on rule** check box selected, if you wish to apply the rule immediately. Click **OK**.

- To allow connections to a service that you previously made inaccessible, click the respective ⊗ icon in the **S** column.

- To temporarily block connections to a service, click the respective ✓ icon in the **S** column.

- To permanently block connections to a service, select the check box corresponding to the rule that allows connections to the respective service, and click **Remove Selected**. Removing a rule blocks the connections that were specified in that rule.

Allowing and Blocking Inbound Connections

By default, all inbound connections that are not explicitly allowed are blocked.

➤ *To allow inbound connections to a service:*

1 Go to **Server** > **IP Addresses** > **Firewall**.

2 Click the network interface you need.

> **Note.** Configuring firewall for specific network interfaces is only available under Microsoft Windows Server 2003. If you are using Microsoft Windows Server 2008, go to the **Firewall Rules** tab.

3 Click **Add Firewall Rule**, and specify the following properties:
- The rule name for future reference
- The port or port range and the protocol for which inbound connections must be allowed

4 Leave the **Switch on rule** check box selected, if you wish to apply the rule immediately.

5 Click **OK**.

➤ *To block the previously allowed inbound connections to a service:*

1 Go to **Server** > **IP Addresses** > **Firewall**.

2 Click the network interface you need.

> **Note.** Configuring firewall for specific network interfaces is only available under Microsoft Windows Server 2003. If you are using Microsoft Windows Server 2008, go to the **Firewall Rules** tab.

3 Select the check box corresponding to the rule that allows connections to the respective service, and click **Remove Selected**.

Removing a rule blocks the connections that were specified in that rule.

Allowing and Blocking ICMP Communications

ICMP communications are used for network troubleshooting purposes. By default, all ICMP communications are allowed. For the detailed description of ICMP messages, please refer to:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/xpehelp/html/xeconconfiguringicmpsettingsinwindowsfirewall.asp

➢ *If you need to block or to allow ICMP communications, follow these steps:*

1 Go to **Server** > **IP Addresses** > **Firewall** > **ICMP Protocol**.

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

2 Do any of the following:

- To allow ICMP requests of a specific type, click the respective ⊗ icon in the **S** column.

- To block ICMP requests of a specific type, click the respective ✓ icon in the **S** column.

- To block all ICMP requests, click **Panic Mode**.

- To restore the default settings for ICMP requests, click **Default**.

Restoring the Default Configuration of the Firewall

➢ *To restore the initial configuration:*

1 Go to **Server** > **IP Addresses** > **Firewall**.

2 Click the network interface you need.

Note. Configuring firewall for specific network interfaces is only available under Microsoft Windows Server 2003. If you are using Microsoft Windows Server 2008, go to the **Firewall Rules** tab.

3 Under **Tools**, click **Default**.

Closing Down All Connections to the Server Using the Panic Mode

If your server is compromised and web sites defaced, you may want to make the server unavailable over the Internet and keep it down until all vulnerabilities are patched and customers' web sites are restored from backups.

➢ *To close all connections to the server:*

1 Go to **Server** > **IP Addresses** > **Firewall**.

2 Click **Panic Mode**.

Note. Configuring firewall for specific network interfaces is only available under Microsoft Windows Server 2003. If you are using Microsoft Windows Server 2008, go to the **Firewall Rules** tab.

Switching the Firewall Off

➢ *To switch off the firewall:*

1 Go to **Server** > **IP Addresses** > **Firewall.**

2 Under **Tools**, click **Switch Off**.

Configuring Mail Services

Your control panel works in cooperation with your mail server, which provides mail services for your domains. After installation the mail server is configured automatically and is ready to serve, however, we recommend that you review the default settings to make sure that they satisfy your needs:

1 Go to **Server** > **Mail**. The server-wide mail preferences screen will open on the **Preferences** tab.

2 If you wish to limit the size of an e-mail message that can be sent through your server, type the desired value in kilobytes into the **Maximum letter size** box, otherwise, leave this field blank.

3 If you wish to protect your users from dictionary attacks by not allowing them to use simple passwords, select the **Check the passwords for mailboxes in the dictionary** option.

A dictionary attack is when someone tries to find out a valid user name and password by running a program that tries different combinations of dictionary words in different languages. Dictionary attacks can be successful because many users choose their passwords carelessly.

> **Note.** In order for this option to work you need to make sure that the **Password must meet complexity requirements** option is switched on in your server's Local Security Policy settings (the option is located in **Start** > **Administrative Tools** > **Local Security Policy** > **Account Polices** > **Password policy**).

4 If you wish to use an additional SMTP port with mandatory authorization for e-mail message submission, select the **Switch on message submission** check box and choose the IP address on which the port will be working. Note that availability of this option depends on the mail server you're using.

5 Select the mail relay mode.

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

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

▪ **POP3 authorization.** With POP3 authorization, once a user has successfully authenticated to the POP server, he or she is permitted to receive and send e-mail through the mail server for the next 20 minutes (default value). You can adjust this interval by specifying another value in the **lock time** box.

▪ **SMTP authorization.** With SMTP authorization, your mail server requires authorization if the e-mail message must be sent to an external address.

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

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

6 Select the **Enable support for Trend Micro RBL+ Service** checkbox to enable the mail abuse prevention system to help you defend your customers from abuse by spammers, and enter the DNS zone name (e.g. domain.com) in the **MAPS zones** field. You can specify several MAPS zones separated by semicolons.

7 Click **OK** to submit any changes.

In this section:

Setting Up Spam Protection

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

- **SpamAssassin spam filter**. It is a powerful spam filter that uses a wide variety of local and network tests to identify spam signatures.

    You can configure the spam filter so as to either delete suspicious messages when they come to your mail server, or change the subject line and add "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers to the messages. The latter can be useful for users who prefer to filter mail with mail filtering programs installed on their own computers.

    To learn more about SpamAssassin, visit http://spamassassin.apache.org.

    To configure and switch on the SpamAssassin filter, proceed to the Setting Up SpamAssassin Spam Filter (on page 69) section.

- **DomainKeys**. DomainKeys is a spam protection system based on sender authentication. When an e-mail claims to originate from a certain domain, DomainKeys provides a mechanism by which the recipient system can credibly determine that the e-mail did in fact originate from a person or system authorized to send e-mail for that domain. If the sender verification fails, the recipient system discards such e-mail messages. To configure the DomainKeys system on your server, refer to the section Switching On Spam Protection Based on DomainKeys (on page 70).

- **DNS blackhole lists**. This spam prevention system is based on DNS queries made by your mail server to a database, which contains known and documented sources of spam, as well as an extensive listing of dynamic IP addresses. Any positive response from this database should result in your mail server returning a '550' error, or rejection of the requested connection.

    To configure your mail server for working with DNSBL databases, proceed to the Switching On Spam Protection Based on DNS Blackhole Lists (on page 72) section.

- **Server-wide black and white lists**. Black and white lists are standard mail server facilities. You can use the black list to specify the domains from which mail must not be accepted, and white list to specify the IP addresses of machines or networks from which mail must always be accepted.

    To set up server-wide black and white lists, proceed to the Setting Up Server-wide Black and White Lists (on page 72) section.

In this section:

Setting Up SpamAssassin Spam Filter

➢ *To switch on SpamAssassin spam filter:*

1 Click **Server** shortcut in the navigation pane.

2 Click **Mail** in the **Services** group.

3 Select **Spam Filtering** tab.

4 To allow server wide filtering based on the settings you define, select the **Use server-wide settings** check box.

5 To let your users set their own spam filtering preferences on a per-mailbox basis, select the **Allow personal settings** check box.

Now all the incoming mail will be filtered on the server side. By default, spam filter does not delete spam mail, it only adds the "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers to the message, and "*****SPAM*****" text string to the beginning of Subject line of each message recognized as spam.

If you have enabled the **Allow personal settings** option, then your users will be able to set their spam filters so as to automatically delete junk mail. They will also be able to set up their personal black and white lists of correspondents that will override the server settings, and teach the spam filter on a per-mailbox basis.

6 Adjust the spam filter sensitivity by specifying the desired value in the **Hits required for spam** box.

SpamAssassin performs a number of different tests on contents and subject line of each message. As a result, each message scores a number of points. The higher the number, the more likely a message is spam. For example, a message containing the text string "BUY VIAGRA AT LOW PRICE!!!" in Subject line and message body scores 8.3 points. By default, the filter sensitivity is set so that all messages that score 7 or more points are classified as spam.

- When your users receive lots of spam messages with the current setting, to make filter more sensitive, try setting a lesser value in the **Hits required for spam** box; for example, 6.

- When your users are missing e-mails because your spam filter thinks they are junk, try reducing filter sensitivity by setting a higher value in the **Hits required for spam** box.

- Testing large messages can slow down the mail server. To reduce the load, you can select the **Do not filter if mail size exceeds specified size** checkbox and specify the maximum size of the message that the spam filter will test. Recommended mail size limit is 150 - 250 Kbytes, which is usual for mail messages in HTML format with images. The size of the mail is considered critical for filter and server overload when it exceeds 500 Kbytes, which is usual for mail messages containing attachments.

- To avoid spam filter leaving some mail messages unchecked (this can happen if the amount of incoming mail is very large), limit the number of letters that can be checked simultaneously in the **Number of threads that spam filter can create** field.

7 Specify how to mark messages recognized as spam.

At the server level, you cannot set the server-wide spam filter to automatically delete spam: you can do it only on a per-mailbox basis. So, for the server-wide policy, you can choose only marking messages as spam: "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers are added to the message source by default, and if you want, the spam filter will additionally include a specific text string to the beginning of Subject line. To include a desired combination of symbols to the message subject, type it into the **by tag** box. If you do not want the spam filter to modify message subject, clear the **Modify spam mail subject** check box. If required, specify the spam detection alert text in the appropriate field.

8 Define the language characteristics of mail that should always pass the filter by specifying trusted languages and locales.

   ▪ Select the required items from the boxes under **Trusted languages** and **Trusted locales** and click **Add >>**.

   ▪ Letters written in the specified languages and with the defined character sets will not be marked as spam.

9 Once finished with setting up SpamAssassin spam filter, click **Up Level** to return to the previous screen.

If you wish to adjust spam filtering settings for a specific mailbox, proceed to the Protecting Mailboxes from Spam (on page 221) section.

Switching On Spam Protection Based on DomainKeys

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

1 Go to **Server** > **Mail** > **Spam Filtering** tab.

2 Under the **DomainKeys spam protection** group, select the following options:

   ▪ **Allow signing outgoing mail.** Selecting this option allows you and your customers to switch on support for DomainKeys e-mail signing on a per-domain basis through the domain administration screens of the control panel (**Domains > *domain name* > Mail > Preferences > Use DomainKeys spam protection system to sign outgoing e-mail messages** option). It does not automatically switch on signing of outgoing e-mail messages.

   ▪ **Verify incoming mail**. Selecting this option will configure the DomainKeys system to check all e-mail messages coming to e-mail users under all domains hosted on the server.

3 Click **OK**.

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

➢ *To switch on signing outgoing e-mail messages for a single domain:*

1 Go to **Domains > *domain name* > Mail > Preferences.**

2 Select the **Use DomainKeys spam protection system to sign outgoing e-mail messages** check box.

3 Click **OK**.

➤ *To switch on signing outgoing e-mail messages for a number of domains at once:*

1 Click **Domains**.

2 Select the check boxes to the left of the domain names you need. To select all domains in the list, select the upper left check box in the column heading.

3 Click **Group Operations**.

4 Under **Preferences**, select the **Switch on** option next to the **Use DomainKeys spam protection system to sign outgoing e-mail messages** field.

5 Click **OK**.

Now, the following will happen for the selected domains:

▪ Private keys are generated and placed in the server's database.

▪ Public keys are generated and placed in the TXT resource records created in the domains' DNS zones.

▪ The sender's policy advertised in the DNS TXT resource records is set to "all e-mail messages sent from this domain must be cryptographically signed; if someone receives an e-mail message claiming to originate from this domain, which is not signed, then this e-mail must be discarded."

▪ Outgoing e-mail messages are digitally signed: the "DomainKeys-Signature" header containing a signature based on a private key is added to the message headers.

Switching On Spam Protection Based on DNS Blackhole Lists

You can use free and paid subscription blackhole lists with your server. Visit http://spamlinks.net/filter-dnsbl-lists.htm and choose a DNSBL server you want to use.

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

1   Click the **Server** shortcut in the navigation pane.

2   Click the **Mail** icon in the **Services** group.

3   Select the **Switch on spam protection based on DNS blackhole lists** check box.

4   In the **DNS zones for DNSBL service** input box, specify the host name that your mail server should query, for example: sbl.spamhaus.org.

5   Click **OK**.

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

Setting Up Server-wide Black and White Lists

➢ *To block mail from specific domains:*

1   Click the **Server** shortcut in the navigation pane.

2   Click **Mail** in the **Services** group.

3   Click the **Black List** tab.

4   To add an entry to the black list, click **Add Domain**, and specify domain name in the **Domain name** field.

5   Click **OK**.

6   Repeat steps 4 and 5 to add as many domains as required.

➢ *To allow mail reception from specific domains or networks:*

1   Click the **Server** shortcut in the navigation pane.

2   Click **Mail** in the **Services** group.

3   Click the **White List** tab.

4   To add an entry to the white list, click **Add Network**, specify network IP and mask into the **IP address/mask** field.

5   Click **OK**.

6   Repeat steps 4 and 5 to add as many networks as required.

➢ *To remove entries from black or white list:*

1   Click the **Server** shortcut in the navigation pane.

2   Click **Mail** in the **Services** group.

3   Click the required tab (**Black List** or **White List**).

4   Select the checkboxes corresponding to the entries you wish to remove and click ✖ **Remove Selected**.

5   Confirm the removal and click **OK**.

Setting Up Virus Protection

To protect your users from viruses and other malicious software that spreads itself through e-mail, you may want to switch on antivirus service that comes with your control panel.

➢   *To set up and switch on antivirus for all users' mailboxes:*

1   Go to **Server** > **Mail** > **Antivirus**.

2   Select the desired scanning mode.

3   To allow users to adjust scanning settings for incoming and outgoing mail, select the respective check boxes.

4   Click OK.

> The antivirus is now switched on. It will scan mail and delete all infected messages.

Configuring Plesk for Database Hosting

You can host users' databases either on a single server or on a number of different servers. Having the user databases on a remote server can be useful in multi-server installations, where centralized database hosting can be preferable for administration, backup, and resource utilization. However, if you have a single Plesk server, you are advised to keep all databases on it.

➢   *To use remote database servers with your hosting machine, you need to:*

1   Set up a remote database server:

1.   Install MySQL or Microsoft SQL software.

2.   Set up database administrator's account.

3.   Enable network access to the database server.

2   Configure Plesk for working with your remote database server.

In this section:

Setting Up Remote Database Hosting

After you have set up the required remote database server, you need to register this database server in Plesk.

➢ *To register a database server with Plesk:*

1   Log in to Plesk.

2   Go to **Server** > **Database Servers** and click **Add Database Server**.

3   Specify the properties of the database server:

- Specify database server engine in the **Database server type** menu.

- Specify hostname or IP address of the database server.

- Specify the port number the database server is listening on. This option is available only for MySQL. By default, MySQL servers listen on port 3306. You can leave the **Port number** box blank, if your MySQL database server is listening on the default port.

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

- Specify which database type is running on the database server.

- To make this database server default for hosting customers' databases, select the **Use this server as default for MySQL** check box. If you have a MS SQL database server, select the check box **Use this server as default for MS SQL** labeled.

- Specify the database server administrator's login name and password.

4   Click **OK**.

➢ *To set up database hosting preferences that will affect all databases created through Plesk:*

1   Go to **Server** > **Database Servers** > **Preferences**.

2   To simplify maintenance of customers' databases, select the **Add client's login name and underscore to beginning of database names** check box. All names of newly created databases will look like client's login name_database name. This will allow you to locate databases related to a particular Plesk user. Note that even if you do not select this check box, on creation of a new database, Plesk will add client's login name to the database name input box, and you will be able to edit it or remove it.

3   You can also set up Plesk to add client's login names to corresponding database user names, further simplifying the maintenance of customers' databases. To do so, select the **Add client's login name and underscore to the beginning of database user names** check box. All names of newly created database users will look like client's login name_database user name. This will allow you to locate database users related to a particular Plesk user.

4 Specify whether creation of databases is allowed on your Plesk
server. Some applications do not support remote databases and can
work only with databases hosted on the same server. We recommend
leaving the default option **Allow local hosting of databases for these site
applications** selected, otherwise, you will not be able to use such
applications.

5 Click **OK**.

> If you want to back up databases hosted on a remote MS SQL Database Server
> you set up earlier, you need to configure the backup settings for that MS SQL
> Database Server.

➢ *To configure backup settings for remote MS SQL Database Server:*

1 Go to **Server** > **Database Servers** and click the required remote MS SQL
Database Server name.

2 Specify the temporary directory for remote MS SQL Database Server
in the **Temporary network directory** field.

This directory can be located anywhere in your network and it is required for
backing up and restoring MS SQL databases. This directory must be accessible
over the network by both the Plesk server and the MS SQL server: both Plesk and
the user that is running remote MS SQL Database Server must have read/write
access to this directory.

3 Provide username and password required for accessing the temporary
network directory.

4 Click **OK**.

Managing Database Servers

➢ *To manage a database server:*

1 Go to **Server** > **Database Servers**.

2 Click the icon corresponding to the database server you need. A web interface of a database management tool will open in a separate browser window.

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

1 Go to **Server** > **Database Servers**.

2 Click the host name of a database server.

3 Click **Change Password**.

4 Type the new password and click **OK**.

➢ *To unregister a database server from Plesk:*

1 Click the **Server** shortcut in the navigation pane.

2 Click the **Database Servers** icon in the **Services** group.

3 Select the check box to the right of the database server's host name.

4 Click ✖ **Remove Selected**.

5 Confirm the operation and click **OK**.

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

1 Delete databases from the database server:

1. Click the **Server** shortcut in the navigation pane.

2. Click the **Database Servers** icon in the **Services** group.

3. Click the host name of a database server that you wish to unregister from Plesk.

4. Select the checkbox in the upper-right corner of the list to select all databases.

5. Click ✖ **Remove Selected**.

6. Confirm removal and click **OK**.

2 Make another database server default:

1. Click the **Database servers** shortcut in the path bar at the top of the screen.

    2. Click the host name of a database server that you wish to make default. This should be the same database server type (MySQL or MS SQL) as the one you are going to delete.

    3. Click Preferences and Select the **Use this server as default for MySQL** check box. If you have a MS SQL database server, select the **Use this server as default for PostgreSQL** check box.

    4. Click **OK**.

3 Return to the list of database servers (**Server** > **Database Servers**).

4 Select a check box corresponding to the database server that you no longer need.

5 Click ✖ **Remove Selected**.

6 Confirm the operation and click **OK**.

Important: You cannot remove site applications' databases this way. To remove them, you should uninstall the respective site applications from the domains that use them.

For instructions on managing databases, refer to the Deploying Databases (on page 155) section of this guide.

Configuring the Connection to External Database Management Systems

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

In this section:

Creating New Connections to External Databases

To let web applications of your clients use external databases for storing the data, you need to create connections to these external databases by installing appropriate ODBC drivers.

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

1 Go to **Server** > **ODBC Data Sources**.

2 Click **Add New ODBC DSN**.

3 Specify the ODBC connection name and description in the corresponding fields.

4 Select the required driver in the **Driver** field.

5 Click **OK**.

6 Choose the appropriate options on the driver configuration screen. Typically, you should specify the path to the database, user credentials and other connection options, depending on the selected driver.

Click **Test** to check whether the connection will function properly with provided settings. Click **Finish** to complete the creation.

Changing Settings Of Existing ODBC Connections

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

1 Go to **Server** > **ODBC Data Sources**.

2 Click the required connection name in the list.

3 Change the settings as needed.

4 Click **Test** to check whether the connection will function properly with new settings. Click **Finish** to save changes.

Removing Connections to External Databases

➢ *To remove a redundant ODBC connection:*

1 Go to **Server** > **ODBC Data Sources**.

2 Select the checkbox corresponding to a connection you want to remove.

3 Click ✖ **Remove Selected**, confirm the removal and click **OK**.

Enabling Support for Miva E-commerce Applications

To allow your customers use Miva e-commerce solutions, you need to install the Miva Empresa package on your server and enable support for Miva applications for the respective hosting accounts. Note that your customers will need to obtain a license from Miva and specify its serial number during the installation of Miva applications.

➢ *To install the support for Miva E-commerce applications on your server:*

1   Download and install the Miva Empresa package from Miva web site on your server. The installation instructions can be found here: http://docs.smallbusiness.miva.com/en-US/merchant/WebHost/webhelp/web_host_resources.htm

2   Run Plesk Reconfigurator and run the **Correct disk permissions** task.

➢ *To enable support for Miva applications for all newly created hosting accounts using domain templates:*

1   Go to **Domains** > **Domain Templates** and click the template name you need.

2   Select the **Miva support** check box and click **OK**.

➢ *To enable support for Miva applications for existing hosting accounts:*

1   Go to **Domains**, select the check boxes corresponding to the domain names you need, then click **Group Operations**.

2   Under the **Hosting** group, select the **Switched on** option to the left of the **Miva support** field.

3   Click **OK**.

➢ *To enable support for Miva applications for an individual hosting account:*

1   Go to **Domains** > **domain name** > **Setup**.

2   Select the **Miva support** check box and click **OK**.

After Miva support is enabled for an individual hosting account, the hosting owner can install and use the required Miva applications. The installation instructions for Miva applications can be found here: http://docs.smallbusiness.miva.com/en-US/merchant/WebHost/webhelp/web_host_resources.htm

To learn more about Miva solutions, refer to http://smallbusiness.miva.com/

Configuring ASP.NET

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

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

1 Go to **Server** > **ASP.NET**. The settings for ASP.NET 1.1.x and ASP.NET 2.0.x are located under the corresponding tabs.

2 Set up the strings that determine database connection data for ASP.NET applications which use databases. This option is available only for ASP.NET 2.0.x.

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

- To add a string, enter the required data into the **Name** and **Connection Parameters** input fields and click ⊕ next to them.

- To remove a string, click ⊖ next to it.

3 Set up custom error messages that will be returned by ASP.NET applications in the **Custom Error Settings** field:

- To set the custom error messages mode, select an appropriate option from the **Custom error mode** menu:

  - **On** - custom error messages are enabled.

  - **Off** - custom error messages are disabled and detailed errors are to be shown.

  - **RemoteOnly** - custom error messages are displayed only to remote clients, and ASP.NET errors are shown to the local host.

- To add a new custom error message (which will be applied unless the **Off** mode was selected), enter the values in the **Status Code** and **Redirect URL** fields, and click ⊕.

  - **Status Code** defines the HTTP status code resulting in redirection to the error page.

  - **Redirect URL** defines the web address of the error page presenting information about the error to the client.

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

- To remove a custom error message from the list, click ⊖ next to it.

4 Configure compilation settings in the **Compilation and Debugging** field:

- To determine the programming language to be used as default in dynamic compilation files, choose an entry from **Page default language** list.

- To enable compiling retail binaries, leave the **Enable debugging** checkbox empty.

- To enable compiling debug binaries, select the **Enable debugging** checkbox. In this case, the source code fragments containing error will be shown in a diagnostic page message.

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

5 Configure encoding settings for ASP.NET applications in the **Globalization Settings** section:

- To set an adopted encoding of all incoming requests, enter an encoding value into the **Request encoding** field (default is utf-8).

- To set an adopted encoding of all responses, enter an encoding value into the **Response encoding** field (default is utf-8).

- To set an encoding which must be used by default for parsing of `.aspx`, `.asmx`, and `.asax` files, enter an encoding value into the **File encoding** field (default is Windows-1252).

- To set a culture which must be used by default for processing incoming web requests, select an appropriate item from the **Culture** list.

- To set a culture which must be used by default when processing searches for a locale-dependent resource, select an appropriate item from the **UI Culture** list.

6 Set a code access security trust level for ASP.NET applications in the **Code Access Security** field.

CAS trust level is a security zone to which applications execution is assigned, defining what server resources the applications will have access to.

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

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

- To set up the default authentication mode for applications, select an appropriate item from the **Authentication mode** list. **Windows** authentication mode should be selected if any form of IIS authentication is used.

- To set up time that a session can idle before it is abandoned, enter appropriate number minutes into the **Session timeout** field.

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

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

Configuring IIS Application Pool

IIS Application Pool contains all web applications on domains hosted on your server. Dedicated IIS application pool allows your clients to have a level of isolation between web applications used by their domains. Since each dedicated application pool runs independently, errors in one application pool belonging to one client will not affect the applications running in other application pools belonging to other clients.

By default, Plesk offers a shared application pool for all your clients and their customers. However, clients and domains can use dedicated application pools if administrator and client policy permit this.

IIS application pool can work in three modes:

- Shared pool is always used for all clients and domains.
- Dedicated pool is always used for every client and domain.
- Shared pool is used for clients and domains by default; clients are allowed to assign dedicated pools for their customers.

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

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

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

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

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

1   Go to **Server** > **IIS Application Pool**.
2   Click **Stop**.

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

1   Go to **Server** > **IIS Application Pool**.
2   Click **Start**.

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

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

Configuring Shared SSL and Master SSL Domain

Shared SSL is a means of securing the access to a site with SSL (Secure Sockets Layer) for site owners without having them purchase their own SSL certificate. Web sites that employ shared SSL are, in fact, using the certificate shared by another domain. The domain that shares its SSL certificate with others is called Master SSL Domain. Before your customers can use shared SSL, you need to configure the Master SSL Domain. It can be done on the server level, so that in theory any domain can use shared SSL, and on the client level, so that only this client's domains can use shared SSL.

➢ *To configure the Master SSL Domain and enable shared SSL on your server:*

1   Go to **Server** > **Shared SSL**.

2   Select the **Enable shared SSL** checkbox.

3   Select the required domain name from the **Domain name** drop-down menu. Only those domains that are hosted on your server and have SSL enabled, are present in the list.

4   Click **OK**.

➢ *To configure the Master SSL Domain and enable shared SSL for a client:*

1   Go to **Clients** > **client** > **Shared SSL**.

2   Select the **Enable shared SSL** checkbox.

3   Select the required domain name from the **Domain name** drop-down menu. Only those domains that are hosted by this client and have SSL enabled, are present in the list.

4   Click **OK**.

➢ *To disable shared SSL on your server:*

1   Go to **Server** > **Shared SSL**.

2   Clear the **Enable shared SSL** checkbox.

3   Click **OK**.

➢ *To disable shared SSL for a client:*

1   Go to **Clients** > **client** > **Shared SSL**.

2   Clear the **Enable shared SSL** checkbox.

3   Click **OK**.

Configuring Statistics

After installation, the control panel's statistical utility is set up to:

▪ Count the inbound and outbound traffic
▪ Count the disk space occupied by web content, log files, databases, mailboxes, web applications, mailing list archives, and backup files
▪ Keep the traffic statistics only for the last three months

➢ *To review or adjust these settings:*

1 Go to **Server** > **System Preferences**.
2 In the **Retain traffic statistics for ... Months** field specify the term during which the bandwidth usage statistics should be kept for your customers.
3 In the **Include in the disk space usage** field and **Include in the traffic calculation** field select the items that should be considered when disk space and bandwidth usage is calculated.
4 Click **OK**.

Note: In addition to the settings related to statistics, this screen provides the means to rename your server's hostname, and the option to allow or forbid users to create new subdomains and domain aliases in the DNS zones belonging to other users (the **Do not let users create DNS subzones in other users' DNS superzones** check box). We recommend that you select this check box, otherwise, users will be able to create subdomains under domains belonging to other users, and set up Web sites and e-mail accounts which could be used for spamming or even phishing or identity theft.

For instructions on viewing statistics, refer to the chapter Viewing Statistics (on page 263).

Configuring E-mail Notification System

The control panel notifies you and your customers of disk space and bandwidth overage by sending e-mail notifications. With the default settings, however, domain and web site owners are not notified. We recommend that you enable resource overage notification for domain and web site owners because they need to know what happens to their domains and web sites.

Apart from resource overage, the control panel can notify the appropriate users when:

▪ New user accounts are created
▪ New domains are added

- Hosting accounts are expired (expiration date is defined for user accounts and Web sites separately)
- There are new requests for assistance (trouble tickets) from your customers in Help Desk
- The requests are fulfilled and the trouble tickets are closed in Help Desk
- New comments are posted to the existing trouble tickets
- The closed trouble tickets are reopened because the customer has encountered the same problem again

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

1 Go to **Server** > **Notifications**.

2 By selecting the check boxes in the **Notifications** table, specify the types of control panel users or external e-mail users who should receive notices on events.

We recommend that you also select all check boxes in the **domain administrator** column in order to let your resellers' customers know what happens to their Web sites.

3 To view or edit the default notice text, click the respective 📝 icon in the **Text** column.

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

4 Specify when to send the user account and domain (Web site) hosting account expiration notices. By default, such notices are sent 10 days in advance. Click **OK**.

Table. Tags used in notification messages

Event type	Tags that can be used in notices	The data that tags denote
Creation of a user account	*<client>* or *<client_contact_name>*	user's first and last name
	<client_login>	user name for authorization in the control panel
	<password>	user's password for authorization in the control panel
	<hostname>	host name for access to control panel
Expiration of a user account	*<client_login>*	user name for authorization in the control panel
	<client> or *<client_contact_name>*	user's first and last name

	<expiration_date>	user account expiration date
Addition of a new domain name to the server	*<domain_name>* or *<domain>*	domain name
	<client_login>	user name for authorization in the control panel
	<client> or *<client_contact_name>*	user's first and last name
	<ip>	IP address the domain is hosted on
Domain (Web site) hosting account expiration	*<domain_name>* or *<domain>*	domain name
	<client_login>	user name for authorization in the control panel
	<client_contact_name> or *<client>*	user's first and last name
	<expiration_date>	account expiration date
Resource overage	*<domain>* or *<domain_name>*	domain name
	<client_login>	user name for authorization in the control panel
	<client> or *<client_contact_name>*	user's first and last name
	<disk_usage>	information on disk space usage
	<disk_space_limit>	information on the disk space allocated to the account
	<traffic>	information on bandwidth usage
	<traffic_limit>	information on the bandwidth amount allotted to the account

Help Desk events	*<ticket_id>*	trouble ticket identification number automatically assigned by the system
	<reporter>	returns user name for requests submitted by resellers or multi-domain customers, a domain name for requests submitted by domain owner, and e-mail address if the request was submitted by e-mail.
	<server>	the host name
	<ticket_comment>	the contents of the ticket, or a comment posted

Configuring Help Desk

Help Desk is a convenient way for your customers to reach you when they need your assistance. After you set it up and switch on, the Help Desk becomes accessible to all users who were granted access to control panel, including your resellers, domain owners, and e-mail users. Additionally, you can allow submission of problem reports by e-mail.

Your Help Desk shows all reports posted by your resellers and their customers. Your reseller's Help Desk shows only reports posted by himself or herself and his or her customers. The domain owner's Help Desk shows only reports posted by himself or herself and by e-mail users under his or her domain.

➢ *To configure Help Desk and allow your customers post problem reports through the control panel:*

1   Go to **Help Desk** > **General Settings**.

2   Select the **Allow customers to submit tickets** check box.

3   Select the trouble ticket queue, priority and category that will be offered to your customers as the default choice.

When users post a new ticket, they can specify the order in which they would prefer their problems to be resolved (queue), the priority of their requests (priority), and the category to which the problem is related (category). The queue, priority and category are abstract entities: they have no effect on the system, but they can help you decide what problems to resolve in the first place. There are three predefined queues and priority levels and nine predefined categories including **Database**, **DNS**, **FTP**, **General**, **Hosting**, **Mail**, **Mailing Lists**, **Site Applications**, and **Tomcat Java**. You can remove these items and add your own.

4   Click **Switch On** in the **Tools** group, then click **OK**.

➢ *If you wish to allow users to submit problem reports by e-mail:*

1   Create a POP3 mailbox with an e-mail address like helpdesk@your-domain.com or anything you like.

2   Configure the Help Desk to periodically retrieve problem reports from that mailbox and post them to your Help Desk.

3   Inform your customers of the Help Desk's e-mail address.

➢ *To allow users to submit problem reports to Help Desk by e-mail:*

1   Go to **Help Desk** > **Mail Gate Settings**.

2   Specify the following settings:

- **Notification sender's name**, and **Notification sender's return address**. Once a report has been retrieved by e-mail and posted to the Help Desk, the Help Desk sends a notice to the report sender. This allows the report sender to subsequently add comments to the report by replying to the message. Therefore, we recommend that you specify your Help Desk's e-mail address in the **Notification sender's return address** box, and type a phrase like "<company name> Help Desk" into the **Notification sender's name** box. Be sure to specify your organization name in place of <company name> and omit the quotation marks.

- **POP3 server**: POP3 server the mail should be fetched from.

- **POP3 login**: user name for authentication to the mail server.

- **New POP3 password**: password that will be used for authentication to the mail server and retrieving problem reports from the mailbox.

- **Confirm POP3 password**: retype password for confirmation.

- **Query mail once in**: specify how often Help Desk should check for new reports.

- **Ticket subject must start with**: specify the combination of symbols the subject line of e-mail messages (problem reports) must start with. This can help filter out spam. All e-mail messages that do not have the specified combination of symbols in the subject line will be deleted.

3 Click **Switch On** in the **Tools** group and click **OK**.

➢ *To view, add, edit, or remove queues:*

1 Go to **Help Desk** > **Queues**. The queues will be presented in a list.

- To add a new queue, click **Add New Queue**, type the desired number into the **Title** box, leave the **Switched on** check box selected, and click **OK**.

- To edit a queue, click its title in the **Title** column. Edit it as required, and click **OK**.

- To temporarily disallow your users to select a queue when posting new reports, click its title in the **Title** column, clear the **Switched on** check box, and click **OK**.

- To delete a queue, select the respective check box and click ✖ **Remove Selected**.

➢ *To view, add, edit, or remove priorities:*

1 Go to **Help Desk** > **Priorities**. The priorities will be presented in a list.

- To add a new priority, click **Add New Priority**, type the desired combination of symbols into the **Title** box, leave the **Switched on** check box selected, and click **OK**.

- To edit a priority, click its title in the **Title** column. Edit it as required, and click **OK**.

- To temporarily disallow your users to select a priority when posting new reports, click its title in the **Title** column, clear the **Switched on** check box, and click **OK**.

- To delete a priority, select the respective check box and click ✖ **Remove Selected**.

➢ *To view, add, edit, or remove categories:*

1 Go to **Help Desk** > **Categories**. The categories will be presented in a list.

- To add a new category, click **Add New Category**, type the desired combination of symbols into the **Title** box, leave the **Switched on** check box selected, and click **OK**.

- To edit a category, click its title in the **Title** column. Edit it as required, and click **OK**.

- To temporarily disallow your users to select a category when posting new reports, click its title in the **Title** column, clear the **Switched on** check box, and click **OK**.

- To delete a category, select the respective check box and click ✖ **Remove Selected**.

➢ *To disallow customers to send reports to Help Desk by e-mail:*

1 Go to **Help Desk** > **Mail Gate Settings**.

2 Click **Switch off** in the **Tools** group.

➢ *To disallow use of Help Desk for all your customers and resellers:*

1 Go to **Help Desk** > **General Settings**.

2 Click **Switch off** in the **Tools** group.

Also see the Using Help Desk for Resolving Your Customers' Issues section.

Configuring Port Range for Passive FTP Mode

➢ *To set a specific port or port range that can be used for passive FTP mode connections on all domains hosted on your server:*

1 Go to **Server** and click **FTP Settings**.

2 Provide the required port or port range in the **Port or port range for passive FTP mode connections** field and click **OK**.

Adjusting System Date and Time

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

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

1   Go to **Server** > **System Time**.

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

3   Select your time zone from the list, and click **Set**.

> **Note**. Clear the **Automatically adjust clock for daylight saving changes** checkbox, if you do not wish Plesk to automatically adjust the server clock.

You will need to reboot your Plesk server for the time zone change to take effect.

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

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

> **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.

Starting, Stopping and Restarting Plesk Services

You can monitor, start, stop, restart and disable various Plesk services, and also change their startup type from the control panel.

➢ *To see the status of a service:*

1 Go to **Server** > **Service Management.**

2 Click ● **Show All** to show all services from the service groups. To hide all services, click ✎ **Hide All**. The current state of a service or a group of services is marked by an icon:

  ▪ ◐ means that the service or all services in a group are running,

  ▪ ⊗ means that the service or all services in a group are stopped,

  ▪ ⊘ means that several services in a group are running and some are stopped,

  ▪ ○ means that the service is not installed or its management capabilities are not supported by the license key.

  ▪ In the **Startup Type** field you can see whether the service is started automatically or should be started manually.

➢ *To start a service:*

1 Go to **Server** > **Service Management.**

2 Click the ▶ icon corresponding to the service you wish to start.

➢ *To restart a service:*

1 Go to **Server** > **Service Management.**

2 Click the ◉ icon corresponding to the service you wish to restart.

➢ *To stop a service:*

1 Go to **Server** > **Service Management.**

2 Click the ■ icon corresponding to the service you wish to stop.

➢ *To set service startup type:*

1 Go to **Server** > **Service Management.**

2 Select the check box corresponding to the required service in the list.

3 Select the required startup type:

  ▪ Click ↻ **Manual** to start selected services manually upon Plesk startup.

- Click **Auto** to start selected services automatically upon Plesk startup.

➢ *To disable a service:*

1 Go to **Server** > **Service Management.**

2 Select the check box corresponding to the required service in the list.

3 Click **Disable**.

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

1 Go to **Server** > **Service Management.**

2 Select the check boxes corresponding to the required services in the list.

3 Click the button corresponding to the action you want to perform on the selected services:

1. Click **Start** to start selected services.

2. Click **Stop** to stop selected services.

3. Click **Restart** to restart selected services.

4. Click **Disable** to disable selected services.

5. Click **Manual** to start selected services manually upon Plesk startup.

6. Click **Auto** to start selected services automatically upon Plesk startup.

Scheduling Tasks

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

During installation of Plesk the following tasks are automatically created:

- Update Dr.Web Antivirus database – updates Dr.Web virus database
- Statistics calculation - generates statistics on resource usage, such as traffic and disk space.

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

Note. You can also schedule tasks on a per-domain basis. To do so, follow the same procedures listed below, but instead of going to **Server** > **Scheduler Tasks**, go to **Domains** > **domain name** > **Scheduler Tasks**.

➢ *To schedule a task:*

1 Go to **Server** > **Scheduler Tasks**.

2 Click **Add New Task**.

3 Leave the **Switched on** checkbox selected if you want your scheduled task to be active immediately after the creation.

4 Input a name for your task in the **Description** field.

5 In **Scheduler notification**, specify whether the scheduler should notify you when it runs this task. The following options are available:

- **Switched off** - do not nofity you.
- **Send to the default e-mail** - send the notification to your default e-mail address.
- **Send to the e-mail I specify** - send the nofitication to the e-mail specified in the corresponding field. After selecting this option, you need to input the required e-mail in the field on the right.

  Click **Set** to save scheduler notifications settings.

6 Specify which command to run. Type it into the **Path to executable file** input box. If you need to run the command with certain options, type them in the **Arguments** field.

7 Select the appropriate priority in the **Task priority** field. Task priority can be set to **Low**, **Normal** or **High**.

8 Specify when to run your command by selecting the appropriate checkboxes in the **Hours**, **Days of Month**, **Months** or **Days of Week** fields.

9 Click **OK** to schedule the task or click **Run Now** to schedule the task and immediately run it.

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

1 Go to **Server** > **Scheduler Tasks**.

2 Choose a task that you wish to suspend and click on the command name.

3 Clear the **Switched on** checkbox.

➢ *To resume execution of scheduled task:*

1 Go to **Server** > **Scheduler Tasks**.

2 Choose a task whose execution you wish to resume and click on the command name.

3 Select the **Switched on** checkbox.

➢ *To unschedule a task:*

1 Go to **Server** > **Scheduler Tasks**.

2 Select a check box to the right of the task that you wish to unschedule.

3 Click ✖ **Remove Selected**.

4 Confirm removal and click **OK**.

Delegating Administrative Privileges to Technical Support Engineers

You can create additional Administrator level accounts for your technical support engineers, enabling them to perform a virtually limitless variety of administrative tasks. All actions performed by additional Plesk Administrator accounts are logged, which gives the actual Plesk Administrator an unprecedented level of control over additional Administrator accounts' activities. Additional Administrator level accounts have virtually all the privileges that the actual Plesk Administrator has, except the following:

▪ View and manage additional Administrator accounts belonging to other users

▪ View and manage Plesk Administrator account settings

▪ Clear Action Log

In this section:

Creating Additional Administrator Accounts

➤ *To create additional Administrator account:*

1 Go to **Server** > **Additional Accounts**.

2 Click **Add New Administrator Subaccount**.

3 Specify Administrator account properties:

- Specify account login, password and e-mail address in the corresponding fields.

- Specify the name of additional Administrator account user in the **Contact name** field.

- Use **Comments** field to add your own comments about this particular additional Administrator account and its user. This can be useful to differentiate between the accounts: for example, you can create one account for a technical support engineer who manages client accounts, and another account for a technical support engineer who works with all mail-related issues. By adding appropriate commentary in the **Comments** field, you can always tell who's doing what, and avoid confusion.

4 Click **OK** to finish the creation of additional Administrator account.

   Now you can tell account login and password to its owner.

Modifying Additional Administrator Accounts

➤ *To modify settings of additional Administrator account:*

1 Go to **Server** > **Additional Accounts**.

2 Click the required additional Administrator account login in the list

3 Specify new Administrator account properties:

- Specify new account login, password and e-mail address in the corresponding fields.

- Specify the new name of additional Administrator account user in the **Contact name** field.

- Use **Comments** field to add your own comments about this particular additional Administrator account and its user. This can be useful to differentiate between the accounts: for example, you can create one account for a technical support engineer who manages client accounts, and another account for a technical support engineer who works with all mail-related issues. By adding appropriate commentary in the **Comments** field, you can always tell who's doing what, and avoid confusion.

4 Click **OK** to update the information of additional Administrator account.

Suspending And Unsuspending Additional Administrator Accounts

> ➢ *To suspend additional Administrator account:*

1 Go to **Server** > **Additional Accounts**.

2 Click the required additional Administrator account login in the list.

3 Clear the **Allow access to control panel** checkbox and click **OK**.

> ➢ *To unsuspend additional Administrator account:*

1 Go to **Server** > **Additional Accounts**.

2 Click the required additional Administrator account login in the list.

3 Select the **Allow access to control panel** checkbox and click **OK**.

Removing Additional Administrator Accounts

> ➢ *To remove additional Administrator account:*

1 Go to **Server** > **Additional Accounts**.

2 Select the check box corresponding to the additional Administrator account you wish to remove and click ✖ **Remove Selected**.

3 Confirm removal and click **OK**.

Serving Your Customers

This chapter provides you with detailed instructions on setting up and managing user accounts, web sites, and e-mail accounts.

In this chapter:

Before You Start Serving Your Customers

This section explains the actions you are suggested to do before you start providing services to your your customers.

In this section:

Simplifying Setup of User Accounts

If you are going to serve numerous users, you may want to create account configuration presets, referred to as client templates, that will simplify setting up user accounts for new customers. The templates cover all resource usage allotments, permissions and limits that you can define for a user account.

➢ *To create a client template:*

1   Go to **Clients** > **Client Templates**.

2   Click **Add New Client Template**.

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

During setup of a new user account, you will be prompted to select the required template by its name. Therefore, we recommend that you choose a meaningful name that corresponds to one of your hosting plans or describes the amount of allotted resources. For example, **Reseller account, 5GB disk space, 100 domains**.

4   Specify the permissions for the template in the **Permissions** section. Use **Select All** to select all permissions and **Clear All** to clear all permissions.

- **Access to control panel**. Specify whether the customer will be able to access the control panel for managing his or her account and sites.

- **Domain creation**. Specify whether the customer will be able to set up hosting accounts for new sites.

- **Physical hosting management**. Specify whether the customer will be able to set up hosting accounts, modify hosting account features and switch on or off support for programming and scripting languages.

- **System access management**. Specify whether the customer will be able to access to the system through Remote Desktop.

- **Hard disk quota assignment**. Specify whether the customer will be able to assign hard quotas on disk space for his or her own web sites and for web sites of his or her customers.

- **Subdomains management**. Specify whether the customer will be able to set up additional sites under his or her domains and allow his or her customers to do so.

- **Domain aliases management**. Specify whether the customer will be able to set up additional alternative domain names for his or her web sites and allow his or her users to do so.

- **Log rotation management**. Specify whether the customer will be able to adjust the cleanup and recycling of processed log files for his or her sites.

- **Anonymous FTP management**. Specify whether the customer will be able to have an FTP directory where all users could download and upload files without the need to enter login and password. A web site should reside on a dedicated IP address in order to use anonymous FTP service.

- **FTP accounts management**. Specify whether the customer will be able to create and manage additional FTP accounts.

- **Scheduler management**. Specify whether the customer will be able to schedule tasks with the task scheduler. Scheduled tasks can be used for running scripts or utilities on schedule.

- **Domain limits adjustment**. Specify whether the customer will be able to change the limits for his or her web sites.

- **DNS zone management**. Specify whether the customer will be able to manage the DNS zones of his or her domains.

- **Java applications management**. Specify whether the customer will be able to install Tomcat Java applications and applets on web sites through the control panel.

- **Mailing lists management.** Specify whether the customer will be able to use mailing lists.

- **Spam filter management**. Specify whether the customer will be able to use SpamAssassin spam filter and customize filtering settings.

- **Antivirus management**. Specify whether the customer will be able to use server-side antivirus protection for filtering incoming and outgoing mail.

- **Backup/restore functions**. Specify whether the customer will be able to use the control panel's facilities to backup and restore their site. Scheduled and on-demand backups are supported.

- **Ability to use remote XML interface**. Specify whether the customer will be able to remotely manage his or her web sites through custom applications. The XML interface can be used for developing custom applications integrated with web sites, which could be used, for instance, for automating setup of hosting accounts and provisioning of services for customers purchasing hosting services from your reseller's site.

- **SiteBuilder**. Specify whether the customer will be able to use SiteBuilder for creating and editing their web site.

- **Hosting perfomance management**. Specify whether the customer will be able to change the hosting performance preferences for their domains.

- **IIS application pool management**. Specify whether the customer will be able to manage their IIS application pool.

- **Web statistics management**. Specify whether the customer will be able to manage web statistics for their domains.

- **Additional write/modify permissions management**. Specify whether the customer will be able to manage additional write/modify permissions for their domains. These permissions are required if customer's web applications are using a file-based database (like Jet) located in the root of `httpdocs` or `httpsdocs` folders. Please note that selecting this option might seriously compromise the web site security.

- **Shared SSL management**. Specify whether the customer will be able to manage shared SSL for their domains.

- **User interface**. Specify the type of user interface the customer will be able to use - standard, desktop, or both.

- **Desktop management**. Specify whether the customer will be able to customize his or her desktop interface.

- **Ability to select a database server**. Specify whether the customer will be able to select a database server of each type for creating his or her databases, not only use the default database server.

5 Specify the limits for the template in the **Limits** section:

- **Maximum number of domains**. Specify the total number of domain names your customer will be able to host on the server. This includes domains hosted on this server, and domain forwarders that point to web sites hosted on other servers. Domain aliases (additional domain names for a site hosted on this server) and subdomains are counted separately and are not limited by this resource type.

- **Maximum number of domain aliases**. Specify the number of domain aliases your customer can use for his or her domains.

- **Maximum number of subdomains**. Specify the total number of subdomains that the customer will be able to host.

- **Disk space**. Specify the total amount of disk space in megabytes that is allocated to the customer. It includes disk space occupied by all files related to user's domains: web site contents, databases, applications, mailboxes, log files and backup files. This is the so-called soft quota: when it is exceeded, the user account and domain names are not suspended automatically, only the appropriate notices are sent to your and your customer's e-mail addresses and the resource overage is indicated by the icon ⚠ shown in your and your customer's control panels to the left of the user name (see the list of clients that opens when you click the **Clients** shortcut in the navigation pane) or domain name (see the list of domain names that opens when you click the **Domains** shortcut in the navigation pane).

- **MySQL databases quota** and **Microsoft SQL databases** quota. Specify the maximum disk space amount in megabytes that MySQL and Microsoft SQL Server databases respectively can occupy on a domains belonging to the customer.

- **Maximum amount of traffic**. Specify the amount of data in megabytes that can be transferred from the customer's web sites during a month. Once the limit is reached, the appropriate notices are sent to your and your customer's e-mail addresses and the resource overage is indicated by the corresponding icon ⚠ shown in the control panel to the left of the user name (see the list of clients that opens when you click the **Clients** shortcut in the navigation pane) or domain name (see the list of domain names that opens when you click the **Domains** shortcut in the navigation pane).

- **Maximum number of web users**. Specify the total number of personal web pages that your customer can host for other users under his or her domains. This service is mostly used in educational institutions that host non-commercial personal pages of their students and staff. These pages usually have web addresses like http://your-domain.com/~username.

- **Maximum number of additional Microsoft FrontPage accounts**. Specify the maximum number of additional Microsoft FrontPage accounts that the customer can create on his or her domains.

- **Maximum number of additional FTP accounts**. Specify the maximum number of additional FTP accounts that the customer can create on his or her domains.

- **Maximum number of MySQL databases** and **Maximum number of Microsoft SQL server databases**. Specify the maximum number of MySQL and Microsoft SQL Server databases respectively that the customer can create on his or her domains.

- **Maximum number of mailboxes**. Specify the total number of mailboxes that the customer can host on the server.

- **Mailbox quota**. Specify the amount of disk space in kilobytes that is allocated to each mailbox.

- **Total mailboxes quota**. Specify the total amount of disk space in megabytes available for all mailboxes on all domains belonging to the customer.

- **Maximum number of mail redirects**. Specify the total number of mail redirects that the customer can set up.

- **Maximum number of mail groups**. Specify the total number of mail groups that the customer can set up.

- **Maximum number of mail autoresponders**. Specify the total number of automatic responses that the customer can set up.

- **Maximum number of mailing lists**. Specify the total number of mailing lists that you customer can host on the server.

- **Maximum number of Java applications**. Specify the total number of Tomcat Java applications or applets that can be hosted on the server.

- **Maximum number of IIS application pools**. Specify the total number of dedicated IIS application pools that the customer can allocate between his or her domains.

- **Maximum number of shared SSL links**. Specify the total number of shared SSL links that the customer can use on his or her domains.

- **Maximum number of ODBC connections**. Specify the total number of ODBC connections that the customer can use on his or her domains.

- **Validity period**. Specify the term for a hosting account. At the end of the term, all customer's domains will be suspended, its Web, FTP and mail services will no longer be accessible to the Internet users, and the reseller and his or her customers (domain owners) will not be able to log in to the control panel. Accounts cannot be automatically renewed, therefore, in order to bring the hosted domain names back to operation, you will need to manually renew the user account by specifying another term in the **Validity period** box (**Clients** > **client name** > **Limits**) and then clicking **Switch On** (**Clients** > **client name**).

6 In the **IP addresses** section specify the shared IP addresses that you wish to allocate to the customer.

If you wish to automatically provision dedicated IP addresses, select the **Allocate exclusive IP addresses to client** check box and specify the number of IP addresses that should be taken from your IP range and assigned to the customer.

7 In the **Preferences** section, select the **Create SiteBuilder User** checkbox if you wish to create a SiteBuilder user for the client template.

8 Click **OK** to complete creation of a template.

Now you can select the required template during the setup of a new user account. The account will be created and allocated the resources you defined.

➢ *To modify a template:*

1 Go to **Clients** > **Client Templates**.

2 Click the template name you need.

3 Modify the settings as required and click **OK**.

Note: Modifying templates does not affect the existing user accounts that were created by these templates.

➢ *To remove a template that you no longer need:*

1 Go to **Clients** > **Client Templates**.

2 Select a check box corresponding to the template you no longer need.

3   Click ✕ **Remove Selected**. Confirm removal and click **OK**.

Simplifying Setup of Domains and Web Sites

If you are going to serve numerous users with a sizeable number of domains, you may want to create hosting configuration presets, referred to as domain templates, that will that will simplify setting up hosting accounts for new domains and web sites. The templates cover all resource usage allotments, permissions and limits that you can define for a hosting account, plus mail bounce and Web statistics retention settings.

➢ *To create a domain template:*

1 Go to **Domains** > **Domain Templates**.

2 Click **Add Domain Template**.

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

   During setup of a new hosting account, you will be prompted to select the required template by its name. Therefore, we recommend that you choose a meaningful name that corresponds to one of your hosting plans or describes the amount of allotted resources. For example, **Mail hosting, 1GB disk space, 500 mailboxes**.

4 Specify the domain-wide mail bounce options in the **Mail** section:

   When somebody sends an e-mail message to an e-mail address that does not exist under your domain, the mail server on your domain accepts mails, processes it, and when it finds out that there is no such a recipient under your domain, it returns the mail back to sender with the "this address no longer accepts mail" notice. You can choose to:

   ▪ change the default notice if you do not like it (leave the **Bounce** option selected and type another message into the input box),

   ▪ forward undelivered mail to another e-mail address (select the **Catch to address** option and specify the e-mail address you need), or

   ▪ reject mail without accepting it (select the **Discard** option). This setting can decrease mail server load caused by a large amount of spam, which is often directed at randomly generated user names. However, for spammers this can somewhat speed up scanning your mail server for valid e-mail addresses.

5 Choose the required WebMail client software in the **WebMail** menu to enable the ability to read mail through a browser-based WebMail application for users of mailboxes in this domain. If you don't want to provide this ability, select **None**.

6 Specify the limits for the template in the **Limits** section:

   ▪ **Maximum number of domain aliases**. Specify the number of domain aliases that can be used for this domain.

   ▪ **Maximum number of subdomains**. Specify the number of subdomains that can be hosted under this domain.

- **Disk space**. Specify the total amount of disk space allocated to a hosting account associated with the domain. This amount is measured in megabytes. It includes disk space occupied by all files related to this domain/web site: web site contents, databases, applications, mailboxes, log files and backup files. This is the so-called soft quota: when it is exceeded, domain names and web sites are not suspended automatically, only the appropriate notices are sent to your and your provider's e-mail addresses and the resource overage is indicated by the icon 🟠 shown in the control panel to the left of the domain name (see the list of domain names on your Home page). And then it is up to you to decide what to do with the domain. You can notify the domain owner and suspend the domain/web site after a grace period until you receive the payment or upgrade the hosting plan for your customer (see the Managing User Accounts (on page 114) section for more information).

- **MySQL databases quota** and **Microsoft SQL databases** quota. Specify the maximum disk space amount that MySQL and Microsoft SQL Server databases respectively can occupy on a domain.

- **Maximum amount of traffic**. Specify the amount of data in megabytes that can be transferred from the web site during a month. Once the limit is reached, the appropriate notices are sent to your and your provider's e-mail addresses and the resource overage is indicated by a corresponding icon shown in the control panel to the left of the domain name (see the list of domain names on your Home page). When a web site starts attracting more visitors and requires more bandwidth, consider upgrading a hosting plan (see the instructions on upgrading hosting plan below).

- **Maximum number of web users**. Specify the number of personal web pages that the domain owner can host for other users under his or her domain. This service is mostly used in educational institutions that host non-commercial personal pages of their students and staff. These pages usually have web addresses like http://your-domain.com/~username.

- **Maximum number of additional Microsoft FrontPage accounts**. Speficy the maximum number of additional Microsoft FrontPage accounts that can be created on a domain.

- **Maximum number of additional FTP accounts**. Speficy the maximum number of additional FTP accounts that can be created on a domain.

- **Maximum number of MySQL databases** and **Maximum number of Microsoft SQL Server databases**. Specify the maximum number of MySQL and Microsoft SQL Server databases respectively that can be hosted on a domain.

- **Maximum number of mailboxes**. Specify the number of mailboxes that can be hosted in a domain.

- **Mailbox quota**. Specify the amount of disk space in kilobytes that is allocated to each mailbox in a domain.

- **Total mailboxes quota**. Specify the total amount of disk space available for all mailboxes on a domain.

- **Maximum number of mail redirects**. Specify the number of mail redirects that can be used in a domain.

- **Maximum number of mail groups**. Specify the maximum number of mail groups that can be used in a domain.

- **Maximum number of mail autoresponders**. Specify the number of automatic responses that can be set up in a domain.

- **Maximum number of mailing lists**. Specify the number of mailing lists that the domain owner can run in a domain. To allow the use of mailing lists, you should also put a check mark into the **Mailing lists** check box under the **Preferences** group.

- **Maximum number of Java applications**. Specify the maximum number of Tomcat Java applications and applets that the domain owner can install in a domain.

- **Maximum number of shared SSL links**. Specify the maximum number of subdomains (including their parent domain) that can link to the Master SSL domain defined by the server administrator.

- **Maximum number of ODBC connections**. Specify the maximum number of ODBC connections that can be set up on a domain.

- **Validity period**. Specify the term for a hosting account. At the end of the term, the domain/web site will be suspended, its Web, FTP and mail services will no longer be accessible to the Internet users, and domain owner will not be able to log in to the control panel. Hosting accounts cannot be automatically renewed, therefore, in order to bring the hosted domain name/web site back to operation, you will need to manually renew the hosting account: on your Home page, click the domain name your need, click **Limits**, specify another term in the **Validity period** box, click **OK**, then click **Switch On** in the **Domain** group (**Home** > **domain name**).

7 Select the required log rotation options in the **Switch on log rotation** section.

All connections to the Web server and requests for files that were not found on the server are registered in log files. These log files are analyzed by the statistical utilities running on the server, which then present graphical reports on demand. If you need to view the contents of these raw log files for debugging purposes, on your Home page, click the domain name you need, click **Log Manager**, and then click the log file name you need. To prevent these log files from growing too large, you should enable automatic cleanup and recycling of log files:

1. Select the **Switch on log rotation** check box.

2. Specify when to recycle log files.

3. Specify how many instances of each log file to store on the server.

4. Specify whether they should be compressed.

5. Specify whether they should be sent to an e-mail address after processing.

8 Specify additional settings in the **Preferences** section.

1. **Mailing lists**. Select this checkbox to enable the ability to create and manage mailing lists on the domain.

2. **Traffic statistics retention**. Specify the number of months during which the bandwidth usage statistics should be kept on the server.

9 In the **DNS** field specify whether the DNS server on your Web host should act as a master (primary) or slave (secondary) name server for the domain name zone. A primary name server stores locally the zone file it serves, while a secondary server only retrieves a copy of this file from the primary. You would normally leave the **Master** option selected.

10 If you are going to host not only domain names, but also web sites, select the **Physical hosting** check box and specify the hosting features:

- **Hard disk quota**. In addition to the soft quota, you can specify the so-called hard quota that will not allow writing more files to the web space when the limit is reached. At attempt to write files, users will get "Out of disk space" error.

- **SSL support**. Secure Sockets Layer encryption is generally used for protecting transfer of sensitive data during online transactions on e-commerce Web sites that run on dedicated IP addresses. SSL certificates that participate in the encryption process are usually applied to a single domain name on a single IP address, therefore, each site that needs SSL protection must be hosted on a dedicated IP address. An exception to this is subdomains, which you can protect with a wildcard certificate. Installing an SSL certificate on a Web server that hosts several web sites with different domain names on a single IP address (shared or name-based hosting) is technically possible, however, it is not recommended: the encryption will be provided, but users will get warning messages on attempt to connect to the secure site. To allow SSL encryption for Web sites, select the **SSL support** check box.

- **SiteBuilder support.** SiteBuilder is an efficient and user-friendly WYSIWYG web site editor running through the web interface. Leave the **Publish site with SiteBuilder** checkbox selected to give domain administrator the ability to access SiteBuilder and build web site through their Plesk control panel interface by clicking **SiteBuilder Wizard** on the domain management page or clicking the **Desktop** shortcut in the **SiteBuilder Admin** navigation pane group. The version of SiteBuilder coming in the standard Plesk distribution is fully functional and its use is not limited in any way by the manufacturer (but you can be restricted from accessing it by your service provider).

- **Microsoft FrontPage support**. Microsoft FrontPage is a popular web site authoring tool. To enable publishing and modifying the site through Microsoft FrontPage, select the **Microsoft FrontPage support** and **Microsoft FrontPage over SSL support** check boxes, and set the **Remote Microsoft FrontPage authoring** option to **allowed**.

  > **Note**. Microsoft FrontPage over SSL support is available only when SSL support is enabled on a domain.

- **Support for programming and scripting languages widely used in development of dynamic Web sites and server-side Web applications**. Specify which of the following programming and scripting languages should be interpreted, executed or otherwise processed by the web server: Active Server Pages (ASP), Active Server Pages on .NET framework (ASP.NET), Server Side Includes (SSI), PHP hypertext preprocessor (PHP), Common Gateway Interface (CGI), Fast Common Gateway Interface (FastCGI), Internet Server Application Programming Interface (ISAPI), Perl, Python, ColdFusion and Miva scripting required for running Miva e-commerce solutions.

  > **Note.** You can change the version of ASP.NET and PHP you want to use in the corresponding drop-down menu. You can also specify the mode for running PHP applications - CGI, FastCGI or ISAPI.

- **Web statistics**. To allow you to view the information on the number of people visited the site and the pages of the site they viewed, select a module in **Web statistics** drop-down menu and select the **accessible via password protected directory /plesk-stat/** checkbox, if required. This will install the selected statistical software module, which will generate reports and place them into the password protected directory. The domain administrator will then be able to access Web statistics at the URL: https://your-domain.com/plesk-stat/ using their FTP account login and password.

> **Note.** If domain administrator changes the FTP credentials, web statistics access credentials do not change. The original login and password specified upon the domain creation should always be used for accessing password-protected web statistics directory.

- **Custom error documents**. When visitors coming to site request pages that the web server cannot find, web server generates and displays a standard HTML page with an error message. To give domain owner the ability to create their own error pages and use them on a web server, select the **Custom error documents** checkbox.

> **Note.** You can enable the support for all programming and scripting languages, web statistics and custom error documents at once by selecting **All services** checkbox in the **Services** group.

- **Additional write/modify permissions.** This option is required if customer's web applications are using a file-based database (like Jet) located in the root of `httpdocs` or `httpsdocs` folders. Please note that selecting this option might seriously compromise the web site security.

- **Use dedicated IIS application pool.** This option enables the use of dedicated IIS application pool for web applications on a domain. Using dedicated IIS application pool dramatically improves the stability of domain web applications due to worker process isolation mode. This mode gives each web site hosted on the server 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. This is especially useful when you are using shared hosting package.

- **Maximum CPU use**. To limit the amount of CPU resources that domain's IIS application pool can use, clear the **Unlimited** checkbox and provide a number (in percents) in the field.

11 Performance. To avoid excessive usage of bandwidth, which can lead to resources overage, you can set various performance limitations for a domain.

- **Maximum network use.** To limit the maximum speed (measured in KB per second) that a domain can share between all its connections, clear the **Unlimited** checkbox and provide a number (in kilobytes) in the field.

- **Connections limiting.** To limit the maximum number of simultaneous connections to a domain, clear the **Unlimited** checkbox and provide a number in the field

12 Click **OK** to complete creation of a template.

During setup of a hosting account for a new domain/web site, you will select the required template and the hosting account will be created and allocated the resources and hosting services you defined.

➢ *To reflect the changes in your domain templates that will apply to the newly created accounts:*

1 Go to **Domains** > **Domain Templates**.

2 Click the template name corresponding to the domain template you wish to update.

3 Modify the settings as required and click **OK**.

Note that modifying templates does not affect the existing domains and web sites.

➢ *To remove a template that you no longer need:*

1   Go to **Domains** > **Domain Templates**.

2   Select a check box corresponding to the template you no longer need.

3   Click ✖ **Remove Selected**. Confirm removal and click **OK**.

Prepackaging Applications Your Customers Can Use

Plesk comes with a number of free site applications that you can choose to provide to your customers or remove from the control panel script library (referred to as application vault). You can also obtain and install applications from third-party vendors through the application portal www.apsstandard.com.

You can set usage rules for any site application you add to the vault. For example, you can make a certain free application a commercial one that will be available to your customers only if you add it to their application pools under your conditions (for instance, after you received payment). When you change a free site application into a commercial one, it is withdrawn from the application pools of all clients. Now only you can add this application to your clients' application pools when needed. When you change a commercial application into a free one, it becomes free of charge for all clients.

All free of charge open source application packages are automatically added to application pools of all clients after installation of Plesk.

➢ *To view the information about the application packages you have in the vault:*

1 Click the **Server** shortcut in the navigation pane.

2 Click the **Application Vault** icon in the **Services** group.

.All application packages stored in the vault are listed in the **Site Application Packages** group.

There are two icons next to the application name. The left icon denotes the following:

✔ - the application is shown in the list of applications available for installation.

⚪ - the application is hidden from the list of applications available for installation.

The icon in the right column denotes the site application usage rules you defined:

❄ - free of charge, automatically added to the application pools of all clients.

$ - commercial application, can be added to a client application pool only by you under certain conditions.

The **Clients** column shows the number of users using the site application.

3 To sort applications by category, select the category you need from the menu located next to the search box.

➢ *To add a new application to the application vault:*

1 Click the **Server** shortcut in the navigation pane.

2 Click the **Application Vault** icon in the **Services** group.

3 Click **Add New Application Package**.

4 Click **Browse** and locate your application package in .zip format, then click **OK**.

> *To make a certain free application a commercial one and to add it to application pools of selected customers:*

1   Click the **Server** shortcut in the navigation pane.

2   Click the **Application Vault** icon in the **Services** group.

3   Click the 🟦 icon next to the application name.

   Now the application was removed from application pools of all clients, and you can manually add this application to the pools of selected clients, as described in the following steps.

4   Go to **Clients > *client name* > Application Pool**.

5   Click **Add an Application Package to Client's Pool**.

6   Select a check box corresponding to the application you need and click **OK**.

> *To upgrade an application package:*

1   Go to **Server** > **Application Vault > Add New Application Package**.

2   Click **Browse** and locate the updated distribution package in .zip format, then click **OK**.

3   Go to **Domains > domain name > Web Applications**.

4   Click the corresponding shortcut in the **U** column.

5   Select the application version to which you want to upgrade, read the terms of the license agreement, and then click **Upgrade**.

6   Repeat the steps 3 to 6 for every domain/Web site hosted on your server, or inform your customers (site owners) who use this application that they can upgrade this application to the new version. To do so, they will need to click the **Web Applications** icon on their home pages in Plesk, and then click a corresponding shortcut in the **U** column.

> *To remove from the application vault the applications that you do not want to provide to your customers:*

1   Click the **Server** shortcut in the navigation pane.

2   Click the **Application Vault** icon in the **Services** group.

3   Select a check box corresponding to the application you want to remove and click ✖ **Remove Selected**.

4   Confirm removal and click **OK**.

   The application distribution package was removed from the server application vault. Note that the applications already installed on users' sites are not removed.

If you need to install an application on a site, refer to the Installing Applications (on page 162) section.

Certain applications (for example, Counter-Strike Game Server) cannot be installed on individual sites, operating on the server level instead.

➢ *To view the list of available server-wide applications:*

1 Go to **Server** > **Application Vault** > **Server Applications**.

2 Click **Add New Server Application**.

  OR

1 Go to **Server** > **Application Vault** > **Server Applications Repository**.

➢ *To install a server-wide application:*

1 Go to **Server** > **Application Vault** > **Server Applications**.

2 To specify which application you wish to install, select a radio button corresponding to the application of your choice.

3 Click **Install**.

4 Specify the installation preferences and other information that may be required by the application (the requirements may vary among applications). When finished, click **Install**.

➢ *To remove a server-wide application:*

1 Go to **Server** > **Application Vault** > **Server Applications**.

2 Select the corresponding check box and click **Remove Selected**.

3 Confirm the removal and click **OK**.

Managing User Accounts

Plesk users hierarchy is limited to three user levels: **client accounts**, **domain administrator accounts**, and **e-mail user accounts**. All these types of users can have access to control panel for managing their own web sites and e-mail accounts.

For users who need to resell hosting services or host numerous domains/web sites, you should create **client accounts**. And then, your resellers can create **domain administrator accounts** for their own customers. A domain administrator's account can be created only after the user's site is hosted on the server. A domain administrator account is limited to having only one site, however, a domain administrator can provide other users with mail hosting services under his or her domain. For that purpose, **e-mail user accounts** are created and granted access to control panel.

In this chapter:

Adding User Accounts

This chapter focuses on client level accounts that you will create for your customers or resellers.

If you need to create a domain administrator's account for your reseller's customer, assign permissions and allocate resources, see the Setting Up Hosting Account for a Web Site (on page 129) section.

If you need to create an e-mail user account, see the Creating Mailboxes (on page 218) section.

➢ *To accommodate a new customer or reseller:*

1 Click the **Clients** shortcut in the navigation pane.

2 Click **Add New Client Account** in the **Tools** group.

3 Specify the contact and billing information. Contact name, login name and password are obligatory fields.

4 Select the default interface language for client in the **Interface language** menu.

5 If you have predefined user account templates, you can select the template you need from the **Select template** drop-down box. If you have selected the client creation without template, you will be offered to create a SiteBuilder user account; clear the **Create SiteBuilder User** checkbox if you don't want to create it.

6 Leave the **Proceed to configuring client's IP pool** check box selected because you should assign at least one IP address to the user - otherwise the customer will not be able to host sites. Click **OK**.

7 Allocate IP addresses to the customer. Select the addresses you need from the **Vacant IPs** box and click **Add >>**. Keep in mind that e-commerce site hosting customers need dedicated (exclusive) IP addresses: one dedicated IP address per one site.

8 Click **OK**. You are now taken to the client account management screen.

This is the first screen with which your customer starts working when he or she is logged in to his or her control panel account. For this reason, this screen is referred to as Client Home page. To take a tour of the customer's control panel environment, you may want to log in to control panel under customer's credentials or you can read the Plesk Client's Guide to get more details.

9 Next, to provision your customer with resources, if you created the user account without using a template, click **Limits** in the **Tools** group.

10 Specify the following items:

- **Maximum number of domains**. Specify the total number of domain names/web sites your customer will be able to host on the server. This includes web sites hosted on this server, and domain forwarders that point to web sites hosted on other servers. Domain aliases (additional domain names for a site hosted on this server) and subdomains are counted separately and are not limited by this resource type.

- **Maximum number of domain aliases**. Specify the number of domain aliases your customer can use for his or her domains.

- **Maximum number of subdomains**. Specify the total number of subdomains that the customer will be able to host.

- **Disk space**. Specify the total amount of disk space in megabytes that is allocated to the customer. It includes disk space occupied by all files related to user's domains/web sites: web site contents, databases, applications, mailboxes, log files and backup files. This is the so-called soft quota: when it is exceeded, the user account and domain names/web sites are not suspended automatically, only the appropriate notices are sent to your and your customer's e-mail addresses and the resource overage is indicated by the icon 🟠 shown in your and your customer's control panels to the left of the user name (see the list of clients that opens when you click the **Clients** shortcut in the navigation pane) or domain name (see the list of domain names that opens when you click the **Domains** shortcut in the navigation pane).

- **MySQL databases quota** and **Microsoft SQL databases** quota. Specify the maximum disk space amount in megabytes that MySQL and Microsoft SQL Server databases respectively can occupy on a domains belonging to the customer.

- **Maximum amount of traffic**. Specify the amount of data in megabytes that can be transferred from the customer's web sites during a month. Once the limit is reached, the appropriate notices are sent to your and your customer's e-mail addresses and the resource overage is indicated by the corresponding icon 🟠 shown in the control panel to the left of the user name (see the list of clients that opens when you click the **Clients** shortcut in the navigation pane) or domain name (see the list of domain names that opens when you click the **Domains** shortcut in the navigation pane).

- **Maximum number of web users**. Specify the total number of personal web pages that your customer can host for other users under his or her domains. This service is mostly used in educational institutions that host non-commercial personal pages of their students and staff. These pages usually have web addresses like http://your-domain.com/~username.

- **Maximum number of additional Microsoft FrontPage accounts**. Specify the maximum number of additional Microsoft FrontPage accounts that the customer can create on his or her domains.

- **Maximum number of additional FTP accounts**. Specify the maximum number of additional FTP accounts that the customer can create on his or her domains.

- **Maximum number of MySQL databases** and **Maximum number of Microsoft SQL server databases**. Specify the maximum number of MySQL and Microsoft SQL Server databases respectively that the customer can create on his or her domains.

- **Maximum number of mailboxes**. Specify the total number of mailboxes that the customer can host on the server.

- **Mailbox quota**. Specify the amount of disk space in kilobytes that is allocated to each mailbox.

- **Total mailboxes quota**. Specify the total amount of disk space in megabytes available for all mailboxes on all domains belonging to the customer.

- **Maximum number of mail redirects**. Specify the total number of mail redirects that the customer can set up.

- **Maximum number of mail groups**. Specify the total number of mail groups that the customer can set up.

- **Maximum number of mail autoresponders**. Specify the total number of automatic responses that the customer can set up.

- **Maximum number of mailing lists**. Specify the total number of mailing lists that you customer can host on the server.

- **Maximum number of Java applications**. Specify the total number of Tomcat Java applications or applets that can be hosted on the server.

- **Maximum number of IIS application pools**. Specify the total number of dedicated IIS application pools that the customer can allocate between his or her domains.

- **Maximum number of shared SSL links**. Specify the total number of shared SSL links that the customer can use on his or her domains.

- **Maximum number of ODBC connections**. Specify the total number of ODBC connections that the customer can use on his or her domains.

- **Validity period**. Specify the term for a hosting account. At the end of the term, all customer's domains/web sites will be suspended, its Web, FTP and mail services will no longer be accessible to the Internet users, and the reseller and his or her customers (domain owners) will not be able to log in to the control panel. Accounts cannot be automatically renewed, therefore, in order to bring the hosted domain names/web sites back to operation, you will need to manually renew the user account.

11 Click **OK**.

12 To specify the operations that the customer will be able to perform through his or her control panel, if you created this user account without using a predefined user account template, click **Permissions** in the **Tools** group.

13 Grant the required permissions to the customer. Use **Select All** to select all permissions and **Clear All** to clear all permissions.

- **Access to control panel**. Specify whether the customer will be able to access the control panel for managing his or her account and sites.

- **Domain creation**. Specify whether the customer will be able to set up hosting accounts for new sites.

- **Physical hosting management**. Specify whether the customer will be able to set up hosting accounts, modify hosting account features and switch on or off support for programming and scripting languages.

- **System access management**. Specify whether the customer will be able to access to the system through Remote Desktop.

- **Hard disk quota assignment**. Specify whether the customer will be able to assign hard quotas on disk space for his or her own web sites and for web sites of his or her customers.

- **Subdomains management**. Specify whether the customer will be able to set up additional sites under his or her domains and allow his or her customers to do so.

- **Domain aliases management**. Specify whether the customer will be able to set up additional alternative domain names for his or her web sites and allow his or her users to do so.

- **Log rotation management**. Specify whether the customer will be able to adjust the cleanup and recycling of processed log filee for his or her sites.

- **Anonymous FTP management**. Specify whether the customer will be able to have an FTP directory where all users could download and upload files without the need to enter login and password. A web site should reside on a dedicated IP address in order to use anonymous FTP service.

- **FTP accounts management**. Specify whether the customer will be able to create and manage additional FTP accounts.

- **Scheduler management**. Specify whether the customer will be able to schedule tasks with the task scheduler. Scheduled tasks can be used for running scripts or utilities on schedule.

- **Domain limits adjustment**. Specify whether the customer will be able to change the limits for his or her web sites.

- **DNS zone management**. Specify whether the customer will be able to manage the DNS zones of his or her domains.

- **Java applications management**. Specify whether the customer will be able to install Tomcat Java applications and applets on web sites through the control panel.

- **Mailing lists management.** Specify whether the customer will be able to use mailing lists.

- **Spam filter management**. Specify whether the customer will be able to use spam filter provided by the SpamAssassin software.

- **Antivirus management**. Specify whether the customer will be able to use server-side antivirus protection for filtering incoming and outgoing mail.

- **Backup/restore functions**. Specify whether the customer will be able to use the control panel's facilities to backup and restore their site. Scheduled and on-demand backups are supported.

- **Ability to use remote XML interface**. Specify whether the customer will be able to remotely manage his or her web sites through custom applications. The XML interface can be used for developing custom applications integrated with web sites, which could be used, for instance, for automating setup of hosting accounts and provisioning of services for customers purchasing hosting services from your reseller's site.

- **SiteBuilder**. Specify whether the customer will be able to use SiteBuilder for creating and editing their web site.

- **Hosting Perfomance Management**. Specify whether the customer will be able to change the hosting performance preferences for their domain.

- **IIS Application Pool Management**. Specify whether the customer will be able to manage their IIS application pool.

- **Web statistics management**. Specify whether the customer will be able to manage web statistics for their domains.

- **Additional write/modify permissions management**. Specify whether the customer will be able to manage additional write/modify permissions for their domains. These permissions are required if customer's web applications are using a file-based database (like Jet) located in the root of `httpdocs` or `httpsdocs` folders. Please note that selecting this option might seriously compromise the web site security.

- **Shared SSL management**. Specify whether the customer will be able to manage shared SSL for their domains.

- **User interface**. Specify the type of user interface the customer will be able to use - standard, desktop, or both.

- **Desktop management**. Specify whether the customer will be able to customize his or her desktop interface.

- **Ability to select a database server**. Specify whether the customer will be able to select a database server of each type for creating his or her databases, not only use the default database server.

14 Click **OK**.

You can now tell your customer the URL to control panel and login credentials.

Modifying User Accounts

➢ *To add or remove an IP address from a customer's IP pool:*

1 Go to **Clients** and click the client name you need.

2 Click **IP pool**.

- To allocate an IP address, click **Add New IP Address**, select the address or addresses (to select multiple IP addresses, press and hold the **Control** button on the keyboard and left-click the required addresses) in the **Vacant IPs** box and click **OK**.

- To revoke an IP address, select the respective check box and click ✖ **Remove Selected**. Confirm removal and click **OK**.

- To assign an SSL certificate to an IP address, click the IP address you need, select the required certificate from the **SSL Certificate** drop-down box and click **OK**.

- To enable the ability to use secure FTP connection (FTP over SSL) for the domain, select the **FTP over SSL** check box. It is recommended to use exclusive IP addresses for this feature to work properly.

- To specify the web site that will open when users refer to the web resource on your server by an IP address (actual only for sites sharing the same IP address), click the number in the **Hosting** column, select the domain name you need, and click ⭐ **Set As Default**.

➢ *To update contact information or change password for access to control panel:*

1 Go to **Clients** and click the client name you need.

2 Click **Edit** in the **Tools** group.

3 Fill in the required information and click **OK**.

➢ *To change user's FTP password:*

1 Go to **Domains** and click the client name you need.

2 Click **Setup** in the **Hosting** group.

3 Type the new password into the **New FTP password** and **Confirm password** boxes.

4 Click **OK**.

➢ *To modify permissions for operations a customer can perform through the control panel:*

1 Go to **Clients** and click the client name you need.

2 Click **Permissions** in the **Tools** group.

3 Specify the required permissions and click **OK**.

➢ *To allocate more resources to the customer:*

1 Go to **Clients** and click the client name you need.

2 Click **Limits** in the **Tools** group.

3 Specify the resource allotments and click **OK**.

➢ *To change user account's preferences:*

1 Go to **Clients** and click the client name you need.

2 Click **Preferences** in the **Tools** group.

3 Specify the interface language, skin, interface customization templates.

4 If required, clear the **Prevent working with Plesk until page is completely loaded** and **Allow multiple sessions** checkboxes, and modify the creation or retention of SiteBuilder User by selecting or clearing the appropriate checkbox.

5 Click **OK**.

In this section:

Modifying Accounts for Your Resellers' Customers (Domain Administrators)

➢ *To allow your reseller's customer access the control panel:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Domain Administrator** in the **Domain** group.

4 Select the **Allow domain administrator access** check box, type the password for access to control panel (the domain administrator's login name is always his or her domain name), fill in the contact information and specify the operations the user will be able to perform through his control panel.

5 Click **OK**.

➢ *To update contact information or change password for access to control panel:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Domain Administrator** in the **Domain** group.

4 Fill in the required information and click **OK**.

➢ *To change user's FTP password:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Setup** in the **Hosting** group.

4 Type the new password into the **New FTP password** and **Confirm password** boxes.

5 Click **OK**.

➢ *To modify permissions for operations the site owner can perform through the control panel:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Domain Administrator** in the **Domain** group.

4 Specify the required permissions and click **OK**.

➢ *To allocate more resources to the site owner:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Limits** in the **Domain** group.

4 Specify the resource allotments and click **OK**.

> ➢ *To change user's control panel interface language and skin:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Domain Administrator** in the **Domain** group.

4 Specify the interface language, skin, interface customization templates and click **OK**.

To learn more information about modifying domain administrator accounts, refer to the Setting Up Hosting Account for a Web Site (on page 129) section.

Introducing Similar Changes to Numerous Hosting Accounts

> ➢ *To change hosting options for a number of hosting accounts at once:*

1 Select the required hosting accounts.

- Click the **Domains** shortcut in the navigation pane and select the check boxes corresponding to the required domains, if you want to change several domain administrator accounts at once.

    or

- Click the **Clients** shortcut in the navigation pane and select the check boxes corresponding to the required clients, if you want to change several client accounts at once.

2 Click **Group Operations**.

3 In the **Permissions** section (available only when editing client accounts), you can see the list of all client permissions. To change the availability of certain actions for the clients, select an appropriate radio-button to **Switch on**, **Switch off**, or **Do not change** to leave it as is.

4 In the **Limits** section, you can see the list of all hosting account limits. To change a certain limit, select an appropriate drop-down box on the left side of the list. Adjust the settings as required:

- Select **Unlimited** to remove the corresponding limit.

- Select **Value** and type the numeric value to set the corresponding limit to the specified value.

- Select **Increase (+)**, select the type of value (specific units or percentage) and type the numeric value to increase the corresponding limit by the specified value (in specific units or percents).

- Select **Decrease (-)**, select the type of value (specific units or percentage) and type the numeric value to decrease the corresponding limit by the specified value (in specific units or percents).

- Leave the **Do not change** value selected, to leave it as is.

5 In the **Hosting** section (available only when editing domain administrator accounts), you can see the list of hosting parameters. To change a certain feature availability for the domains, select an appropriate option button: **Switch on**, **Switch off**, or **Do not change** to leave it as is.

6 In the **Preferences** section, you can see the list of hosting account preferences. To set a certain preferences setting for the clients or domains, select an appropriate option button: **Switch on**, **Switch off**, or **Do not change** to leave it as is.

7 In the **Services** section (available only when editing domain administrator accounts), you can define the various domain services availability. To do this, select an appropriate option button: **Switch on**, **Switch off**, or **Do not change** to leave it as is.

8 Click **OK**.

Suspending and Unsuspending User Accounts

➢ *To suspend a user account and user's sites:*

1 Go to **Clients** and click the client name you need.

2 Click **Switch off** in the **Tools** group.

Access to control panel will be blocked for the user and his or her customers (site owners). User's domains/web sites will be suspended, their Web, FTP and mail services will no longer be accessible to the Internet users.

➢ *To unsuspend a user account and user's sites:*

1 Go to **Clients** and click the client name you need.

2 Click **Switch On** in the **Tools** group.

➢ *To suspend a domain administrator account with domain/web site:*

1 Go to **Domains** and click the client name you need.

2 Click **Switch off**.

The domain/web site will be suspended, its Web, FTP and mail services will no longer be accessible to the Internet users, and domain owner will not be able to log in to the control panel.

➢ *To unsuspend a domain administrator account with domain/web site:*

1 Go to **Domains** and click the client name you need.

2 Click **Switch On**.

Removing User Accounts

➢ *To remove a user account with user's Web sites:*

1 Click the **Clients** shortcut in the navigation pane.

2 Select a check box corresponding to the user account you want to remove and click ✖ **Remove Selected**.

3 Confirm removal and click **OK**.

The user account with all user's sites will be removed from the server.

➢ *To remove a site owner's account from the server:*

1 Click the **Domains** shortcut in the navigation pane.

2 Select the check box corresponding to the domain/Web site you wish to remove and click ✖ **Remove Selected**.

3 Confirm removal and click **OK**.

The domain administrator account and all data related to the domain/web site will be removed from the server.

Hosting Web Sites

In this section:

Predefining Content for New Web Sites

You can set your control panel to automatically include specific files and directories into Web spaces created for newly hosted Web sites. This can be a set of useful scripts, custom error messages, a placeholder index.html page, or any other files of your choice. These files can then be replaced, edited or removed on a per-site basis.

➢ *To set up the control panel so as to automatically include your web content into web spaces:*

1 On your local file system, create the required directories: `httpdocs`, `httpsdocs`, `cgi-bin`, `anon_ftp`, `error_docs`.

2 Place the files you need into the directories you have created: Place web pages into `httpdocs` and `httpsdocs` directories, scripts to `cgi-bin` directory, and custom error messages to `error_docs` directory.

3 Pack the directories and files into an archive file in rar, tgz, tar, gz, or zip format.

   Make sure that the directories are in the root of the archive file and not in a subdirectory.

4 Log in to your Plesk control panel.

5 Select the **Server** shortcut in the navigation pane.

6 Click **Skeleton** in the **Services** group.

7 Click **Browse** to locate the archive file on your local computer, select the file, and click **Send File**.

➢ *To revert back to the original structure of web server directories and files:*

1 Go to **Server** > **Skeleton**.

2 Click **Default**.

Obtaining Domain Names

Before you publish a site on the Internet, you must register your unique domain name with a domain name registration authority. A domain name is an easy-to-remember web site address.

When you want to visit a web site, you enter a domain name (e.g. your-domain.com) or a Uniform Resource Locator (e.g. http://www.your-domain.com) into your browser's address bar. In order to show you the requested site, your browser first needs to find out the IP address corresponding to the requested domain name because machines address each other by IP addresses—domain names were devised for humans. So, the browser queries the name servers in the distributed Domain Name System, which translates the requested domain name to IP address and returns the IP address to the browser. Finally, the browser connects to the web server at the specified IP address and retrieves the web pages from there. Thus, to allow other users to find your site by its domain name, you must register your domain name with the Domain Name System.

When choosing a domain name for your site, consider a word or combination of words that is relevant to your business, brand name, or topic of interest. A domain name should be easy to remember. If your domain name will comprise several words, you may want to separate these words with hyphens: this will help search engines distinguish between words, therefore, the users will be able to find your site faster.

To increase the chances to find your site for your customers, you may also want to buy the non-hyphenated version of the same domain name, for example, yourdomain.com and redirect it to your original domain - your-domain.com. To protect your domain name, you may want to register it in different top level domains: your-domain.com, your-domain.net. For a domain name comprising a single word that users can misspell and type incorrectly, you may also want to purchase one or few misspelled versions of your domain name that you will point to your original site. To give you a real life example of how this can be: there is the Google search engine with a primary web site address www.google.com. Knowing that people sometimes swap two adjacent letters or type more letters than required, the three additional domain names pointing to the original site were set up: www.gogle.com, www.goolge.com, and www.gooogle.com.

Once you have decided on the right domain name, you can register it with a domain name registration authority, or ask your service provider to do that for you. Registration cost varies among registrars (usually from 4 to 10 US dollars per year).

It is possible to register and manage domain names through Plesk, if your service provider enabled this option.

- To register a domain name through Plesk, click **Register** on your Home page. You will be taken to MyPlesk.com website, where a simple step-by-step wizard will guide you through the registration procedure.

- To manage domain names through Plesk, click **Manage** on your Home page. You will be taken to MyPlesk.com website, where you can log in and manage your domain names.

Setting Up Hosting Account for a Web Site

➢ *To host a web site on the server:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click **Add New Domain** in the **Tools** group.

3 Specify the domain name just as you have registered it. Leave the **www** check box selected if you wish to allow users to access your site by a common and habitual URL like www.your-domain.com.

   Having the www alias preceding your domain name will not cost you anything, but it will allow users to get to your site no matter what they type in their browsers: www.your-domain.com and your-domain.com will both point to your site.

4 If you have previously created a domain template and predefined all hosting features and resource usage allotments, select the required template from the **Select template** box.

5 If you have a number of IP addresses to choose from, select the required address from the **Select an IP address** drop-down box.

   Bear in mind that e-commerce sites need a dedicated IP address (not shared among other sites) to implement Secure Sockets Layer data encryption.

6 Make sure that there is a check mark in the **Proceed to hosting setup** check box and click **OK**.

7 Select the **Physical hosting** option to host the Web site on this machine and click **OK**.

   Upon completion of this procedure, your control panel will set up the domain name server on this machine to serve the new domain name and prepare the web server to serve the new Web site: a new zone file with appropriate resource records will be added to the Domain Name Server's configuration files, a web space will be created inside the Web server's directory, and necessary user accounts will be created on the server.

   Note: If your site is hosted on another machine, and you wish to set up your control panel's DNS server only to serve the DNS zone for that site, select either **Frame forwarding** or **Standard forwarding** option. With standard forwarding, a user is redirected to the site and the actual site's URL is shown in the user's browser, so the user always knows that he or she is redirected to another URL. With frame forwarding, a user is redirected to the site without knowing that the site actually resides at another location. For example: your customer has a free personal web site with his or her Internet Service Provider or a free Web host, and the Web site address is http://www.geocities.com/~myhomepage. The customer purchased a second level domain name www.myname.com and wants you to provide domain forwarding to his Web site. In this case you would normally choose the **Frame forwarding** service. See the section Serving Domain Names for Sites Hosted on Other Servers (Domain Forwarding) (on page 195) for details.

8 Specify the properties of a hosting account:

- **SSL support**. Secure Sockets Layer encryption is generally used for protecting transfer of sensitive data during online transactions on e-commerce Web sites that run on dedicated IP addresses. SSL certificates that participate in the encryption process are usually applied to a single domain name on a single IP address, therefore, each site that needs SSL protection must be hosted on a dedicated IP address. An exception to this is subdomains, which you can protect with a wildcard certificate. Installing an SSL certificate on a Web server that hosts several web sites with different domain names on a single IP address (shared or name-based hosting) is technically possible, however, it is not recommended: the encryption will be provided, but users will get warning messages on attempt to connect to the secure site. To allow SSL encryption for Web sites, select the **SSL support** check box.

- **FTP/Microsoft FrontPage Login** and **FTP/Microsoft FrontPage password**. Specify the user name and password that will be used for publishing the site to the server through FTP. Retype the password into the **Confirm Password** box.

- **Hard disk quota**. Specify the amount of disk space in megabytes allocated to the web space for this site. This is the so-called hard quota that will not allow writing more files to the web space when the limit is reached. At attempt to write files, users will get the "Out of disk space" error. Hard quotas should be enabled in the server's operating system, so if you see the "Hard disk quota is not supported" notice to the right of the **Hard disk quota** field, but would like to use the hard quotas, contact your provider or the server administrator and ask to enable the hard quotas.

- **Access to system**. This allows you to directly access the system through a Remote Desktop connection. However, allowing system access via RDP also poses a potential threat to the server security, so we recommend that you do not allow it, leaving the **Login prohibited** option selected.

- **SiteBuilder support.** SiteBuilder is an efficient and user-friendly WYSIWYG web site editor running through the web interface. Leave the **Publish site with SiteBuilder** checkbox selected to be able to access SiteBuilder and build web site through your Plesk control panel interface by clicking **SiteBuilder Wizard** on the domain management page or clicking the **Desktop** shortcut in the **SiteBuilder Admin** navigation pane group. The version of SiteBuilder coming in the standard Plesk distribution is fully functional and its use is not limited in any way by the manufacturer (but domain administrators can be restricted from accessing it).

- **Microsoft FrontPage support**. Microsoft FrontPage is a popular web site authoring tool. To enable publishing and modifying the site through Microsoft FrontPage, select the **Microsoft FrontPage support** and **Microsoft FrontPage over SSL support** check boxes, and set the **Remote Microsoft FrontPage authoring** option to **allowed**.

  Note. Microsoft FrontPage over SSL support is available only when SSL support is enabled on a domain.

- **Support for programming and scripting languages widely used in development of dynamic Web sites and server-side Web applications**. Specify which of the following programming and scripting languages should be interpreted, executed or otherwise processed by the web server: Active Server Pages (ASP), Active Server Pages on .NET framework (ASP.NET), Server Side Includes (SSI), PHP hypertext preprocessor (PHP), Common Gateway Interface (CGI), Fast Common Gateway Interface (FastCGI), Internet Server Application Programming Interface (ISAPI), Perl, Python, ColdFusion and Miva scripting required for running Miva e-commerce solutions.

> **Note.** You can change the version of ASP.NET and PHP you want to use in the corresponding drop-down menu. You can also specify the mode for running PHP applications - CGI, FastCGI or ISAPI.

- **Web statistics**. To allow you to view the information on the number of people visited the site and the pages of the site they viewed, select a module in **Web statistics** drop-down menu and select the **accessible via password protected directory /plesk-stat/** checkbox, if required. This will install the selected statistical software module, which will generate reports and place them into the password protected directory. The domain administrator will then be able to access Web statistics at the URL: https://your-domain.com/plesk-stat/ using their FTP account login and password.

   > **Note.** If domain administrator changes the FTP credentials, web statistics access credentials do not change. The original login and password specified upon the domain creation should always be used for accessing password-protected web statistics directory.

- **Custom error documents**. When visitors coming to your site request pages that the web server cannot find, the web server generates and displays a standard HTML page with an error message. If you wish to create your own error pages and use them on your web server, select the **Custom error documents** check box.

   > **Note.** You can enable the support for all programming and scripting languages, web statistics and custom error documents at once by selecting **All services** checkbox in the **Services** group.

- **Additional write/modify permissions**. This option is required if customer's web applications are using a file-based database (like Jet) located in the root of `httpdocs` or `httpsdocs` folders. Please note that selecting this option might seriously compromise the web site security.

- **Use dedicated IIS application pool.** This option enables the use of dedicated IIS application pool for your web applications. Using dedicated IIS application pool dramatically improves the stability of your web applications due to worker process isolation mode. This mode gives each web site hosted on the server 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. This is especially useful when you are using shared hosting package.

9 Click **OK**.

Now your server is ready to accommodate the new web site, and the site owner can publish the site to the server. For instructions on publishing a Web site, refer to the Publishing a Site (on page 136) section of this guide.

Note: If you transferred this domain name from another Web host, you will need to update the host DNS address with the domain name registrar so as to point to your name servers: log in to your registrar's web site, locate the forms used to manage the domain host pointers, and replace the current DNS host settings with your name servers' hostnames. The information on new name servers will spread across the DNS system within 48 hours.

If you have registered several domain names that you would like to point to a site hosted on this server, you should set up domain aliases. Refer to the Setting Up Additional Domain Names for a Site (Domain Aliases) (on page 171) section for details.

If you need to host several domains on your machine that will point to a site hosted on another server, you should set up domain forwarding. Refer to the Serving Domain Names for Sites Hosted on Other Servers (Domain Forwarding) (on page 195) section for details.

In this section:

Limiting the Amount of Resources a Site Can Consume

By default, new web sites that you set up without the help of domain templates, are allowed to consume unlimited amounts of bandwidth (data transfer) and disk space.

> ➢ *To limit the amount of resources this site can consume:*

1 Click the **Domains** shortcut in the navigation pane and click the required domain name in the list.

2 Click **Limits** in the **Domain** group.

3 Adjust the resource usage allotments as required:

1. **Maximum number of domain aliases**. Specify the number of domain aliases that can be used for this domain.

2. **Maximum number of subdomains**. Specify the number of subdomains that can be hosted under this domain.

3. **Disk space**. Specify the total amount of disk space allocated to a hosting account associated with the domain. This amount is measured in megabytes. It includes disk space occupied by all files related to this domain/web site: web site contents, databases, applications, mailboxes, log files and backup files. This is the so-called soft quota: when it is exceeded, domain names and web sites are not suspended automatically, only the appropriate notices are sent to your and your provider's e-mail addresses and the resource overage is indicated by the icon 🔔 shown in the control panel to the left of the domain name (see the list of domain names on your Home page). And then it is up to you to decide what to do with the domain:

   - you can notify the domain owner and suspend the domain/web site after a grace period until you receive the payment

     or

   - upgrade the hosting plan for your customer (see the Managing User Accounts (on page 114) chapter for more information).

1. **MySQL databases quota** and **Microsoft SQL databases** quota. Specify the maximum disk space amount that MySQL and Microsoft SQL Server databases respectively can occupy on a domain.

2. **Maximum amount of traffic**. Specify the amount of data in megabytes that can be transferred from the web site during a month. Once the limit is reached, the appropriate notices are sent to your and your provider's e-mail addresses and the resource overage is indicated by a corresponding icon shown in the control panel to the left of the domain name (see the list of domain names on your Home page). When a web site starts attracting more visitors and requires more bandwidth, consider upgrading a hosting plan (see the instructions on upgrading hosting plan below).

3. **Maximum number of web users**. Specify the number of personal web pages that the domain owner can host for other users under his or her domain. This service is mostly used in educational institutions that host non-commercial personal pages of their students and staff. These pages usually have web addresses like http://your-domain.com/~username. If you wish to allow execution of scripts embedded in personal web pages, select also the **Allow the web users scripting** check box.

4. **Maximum number of additional Microsoft FrontPage accounts**. Specify the maximum number of additional Microsoft FrontPage accounts that can be created on a domain.

5. **Maximum number of additional FTP accounts**. Specify the maximum number of additional FTP accounts that can be created on a domain.

6. **Maximum number of MySQL databases** and **Maximum number of Microsoft SQL server databases**. Specify the maximum number of MySQL and Microsoft SQL Server databases respectively that can be hosted on a domain.

7. **Maximum number of mailboxes**. Specify the number of mailboxes that can be hosted in a domain.

8. **Mailbox quota**. Specify the amount of disk space in kilobytes that is allocated to each mailbox in a domain.

9. **Total mailboxes quota**. Specify the total amount of disk space available for all mailboxes on a domain.

10. **Maximum number of mail redirects**. Specify the number of mail redirects that can be used in a domain.

11. **Maximum number of mail groups**. Specify the maximum number of mail groups that can be used in a domain.

12. **Maximum number of mail autoresponders**. Specify the number of automatic responses that can be set up in a domain.

13. **Maximum number of mailing lists**. Specify the number of mailing lists that the domain owner can run in a domain. To allow the use of mailing lists, you should also put a check mark into the **Mailing lists** check box under the **Preferences** group.

14. **Maximum number of Java applications**. Specify the maximum number of Tomcat Java applications and applets that the domain owner can install in a domain.

15. **Maximum number of ODBC connections**. Specify the maximum number of ODBC connections that can be set up on a domain.

16. **Validity period**. Specify the term for a hosting account. At the end of the term, the domain/web site will be suspended, its Web, FTP and mail services will no longer be accessible to the Internet users, and domain owner will not be able to log in to the control panel. Hosting accounts cannot be automatically renewed, therefore, in order to bring the hosted domain name/web site back to operation, you will need to manually renew the hosting account: on your Home page, click the domain name your need, click **Limits**, specify another term in the **Validity period** box, click **OK**, then click **Switch On** in the **Domain** group (**Home** > **domain name**).

4 Click **OK**.

Allowing the Site Owner to Log in to Control Panel

> ➢ *To allow the site owner to log in to control panel for managing his or her web site:*

1 Click the **Domains** shortcut in the navigation pane and click the required domain name in the list.

2 Click **Domain Administrator** in the **Domain** group.

3 Select the **Allow domain administrator's access** check box.

4 Type the password for access to the site owner's control panel.

For security reasons, the password should be more than 8 symbols, and it should comprise a combination of letters, numbers, and punctuation; dictionary words and proper names should be avoided.

5 Specify the settings related to the appearance of user's control panel, if desired: interface language, theme (skin), the limit on number of characters that can appear on custom buttons placed into the control panel by the site owner.

6 Leave the **Allow multiple sessions** check box selected to allow the site owner to have several simultaneous sessions in the control panel.

7 Leave the **Prevent users from working with the control panel until interface screens are completely loaded** check box selected.

This will forbid users from submitting data or performing operations until the control panel is ready to accept them.

8 Specify the operations that the site owner will be able to perform in his or her control panel:

- **Physical hosting management**. Allow or disallow full control of the hosting account and webspace.

- **Hard disk quota assignment**. Allow or disallow the site owner to adjust the hard quota on disk space allocated to their web space.

- **Subdomains management**. Allow or disallow the site owner to set up, modify and remove subdomains.

- **DNS zone management**. Allow or disallow the site owner to manage the DNS zone of his or her domain. This is recommended only for experienced users.

- **Log rotation management**. Allow or disallow the site owner to adjust the cleanup and recycling of processed log files.

- **Scheduler management**. Allow or disallow the site owner to schedule tasks with the Scheduler. Scheduled tasks can be used for running scripts or utilities on schedule.

- **Anonymous FTP management**. Allow or disallow the site owner to have an FTP directory where all users could upload and download files without the need to enter login and password. A web site should reside on a dedicated IP address in order to use anonymous FTP.

- **FTP accounts management.** Allow or disallow the site owner to create, modify and remove additional FTP accounts.

- **Java applications management**. Allow or disallow the site owner to install Tomcat Java applications and applets on the web site.

- **System access management**. Allow or disallow the site owner to access to the system through Remote Desktop.

- **Mailing lists management.** Allow or disallow the site owner to use mailing lists.

- **Backup/restore functions**. Allow or disallow the site owner to use the control panel's facilities to backup and restore their site. Scheduled and on-demand backups are supported.

- **Spam filter management**. Allow or disallow the site owner to use spam filter provided by the SpamAssassin software.

- **Antivirus management**. Allow or disallow the site owner to use server-side antivirus protection for filtering incoming and outgoing mail.

- **SiteBuilder**. Allow or disallow the site owner to use SiteBuilder for creating and editing their web site.

- **Hosting Perfomance Management**. Allow or disallow the site owner to change the hosting performance preferences for their web site.

- **IIS Application Pool Management**. Allow or disallow the site owner to manage their IIS application pool.

- **Web statistics management.** Allow or disallow the site owner to manage web statistics for their web site.

- **Additional write/modify permissions management.** Allow or disallow the site owner to manage additional write/modify permissions for their web site. These permissions are required if customer's web applications are using a file-based database (like Jet) located in the root of `httpdocs` or `httpsdocs` folders.

- **User interface**. Shows what type of Plesk control panel interface the site owner can use - standard, desktop, or both.

- **Desktop management**. Shows whether the site owner can customize and manage their desktop interface.

- **Ability to select a database server**. Specify whether the site owner will be able to select a database server of each type for creating his or her databases, not only use the default database server.

9 Specify the site owner's contact information.

10 Click **OK**.

Now you can tell your customer the control panel's URL, login and password. The URL is https://<user's_domain_name>:8443, where <user's_domain_name> is the domain name without the www alias. The login name that the site owner should specify in order to log in to the control panel is his or her domain name, for example, your-domain.com.

Publishing a Site

Publishing your site means uploading web pages, scripts and graphic files that compose your site to your web space in any of the following ways:

- Through FTP connection

- Through Plesk File Manager
- Through Microsoft FrontPage software (only for users of Microsoft Windows operating systems)
- Through Sitebuilder

FTP is one of the most common and easiest ways to upload files. You can secure your FTP connection by using FTP over SSL.

In this section:

Publishing Sites Through FTP

1 Connect to the server with an FTP client program, using FTP account credentials that you specified during setup of hosting account or obtained from your provider.

Enable the passive mode if you are behind a firewall.

2 Upload files and directories that should be accessible through HTTP protocol to the `httpdocs` directory, and files/directories that should be transferred securely over SSL protocol to the `httpsdocs` directory.

3 Place your CGI scripts into the `cgi-bin` directory.

4 Close your FTP session.

In this section:

Changing FTP Password

➢ *To change FTP password for a Web site owner:*

1 Go to **Domains** > *domain name* > **Setup**.

2 Specify new password and click **OK**.

Using Additional FTP Accounts

If you are working on your web site together with someone else or host subdomains for other users, you might want to create additional FTP accounts.

In this section:

Creating Additional FTP Accounts

➢ *To create a new additional FTP account:*

1 Click the **Domains** shortcut in the navigation pane and click the required domain name.

2 Click **FTP Accounts**.

3 On the **Additional FTP Accounts** tab, click **Add New FTP Account**.

4 Specify the **FTP account name** in the appropriate field.

5 Specify the **Home directory** by clicking 📁 and select the directory required. Alternatively, you can specify the path in the input field.

6 Type the new password into the **New password** and **Confirm password** boxes.

7 By default, the **Hard disk quota** is set to **Unlimited**. To set the required parameter, clear the **Unlimited** checkbox and type the amount of disk space in megabytes into the **Hard disk quota** box.

8 If required, select the **Read permission** checkbox. The FTP account users will be able to view the content of the home directory and download files from it.

9 If required, select the **Write permission** checkbox. The FTP account users will be able to create, view, rename and delete directories in the home directories.

If you don't grant any permissions, the connection to the FTP account will be made, but the home directory will be not displayed for users.

10 Click **OK**. A new FTP account will be added.

Changing Settings of Additional FTP Accounts

➢ *To change the properties of an additional FTP account:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name.

3   Click **FTP Accounts** in the **Hosting** group.

4   On the **Additional FTP Accounts** tab click the required FTP account name in the list.

5   Specify the changes as required and click **OK**.

Removing Additional FTP Accounts

➢ *To remove an additional FTP account:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name.

3   Click **FTP Accounts** in the **Hosting** group.

4   On the **Additional FTP Accounts** tab, select the checkbox corresponding to the FTP account name you want to remove and click ✖ **Remove Selected**.

5   Confirm removal and click **OK**. The FTP account will be removed.

Uploading Sites Through Plesk File Manager

1 Log in to Plesk control panel.

2 Click the **Domains** shortcut in the navigation pane.

3 Click the required domain name in the list.

4 Click **File Manager** in the **Hosting** group.

5 Create and upload files and directories.

Place the files and directories that should be accessible via HTTP protocol to the `httpdocs` directory, and files/directories that should be transferred securely over SSL protocol to the `httpsdocs` directory. Place your CGI scripts into the `cgi-bin` directory.

- To create a new directory within your current location, click **Add New Directory** in the **Tools** group, specify the directory name and click **OK**.

- To create new files in the required directory, click **Add New File** in the **Tools** group, in the **File creation** section specify the file name, select the **Use html template** check box, if you want file manager to insert some basic html tags to the new file, and click **OK**. A page will open allowing you to enter the content or html-formatted source of a new file. After you are done, click **OK**.

- To upload a file from the local machine, click **Add New File** in the **Tools** group, specify the path to its location in the **File source** box (or use **Browse** to locate the file), and click **OK**. You can upload up to 3 files at once through three separate **File Source** boxes. If you are uploading an archive file (.zip or .rar), select the corresponding **Upload archive and extract it** check box to extract the uploaded archive contents in the folder where the file was uploaded.

- To view or edit an existing file, click its name. When editing an HTML file, Plesk opens internal WYSIWYG editor by default. If you want to edit the source code of the HTML file, click **Html**. To return back to WYSIWYG mode, click **Design**.

When you upload web content through File Manager or FTP, your control panel automatically sets the appropriate access permissions for files and directories. To change the permissions of files and directories, click 🔒. For more information about the system of permissions, refer to the Setting File and Folder Access Permissions (on page 211) section.

To preview a Web page in your browser, click 🔁.

To rename a file or directory, click 🖥️. Type in a new name and click **OK**.

To copy or move a file or directory to another location, select the required file or directory using the appropriate check box, and click 📋 **Copy/Move**. Specify the destination for the file or directory to be copied or renamed to, then click **Copy** to copy, or **Move** to move it.

To update the file or directory creation date, click 🖼️ **Change Timestamp**. The time stamp will be updated with the current local time.

To calculate the size of selected files, select the checkboxes corresponding to the files which size you wish to see and click 📄 **Size**.

To remove a file or directory, select the corresponding check box, and click ✖ **Remove Selected**. Confirm removal and click **OK**.

Publishing from Microsoft FrontPage

Microsoft FrontPage deals with two kinds of Web sites: disk-based and server-based. In short, a disk-based site is a FrontPage Web site you create on your local hard disk and then later publish to a Web server. A server-based site is one you create and work with directly on a Web server, without the extra step of publishing. This section provides you with instructions on publishing only disk-based web sites.

You can publish disk-based web sites either through FTP or HTTP. If your server is running FrontPage Server Extensions, you would publish your site to an HTTP location. For example: http://your-domain.com/MyWebSite. If your server supports FTP, you would publish to an FTP location. For example: ftp://ftp.your-domain.com/myFolder.

After publishing, you can manage your site through FrontPage Server Extensions.

➢ *To access FrontPage Server Extensions management interface:*

1 Log in to Plesk.

2 Click the **Domains** shortcut in the navigation pane.

3 Click the required domain name in the list.

4 Click **FrontPage Management** in the **Hosting** group.

5 According to the **Microsoft FrontPage support** settings of the domain, one of the following icons will appear next to **Add New FrontPage Subaccount**:

- Click **FrontPage WebAdmin** to manage a site, which is not protected by SSL.

- Click **FrontPage-SSL WebAdmin** to manage an SSL-enabled site.

6 Type your FrontPage administrator's login name and password, and click **OK**.

For instructions on using FrontPage server extensions, see online help (**FrontPage WebAdmin** > **Help**) or visit Microsoft web site.

In this section:

Publishing from Microsoft FrontPage through FTP

> ➢ *To publish files through FTP:*

1   Open your FrontPage program.

2   Open a FrontPage Web site: open **File** menu and select the **Open Site** item.

3   Go to **Remote Web site** view: click the **Web Site** tab, and then the **Remote Web Site** button at the bottom of the window.

4   Set up your Remote Web Site Properties:

- Click the **Remote Web Site Properties** button in the upper-right corner of the window.

- Select **FTP** as the remote Web server.

- In the **Remote Web site location** box, type your host name (e.g., ftp://ftp.your-domain.com)

- In the **FTP directory** box, type your FTP directory if your hosting company provided one. Leave it blank if they did not specify one.

- Select the **Use Passive FTP** check box if your computer or network is protected by a firewall.

5   Click **OK** to connect to the remote site.

The Remote Web site view will show files that you have in your local and remote sites.

6   Click the **Publish Web site** button in the lower-right corner of the window.

Publishing from Microsoft FrontPage through HTTP

➢ *To publish files through HTTP on a server that supports FrontPage Server Extensions:*

1 Open your FrontPage program.

2 Open a FrontPage Web site: open **File** menu and select the **Open Site** item.

3 Go to **Remote Web site** view: click the **Web Site** tab, and then the **Remote Web Site** button at the bottom of the window.

4 Click the **Remote Web Site Properties** button in the upper-right corner of the window.

5 On the **Remote Web Site** tab, under **Remote Web server type**, click **FrontPage or SharePoint Services.**

6 In the **Remote Web site location** box, type the Internet address, including the protocol, of the remote Web site that you want to publish folders and files to — for example, http://www.your-domain.com — or click **Browse** to locate the site.

7 Do any of the following:

- To use Secure Sockets Layer (SSL) for establishing a secure communications channel to prevent the interception of critical information, click **Encryption connection required (SSL)**. To use SSL connections on your Web server, the server must be configured with a security certificate from a recognized certificate authority. If the server does not support SSL, clear this check box. Otherwise, you will not be able to publish folders and files to the remote Web site.

- To remove specific types of code from Web pages as they are being published, on the **Optimize HTML** tab, select the options you want.

- To change the default options for publishing, on the **Publishing** tab, select the options you want.

8 Click **OK** to connect to the remote site.

The **Remote Web site** view will show files that you have in your local and remote sites.

9 Click the **Publish Web site** button in the lower-right corner of the window.

Using Additional Microsoft FrontPage Accounts

If you are working on your web site together with someone else or host subdomains for other users, you might need to create additional Microsoft FrontPage accounts.

In this section:

Creating Additional Microsoft FrontPage Accounts

➢ *To create an additional Microsoft FrontPage account for a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **FrontPage Management** in the **Hosting** group.

4 Click **Add New FrontPage Account**.

5 Specify the login and password for this account.

6 If you wish to limit the amount of disk space that can be used by this account, clear the **Unlimited** checkbox and type the desired value in megabytes into the **Hard disk quota** box.

   When the specified limit is exceeded, the account owner will not be able to add files to his or her web space.

7 Click **OK** to finish the creation of an additional Microsoft FrontPage account.

Changing Settings of Additional Microsoft FrontPage Accounts

➢ *To change settings for an additional Microsoft FrontPage account:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **FrontPage Management** in the **Hosting** group.

4 Click the required account in the list.

5 Adjust the settings as necessary and click **OK** to save changes.

Removing Additional Microsoft FrontPage Accounts

➢ *To remove an additional Microsoft FrontPage account:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **FrontPage Management** in the **Hosting** group.

4 Select the checkbox corresponding to the account you wish to remove.

5 Click ✖ **Remove Selected**.

6 Confirm the removal and click **OK**.

Changing Microsoft FrontPage Settings

If you want Microsoft FrontPage to use its own IIS Index Server to build the full-text index of your Web site.

➢ *To make Microsoft FrontPage use its own IIS Index Server:*

1 Go to **Domains** > **domain name** > **FrontPage Management** > **Preferences**.

2 Select **Use the IIS Index Server** check box and click **OK**.

> If you use FrontPage forms that submit information by e-mail on your site, you may want to specify the following preferences:

▪ **SMTP mail server that will be used for sending mail.** By default, SMTP server specified in the domain's DNS zone is used for sending mail. If no SMTP server is specified in the zone, then FrontPage uses the mail service running on the server where the domain (site) is hosted.

▪ **Sender's e-mail address.** By default, domain owner's e-mail address is used. If the domain owner's e-mail address is not specified in domain owner's profile, then FrontPage uses the e-mail address of the client, to whom the domain belongs. If the client's e-mail address is not specified in the client's profile, then the server administrator's e-mail address is used.

➢ *To change the preferences:*

1 Go to **Domains** > **domain name** > **FrontPage Management** > **Preferences**.

2 Under **Mail Settings** specify the SMTP server and the e-mail address you want to use, and then click **OK**.

Publishing Sites with Sitebuilder

> *To publish a Web site with Sitebuilder:*

1 Log in to your control panel.

2 Click the required domain name in the list.

3 Click **Setup** and check whether **Publish site with Sitebuilder** check box is selected. Click **OK** to return to the domain page.

4 Click **Sitebuilder Wizard**.

5 After Sitebuilder is loaded, follow the instructions provided in Sitebuilder documentation to publish the Web site. You can find Sitebuilder documentation at http://www.parallels.com/en/products/sitebuilder/win/docs/ (http://www.parallels.com/en/products/sitebuilder3win/docs).

To access Sitebuilder Wizard for a domain, you can also click the corresponding button in the list of domains.

Previewing a Site

Once you published a site on the server, you may want to make sure that it functions properly in the actual hosting environment. You can preview the site through your favorite Web browser, even if the information on the domain name has not yet propagated in the Domain Name System. Note that Adobe Flash and CGI scripts will not work during preview. Also, site preview does not work for Web sites and Web pages that include absolute paths to other files (like <a href="http://domain.tld/image.gif">).

> *To preview a site:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Site Preview** in the **Hosting** group.

Configuring ASP.NET

ASP.NET is a flexible set of tools and web development technologies that allows you to employ a number of applications based on ASP.NET framework. Plesk supports both 1.1.x and 2.0.x versions of the .NET framework and allows configuring most of its settings.

In this section:

Configuring ASP.NET for Domains

Most ASP.NET configuration settings that commonly need to be customized in order for ASP.NET applications to function in a desirable way can be edited through Plesk.

➢ *To configure ASP.NET for a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **ASP.NET** in the **Hosting** group.

4 Set up the strings that determine database connection data for ASP.NET applications which use databases. This option is available only for ASP.NET 2.0.x.

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

▪ To add a string, enter the required data into the **Name** and **Connection Parameters** input fields and click ⊕ next to them.

▪ To remove a string, click ⊖ next to it.

5 Set up custom error messages that will be returned by ASP.NET applications in the **Custom Error Settings** field:

▪ To set the custom error messages mode, select an appropriate option from the **Custom error mode** menu:

   ▪ **On** - custom error messages are enabled.

   ▪ **Off** - custom error messages are disabled and detailed errors are to be shown.

   ▪ **RemoteOnly** - custom error messages are displayed only to remote clients, and ASP.NET errors are shown to the local host.

▪ To add a new custom error message (which will be applied unless the **Off** mode was selected), enter the values in the **Status Code** and **Redirect URL** fields, and click ⊕.

   ▪ **Status Code** defines the HTTP status code resulting in redirection to the error page.

   ▪ **Redirect URL** defines the web address of the error page presenting information about the error to the client.

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

▪ To remove a custom error message from the list, click ⊖ next to it.

6 Configure compilation settings in the **Compilation and Debugging** field:

▪ To determine the programming language to be used as default in dynamic compilation files, choose an entry from **Page default language** list.

▪ To enable compiling retail binaries, leave the **Switch on debugging** checkbox empty.

- To enable compiling debug binaries, select the **Switch on debugging** checkbox. In this case, the source code fragments containing error will be shown in a diagnostic page message.

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

7 Configure encoding settings for ASP.NET applications in the **Globalization Settings** section:

- To set an adopted encoding of all incoming requests, enter an encoding value into the **Request encoding** field (default is utf-8).

- To set an adopted encoding of all responses, enter an encoding value into the **Response encoding** field (default is utf-8).

- To set an encoding which must be used by default for parsing of `.aspx`, `.asmx`, and `.asax` files, enter an encoding value into the **File encoding** field (default is Windows-1252).

- To set a culture which must be used by default for processing incoming web requests, select an appropriate item from the **Culture** list.

- To set a culture which must be used by default when processing searches for a locale-dependent resource, select an appropriate item from the **UI Culture** list.

8 Set a code access security trust level for ASP.NET applications in the **Code Access Security** field.

CAS trust level is a security zone to which applications execution is assigned, defining what server resources the applications will have access to.

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

9 Enable the usage of the auxiliary scripts in the **Script Library Settings** field. Specifying the script library settings is necessary if the validation web controls are used on your web site. This option is available only for ASP.NET 1.1.x.

- If you need to use auxiliary scripts (specifically, scripts implementing objects for validating input data), provide the settings for .NET framework script library. To do so, enter the path beginning with the domain root directory preceded by the forward slash into the **Path to Microsoft script library** field, or click the folder icon next to the **Path to Microsoft script library** field and browse for the required location.

- To initiate the auto-installation of files containing the scripts to the specified location, select the **Install** checkbox. If the files already exist there, they will be rewritten.

10 Set client session parameters in the **Session Settings** field:

- To set up the default authentication mode for applications, select an appropriate item from the **Authentication mode** list. **Windows** authentication mode should be selected if any form of IIS authentication is used.

- To set up time that a session can idle before it is abandoned, enter appropriate number minutes into the **Session timeout** field.

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

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

Configuring ASP.NET for Virtual Directories

To improve the performance of ASP.NET-based web applications, Plesk allows using individual settings of .NET framework per virtual directory.

> ➢ *To configure ASP.NET for a virtual directory:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories**.

4 Browse to the required directory and enter it.

5 Click **ASP.NET**.

6 Set up the strings that determine database connection data for ASP.NET applications which use databases. This option is available only for ASP.NET 2.0.x.

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

   ▪ To add a string, enter the required data into the **Name** and **Connection Parameters** input fields and click 🟢 next to them.

   ▪ To remove a string, click 🔴 next to it.

7 Set up custom error messages that will be returned by ASP.NET applications in the **Custom Error Settings** field:

   ▪ To set the custom error messages mode, select an appropriate option from the **Custom error mode** menu:

     ▪ **On** - custom error messages are enabled.

     ▪ **Off** - custom error messages are disabled and detailed errors are to be shown.

     ▪ **RemoteOnly** - custom error messages are displayed only to remote clients, and ASP.NET errors are shown to the local host.

   ▪ To add a new custom error message (which will be applied unless the **Off** mode was selected), enter the values in the **Status Code** and **Redirect URL** fields, and click 🟢.

     ▪ **Status Code** defines the HTTP status code resulting in redirection to the error page.

     ▪ **Redirect URL** defines the web address of the error page presenting information about the error to the client.

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

   ▪ To remove a custom error message from the list, click 🔴 next to it.

8 Configure compilation settings in the **Compilation and Debugging** field:

- To determine the programming language to be used as default in dynamic compilation files, choose an entry from **Page default language** list.

- To enable compiling retail binaries, leave the **Switch on debugging** checkbox empty.

- To enable compiling debug binaries, select the **Switch on debugging** checkbox. In this case, the source code fragments containing error will be shown in a diagnostic page message.

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

9 Configure encoding settings for ASP.NET applications in the **Globalization Settings** section:

- To set an adopted encoding of all incoming requests, enter an encoding value into the **Request encoding** field (default is utf-8).

- To set an adopted encoding of all responses, enter an encoding value into the **Response encoding** field (default is utf-8).

- To set an encoding which must be used by default for parsing of `.aspx`, `.asmx`, and `.asax` files, enter an encoding value into the **File encoding** field (default is Windows-1252).

- To set a culture which must be used by default for processing incoming web requests, select an appropriate item from the **Culture** list.

- To set a culture which must be used by default when processing searches for a locale-dependent resource, select an appropriate item from the **UI Culture** list.

10 Set a code access security trust level for ASP.NET applications in the **Code Access Security** field.

CAS trust level is a security zone to which applications execution is assigned, defining what server resources the applications will have access to.

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

11 Enable the usage of the auxiliary scripts in the **Script Library Settings** field. Specifying the script library settings is necessary if the validation web controls are used on your web site. This option is available only for ASP.NET 1.1.x.

- If you need to use auxiliary scripts (specifically, scripts implementing objects for validating input data), provide the settings for .NET framework script library. To do so, enter the path beginning with the domain root directory preceded by the forward slash into the **Path to Microsoft script library** field, or click the folder icon next to the **Path to Microsoft script library** field and browse for the required location.

- To initiate the auto-installation of files containing the scripts to the specified location, select the **Install** checkbox. If the files already exist there, they will be rewritten.

12 Set client session parameters in the **Session Settings** field:

- To set up the default authentication mode for applications, select an appropriate item from the **Authentication mode** list. **Windows** authentication mode should be selected if any form of IIS authentication is used.

- To set up time that a session can idle before it is abandoned, enter appropriate number minutes into the **Session timeout** field.

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

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

Restoring Default ASP.NET Configuration

➢ *To restore the default ASP.NET configuration:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **ASP.NET** in the **Hosting** group.

4 Click **Set to Default**.

5 Confirm the restoring and click **OK**.

Changing .NET Framework Version for Domains

Since Plesk supports both 1.1.x and 2.0.x versions of the .NET framework, it is possible to choose the version used by your domains on a per-domain basis.

➢ *To change the version of .NET framework used by a domain:*

1   Click the **Domains** shortcut in the navigation pane.
2   Click the required domain name in the list.
3   Click **ASP.NET** in the **Hosting** group.
4   Click **Change Version** in the **Tools** group. If this button is absent, only one version of .NET framework is available. You can see the version number in the **Framework Version** field.
5   Select the required version number and click **OK**.
6   Click **OK** to save changes.

> Alternatively, on your home page you can click the domain name you need, then click **Setup** and select the .NET framework version in the **Microsoft ASP.NET support** drop-down menu.

Changing .NET Framework Version for Virtual Directories

In order to provide running ASP.NET applications which use different .NET framework versions within one domain, Plesk allows setting up the framework version per virtual (web) directory, where the applications are deployed.

➢ *To choose the version of .NET framework for a virtual (web) directory:*

1   Click the **Domains** shortcut in the navigation pane.
2   Click the required domain name in the list.
3   Click **Web Directories** in the **Hosting** group.
4   Enter the required web directory and click **ASP.NET** in the **Tools** group.
5   Select the required .NET framework version and adjust other settings as necessary.
6   Click **OK**.

Setting PHP Version for a Domain

➢ *To set PHP version for a domain:*

1   Click the **Domains** shortcut in the navigation pane.
2   Click the required domain name in the list.
3   Click **PHP Settings**.
4   Choose the required version of PHP and click **OK**.

Deploying Databases

If your web server incorporates data processing applications or is designed to generate web pages dynamically, your clients will most likely need a database for storing and retrieving data. You can either create a new database for their sites or import the data from your previously backed up MySQL or Microsoft SQL database.

In this section:

Creating and Importing Databases

> ➢ *To create a new database on your hosting account:*

1 Go to **Domains** > *domain name* > **Databases** and click **Add New Database**.

2 Enter a name for the database.

We recommend that you choose a name that starts with a Latin alphabet symbol and comprises only alphanumeric and underscore symbols (up to 64 symbols).

3 Select the database type that you are going to use: **MySQL** or **Microsoft SQL Server**.

4 Select the database server of the selected type from the list. Click **OK**.

5 To set up database administrator's credentials, click **Add New Database User**.

6 Type a user name and a password that will be used for accessing the contents of the database.

7 Click **OK**.

> ➢ *To import an existing database:*

1 Go to **Domains** > *domain name* > **Databases** and click **Add New Database**.

2 Enter a name for the database. We recommend that you choose a name that starts with a Latin alphabet symbol and comprises only alphanumeric and underscore symbols (up to 64 symbols).

3 Select the database type that you are going to use: **MySQL** or **Microsoft SQL Server**.

4 Select the database server of the selected type from the list. Click **OK**.

5 To set up database administrator's credentials, click **Add New Database User**.

6 Type a user name and a password that will be used for accessing the contents of the database. Click **OK**.

7 Click **WebAdmin** in the **Tools** group. An interface to phpMyAdmin (or ASPEnterpriseManager) database management tool will open in a separate browser window.

If you have a MySQL database:

1. Click **Query window** in the left frame, click the **Import files** tab,

2. Select the text file that contains the data and click **Go**.

3. Click the **Insert data from a text file** link.

If you have a MS SQL database:

1. Click the name of your database in the left frame

2. Click **Query** (the magnifying glass button)

3. Copy the text of your script into the text area and click **Run Query**.

To manage your databases and their contents, use your favorite MySQL or Microsoft SQL Server client or the web based database management tool accessible from Plesk control panel (**Domains** > *domain name* > **Databases** > **Database name** > **WebAdmin**).

Creating Database User Accounts

If you collaborate with other people on managing a web site and wish to give them access to the database, you should create separate user accounts for them.

➢ *To create a database user account:*

1 Go to **Domains** > *domain name* > **Databases** > *database name* and click **Add New Database User**.

2 Type a user name and a password that will be used for accessing the contents of the database. Click **OK**.

Changing Database User Passwords

➢ *To change password for a database user:*

1 Go to **Domains** > *domain name* > **Databases** > *database name* > *database user name*.

2 Type a new password and click **OK**.

Removing Database User Accounts

➢ *To remove a database user account:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Databases** in the **Services** group.

4 Click the required database name. A list of database users will open.

5 Select a check box corresponding to the user account that you wish to remove.

6 Click ✖ **Remove Selected**. Next, confirm removing and click **OK**.

Removing Databases

> ➢ *To remove a database with its contents:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Databases** in the **Services** group.

4 Select a check box corresponding to the database that you wish to remove.

   If the required check box appears grayed out, this means that this database is used by a site application and you can remove it only by uninstalling the respective application.

5 Click ✖ **Remove Selected**.

6 Confirm removal and click **OK**.

Accessing Data From External Databases

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

In this section:

Creating Connections to External Databases by Installing New ODBC Drivers

To let your web applications use external databases for storing the data, you need to create connections to these external databases by installing appropriate ODBC drivers.

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

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **ODBC Data Sources** in the **Services** group.

4 Click **Add New ODBC DSN**.

5 Specify the ODBC connection name and description in the corresponding fields.

6 Select the required driver in the **Driver** field.

7 Click **OK**.

8 Choose the appropriate options on the driver configuration screen. Typically, you should specify the path to the database, user credentials and other connection options, depending on the selected driver.

9 Click **Test** to check whether the connection will function properly with provided settings. Click **Finish** to complete the creation.

Changing Settings Of Existing ODBC Connections

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

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **ODBC Data Sources** in the **Services** group.

4 Click the required connection name in the list.

5 Change the settings as needed.

6 Click **Test** to check whether the connection will function properly with new settings. Click **Finish** to save changes.

Removing Connections to External Databases

> ➢ *To remove a redundant ODBC connection:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **ODBC Data Sources** in the **Services** group.

4   Select the checkbox corresponding to a connection you want to remove.

5   Click ✖ **Remove Selected**, confirm the removal and click **OK**.

Configuring Data Source Names for Adobe ColdFusion

If you are using Adobe ColdFusion, you can configure data source names (DSNs) for ColdFusion through Plesk. Data name sources allow your ColdFusion web applications to use local and remote databases for processing and storing application data.

In this section:

Creating a New Data Source Name

> ➢ *To create a new Data Source Name for Adobe ColdFusion on a domain:*

1   Go to **Domains** > *domain name* > **ColdFusion DSN** and click **Add New ColdFusion DSN**.

2   Specify the data source name and select the required driver for this data source in the **Driver** menu. **Click Next >>**.

3   Choose the appropriate options on the driver configuration screen. Typically, you should specify the path to the database, user credentials and other connection options, depending on the selected driver. Refer to Adobe ColdFusion documentation for more information on the driver configuration options.

4   Click **OK** to finish.

Changing Settings of a Data Source Name

➢ *To change the settings Data Source Name for Adobe ColdFusion on a domain:*

1 Go to **Domains** > *domain name* > **ColdFusion DSN** and click the required data source name in the list.

2 Specify the data source name and select the required driver for this data source in the Driver menu. Click **Next >>**.

3 Choose the appropriate options on the driver configuration screen. Typically, you should specify the path to the database, user credentials and other connection options, depending on the selected driver. Refer to Adobe ColdFusion documentation for more information on the driver configuration options.

4 Click **OK**.

Removing a Data Source Name

➢ *To remove a redundant ColdFusion DSN connection:*

1 Go to **Domains** > *domain name* > **ColdFusion DSN**.

2 Select the check box corresponding to a DSN connection you want to remove.

3 Click ✖ **Remove Selected**, confirm the removal and click **OK**.

Installing Applications

To enhance a web site with valuable features, such as guest books, forums, hit counters, photo galleries, and e-commerce solutions, you can install the respective applications from Plesk web application library (**Domains** > *domain name* > **Web Applications**).

➢ *To install an application on your site:*

1 Go to **Domains** > *domain name* > **Web Applications** and click **Install New Application**.

2 In the left menu, select a category to which the application you need belongs.

3 Select the required application in the list, and then click ![icon] **Install**.

4 Some applications will display a license agreement. Read the license agreement carefully, and if you agree with it, select the **I agree** check box and click **Next >>**.

5 Specify whether you wish to create a hyperlink to the application and place it in the control panel.

6 Specify the installation preferences and other information that may be required by the application (the requirements may vary among applications). When finished, click **Install**.

After the application was installed, you can insert a link to this application into the web pages of your site, for example, on your home page. Otherwise, you and your users will have to access this application by typing its URL, which can be too long to remember.

➢ *To access the web interface of an application, do any of the following:*

▪ Type the URL in your browser. For example: http://your-domain.com/forum/.

▪ Go to **Domains** > *domain name* > **Web Applications** and click ![icon] corresponding to the application you need.

▪ If you chose to add a hyperlink button to your Plesk control panel during installation of an application, then click the respective button on the domain administration screen (**Domains** > *domain name*) or navigation pane.

➢ *To reconfigure an application, change the application administrator's password, or to install a license key for a commercial application:*

1 Go to **Domains** > **domain name** > **Web Applications**.

2 Click an icon ![icon] corresponding to the application.

➢ *To upgrade an application to a newer version (if it is available on the server):*

1 Go to **Domains** > **domain name** > **Web Applications**.

2 Click a corresponding shortcut in the **U** column.

➢ *To uninstall an application:*

1 Go to **Domains** > *domain name* > **Web Applications**, and select a check box corresponding to the application that you no longer need.

2 Click ✖ **Remove Selected**, confirm the removal and click **OK**. The application will be uninstalled and its databases removed from the server.

If you want a certain Web-application to be started when someone tries to enter a domain, it can be done by creating a default domain application.

➢ *To set an application as default for a domain:*

1 Go to **Domains** > *domain name* > **Web Applications.**

2 Select a check box corresponding to Web Application you want to set as default and click ☑ **Default**. Click **OK** to confirm.

Now, when a user enters an URL in the address field of his browser (e.g. http://example.com), he is taken to the default Web-application.

In this section:

Installing Java Web Applications

You can install Java Web application packages in the Web archive format (WAR). These Java applications are not distributed with Plesk, therefore you should obtain them separately.

➢ *To install a Java Web application:*

1 Go to **Domains** > *domain name* > **Web Applications** > **Java Applications** tab and click **Switch On**.

This will start the Tomcat service, which provides an environment for Java code to run in cooperation with a web server.

2 Click **Install New Application**.

3 Specify the path to an application package you wish to install (this can be an application package in WAR format saved on your computer's hard drive), or click **Browse** to navigate to it, then click **OK**.

Now the application is installed and the respective entry is added to the list of installed Java applications (**Domains** > *domain name* > **Web Applications** > **Java Applications**).

➢ *To access the web interface of a Java Web application, do any of the following:*

▪ Go to **Domains** > *domain name* > **Web Applications** > **Java Applications** tab, and click a respective hyperlink in the **Path** column.

▪ Type the URL in your browser. For example: http://your-domain.com:9080/storefront/.

➢ *To stop, start or restart a Java Web application:*

1 Go to **Domains** > *domain name* > **Web Applications** > **Java Applications** tab. A list of installed applications will open.

2 Locate an application on the list, and use the icons in the right part of the list to perform the required operations:

▪ To start an application, click the icon .

▪ To stop an application, click the icon .

▪ To restart an application, click the icon .

➢ *To uninstall a Java Web application:*

1 Go to **Domains** > *domain name* > **Web Applications** > **Java Applications** tab.

2 Select a check box corresponding to the application that you no longer need. Click **Remove Selected**, confirm the removal and click **OK**.

The application will be uninstalled and its databases removed from the server.

Installing ASP.NET Web Applications

In addition to the applications from the Application Vault and Java Web Applications, you can install ASP.NET Web application packages provided with Plesk.

➢ *To install an application on your site:*

1 Go to **Domains** > *domain name* > **Web Applications** > **ASP.NET 1.1 Applications**.

A list of ASP.NET 1.1 web applications installed on your site will be displayed.

2 Click **Install New Application** in the **Tools** group. A list of site applications available for installation will be displayed. To specify which application you wish to install, select a radio button corresponding to the application of your choice.

3 Click ⚙ **Install**.

4 Specify the domain folder in which the application should be installed, database name for the application, and click **Install**.

Now the application is installed and you can insert a link to this application into the web pages of your site, for example, on your home page. Otherwise, you and your users will have to access this application by typing its URL, which can be long enough to remember.

➢ *To access the web interface of an application, do any of the following:*

▪ Type the URL in your browser. For example: http://your-domain.com/forum/.

▪ Go to **Domains** > *domain name* > **Web Applications** > **ASP.NET 1.1 Applications**, and click an icon ➡, corresponding to the application.

➢ *To reconfigure an application or change the application administrator's password:*

Go to **Domains** > *domain name* > **Web Applications** > **ASP.NET 1.1 Applications**, and click an icon ⚙, corresponding to the application.

➢ *To uninstall an application:*

1 Go to **Domains** > *domain name* > **Web Applications** > **ASP.NET 1.1 Applications**, and select a check box corresponding to the application that you no longer need.

2 Click ✖ **Remove Selected**. The application will be uninstalled and its databases removed from the server.

If you want a certain Web-application to be started when someone tries to enter a domain, it can be done by creating a default domain application.

➢ *To set an application as default for a domain:*

1 Go to **Domains** > *domain name* > **Web Applications** > **ASP.NET 1.1 Applications**.

A list of application packages installed on the site will be displayed.

2 Select a checkbox corresponding to the application package you want to set as default, then click ☑ **Default**. Click **OK** to confirm the creation of the default Site Application.

Now, when a user enters an URL in the address field of his browser (e.g. http://example.com), he is taken to the default Web-application.

Using IIS Application Pool

IIS Application Pool contains all web applications on domains hosted on your server. Dedicated IIS application pool allows your clients to have a level of isolation between web applications used by their domains. Since each dedicated application pool runs independently, errors in one application pool belonging to one client will not affect the applications running in other application pools belonging to other clients.

By default, Plesk offers a shared application pool for all your clients and their customers. However, clients and domains can use dedicated application pools if administrator and client policy permit this.

➢ *To stop all applications in the domain's application pool:*

1   Click the **Domains** shortcut in the navigation pane and click the required domain name.

2   Click **IIS Application Pool**.

3   Click **Stop**.

➢ *To start all applications in the domain's application pool:*

1   Click the **Domains** shortcut in the navigation pane and click the required domain name.

2   Click **IIS Application Pool**.

3   Click **Start**.

➢ *To restart all applications running in the domain's application pool:*

1   Click the **Domains** shortcut in the navigation pane and click the required domain name.

2   Click **IIS Application Pool**.

3   Click **Recycle**. This can be handy if some applications are known to have memory leaks or become unstable after working for a long time.

In this section:

Setting Up IIS Application Pool

➢ *To enable IIS application pool for a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **IIS Application Pool**.

4 Click **Switch On**.

5 To limit the amount of CPU resources that this domain's application pool can use, select the **Switch on CPU monitoring** checkbox and provide a number (in percents) in the **Maximum CPU use (%)** field.

6 Click **OK**.

➢ *To enable IIS application pool for all domains of a specific client:*

1 Click the **Clients** shortcut in the navigation pane.

2 Click the required client name in the list.

3 Click **IIS Application Pool**.

4 Click **Switch On**.

5 To limit the amount of CPU resources that the application pool can use for all your domains, select the **Switch on CPU monitoring** checkbox and provide a number (in percents) in the **Maximum CPU use (%)** field.

6 Click **OK**.

Disabling IIS Application Pool

> ➢ *To disable IIS application pool for a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **IIS Application Pool**.

4 Click **Switch off**.

5 Click **OK**.

> ➢ *To disable IIS application pool for all domains of a specific client:*

1 Click the **Clients** shortcut in the navigation pane.

2 Click the required client name in the list.

3 Click **IIS Application Pool**.

4 Click **Switch Off**.

5 Click **OK**.

Organizing Site Structure with Subdomains

Subdomains are additional domain names that enable you to:

▪ Organize logically the structure of your site

▪ Host additional Web sites or parts of a Web site on the same server without the need to pay for registration of additional domain names

An example of using subdomains:

You have a Web site your-product.com dedicated to promoting your software product. For publishing user's guides, tutorials and list of frequently asked questions, you can organize the subdomain 'userdocs' so that your users will be able to access online user documentation directly by visiting the domain name userdocs.your-product.com.

In this section:

Setting Up Subdomains

➢ **To set up a subdomain:**

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Subdomains**.

4 Click **Add New Subdomain**.

5 Select the required **Hosting type** and click **OK**:

▪ Select **Physical hosting** to create a virtual host for the domain.

▪ Select **Subdomain on subfolder** to create a virtual subdomain. **Subdomain on subfolder** will use physical structure of the domain. The creation of a separate FTP user account will be not possible: the FTP user account of the domain will be used.

6 Type the subdomain name as required. This can be, for example, a topic of a site, organization department, or any other combination of letters, numbers and hyphens (up to 63 characters in length). To add the **WWW** prefix, select the appropriate checkbox.

The subdomain name must begin with an alphabet character. Subdomain names are case insensitive.

7 If you are creating subdomain on subfolder, specify the physical location for the subdomain files in the **Site home directory** field:

▪ Clear the **Create physical directory for subdomain** checkbox and specify the existing directory to the right of **httpdocs** field. You can click 📁 to browse for the required directory, select it and click **OK**.

▪ Leave the **Create physical directory for subdomain** checkbox selected to create a corresponding physical directory with the same name as the subdomain.

8 If you are creating subdomain with physical hosting, specify the FTP user account for it:

▪ If this subdomain will hold a part of your own Web site that you manage on your own, leave the **Use the FTP user account of the main domain** option selected.

▪ If this subdomain will hold a separate web site that will belong to or will be managed by another person, select the **Create a separate user account for this subdomain** option, and specify the login name and password that will be used for accessing the web space through FTP and publishing web site content. Specify the hard disc quota in the appropriate field in megabytes or leave the **Unlimited** checkbox selected. When the specified limit is exceeded, you will not be able to add files to the web space, and editing existing files may corrupt them.

9 Leave the **Publish site with SiteBuilder** checkbox selected to be able to access SiteBuilder and build web site through your Plesk control panel interface. When the **Publish site with SiteBuilder** option is selected, a site will be created in SiteBuilder.

All publishing parameters will be set in the paths predefined: for subdomain with **Physical hosting** - /subdomains/SUBDOMAINNAME/httpdocs/sitebuilder; for subdomain with **Subdomain on subfolder** - /httpdocs/SUBDOMAINNAME/.

10 If you want to enable **Microsoft FrontPage support**, select the appropriate checkbox. Enable or disable **Remote Microsoft FrontPage authoring** by selecting the appropriate option.

11 Specify the programming languages support in the **Services** group by selecting the required languages. Use **select all** or **clear all** to select or clear all of the languages available.

If the ASP.NET support is disabled on the domain for which you are creating subdomain, it is also unavailable on **Subdomain on subfolder**. In case the ASP.NET support is enabled on the domain, the ASP.NET is available for subdomain created on a subfolder.

12 To allow you to view the information on the number of people visited the site and the pages of the site they viewed, select a module in **Web statistics** drop-down menu and select the **accessible via password protected directory /plesk-stat/** checkbox, if required. This will install the selected statistical software module, which will generate reports and place them into the password protected directory. The subdomain administrator will then be able to access Web statistics at the URL: https://subdomain.domain.com/plesk-stat/ using their FTP account login and password.

Note. If subdomain administrator changes the FTP credentials, web statistics access credentials do not change. The original login and password specified upon the subdomain creation should always be used for accessing password-protected web statistics directory.

13 Select the **Additional write/modify permissions** option if this subdomain's web applications will use a file-based database (like Jet) located in the root of `httpdocs` or `httpsdocs` folders. Please note that selecting this option might seriously compromise the web site security.

14 To complete the setup, click **OK**. It may take up to 48 hours for the information on new subdomain to spread in the Domain Name System and become available to the Internet users.

To publish web content to the subdomain's web space, follow the instruction presented in the Publishing a Site (on page 136) section.

Removing Subdomains

➢ *To remove a subdomain with its web content:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Subdomains**.

4 Select a check box corresponding to the subdomain name that you wish to remove, and click ✖ **Remove Selected**.

5 Confirm removal and click **OK**. The subdomain configuration and its web content will be removed from the server.

Setting Up Additional Domain Names for a Site (Domain Aliases)

If you have registered with a domain name registrar several domain names that you would like to point to the same web site that you host on your server, you should set up domain aliases.

If you need to serve several domain names that point to a web site hosted on another server, you should set up domain forwarding: see the Serving Domain Names for Sites Hosted on Other Servers (Domain Forwarding) (on page 195) section for instructions.

In this section:

Setting Up Domain Aliases

> ➢ *To set up a domain alias:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click the **Domain Aliases** icon.

4 Click the **Add Domain Alias** icon.

5 Type the desired domain alias name, for example alias.com.

Domain aliases can comprise letters, digits and hyphens. Each part of the domain alias between dots should not be longer than 63 symbols.

6 Select the **Synchronize DNS zone with the primary domain** check box if you want the domain alias to use the same DNS zone resource records as in primary domain. With this setting, any subsequent changes in resource records of the primary domain's zone will be applied to the DNS zone of this domain alias.

7 Select the **Mail** check box, if you want e-mail directed at the e-mail addresses under the domain alias to be redirected to the e-mail addresses under your original domain name.

Example: You have an e-mail address mail@yourdomain.com. You have set up an alias for your domain name, for example, alias.com. If you want to receive mail to your mailbox mail@yourdomain.com when it is sent to mail@alias.com, select the **Mail** check box.

8 Select the **Web** check box. Otherwise, the web server will not serve the web content to users coming to your site by typing the domain alias in their browsers.

9 Select the **Java Web applications** check box if you have Java applications installed on your site and you want them to be accessible through the domain alias.

10 Click **OK**.

Modifying Properties of Domain Aliases

➢ *To change the properties of an alias:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click the **Domain Aliases** icon.

4 Click the alias name you need.

5 Click the **Preferences** icon in the **Tools** group.

➢ *To modify resource records in the DNS zone of a domain alias:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Domain Aliases**.

4 Click the alias name you need.

5 Click **DNS Settings**.

6 Add, edit or remove the resource records as required:

- To add a resource record to the zone, click **Add New Record**. Specify the required values and click **OK** to write the values to the zone.

- To modify a resource record, under the **Host** column, click a hyperlink corresponding to the record you need.

- To remove a record, select a check box corresponding to the record you wish to remove and click ✖ **Remove Selected**.

Removing Domain Aliases

➢ *To remove an alias from a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click the **Domain Aliases** icon.

4 Select a check box corresponding to the domain alias that you want to remove.

5 Click ✖ **Remove Selected**. Confirm removal and click **OK**.

Using Virtual Directories

A virtual directory in Plesk is a link to existing physical directory that is present on the server's hard disk. Virtual directories can have a number of specific settings like custom ASP.NET configuration, access permissions, URL password protection, and so on.

Since any virtual directory can have its own settings, including customized ASP.NET configuration, virtual directories are very useful in setting up your web applications, especially those written in ASP.NET. For example, if you have three web applications that use ASP.NET version 1.1, and you need to install one web application that uses ASP.NET version 2.0, you can create a virtual directory for the ASP.NET 2.0 application, configure ASP.NET settings for this directory, enabling version 2.0 only for this directory, and successfully install the required application.

Virtual directories can also be used as aliases. For example, you have a web application installed on your domain 'example.com' in the physical folder '/my_data/web_apps/forum'. To access this web application, users need to type 'example.com/my_data/web_apps/forum', which is hard to remember and too long to type. You can create virtual directory 'forum' in the root of your virtual host, and link this virtual directory to '/my_data/web_apps/forum', so users who want to access the web application have to type 'example.com/forum', which is much shorter and easier to remember.

➢ *To open a virtual directory in your browser:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Directories**.

4   Click the 🌐 icon corresponding to the directory you wish to open.

In this section:

Creating Virtual Directories

➢ *To create a new virtual directory on a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories** in the **Hosting** group. You are in your web site root now.

4 Navigate to the directory in which you want to create a new virtual directory.

5 Click **Add New Virtual Directory**.

Note. To create a physical directory instead of virtual directory, click **Add New Directory**, specify the name of the directory and click **OK**.

6 Specify the required parameters:

- **Name** - specify the virtual directory name.

- **Path** - specify the virtual directory path:

  - Select the **Create physical directory with the same name as virtual directory** checkbox to automatically create a physical directory with the same name as the virtual directory you are creating.

  - Clear the **Create physical directory with the same name as virtual directory** checkbox and specify the path in the field to select the physical directory that already exists.

- **Script source access** - select this checkbox to allow users to access source code if either Read or Write permissions are set. Source code includes scripts in ASP applications.

- **Read permission** - select this checkbox to allow users to read files or directories and their associated properties.

- **Write permission** - select this checkbox to allow users to upload files and their associated properties to the virtual directory or to change content in a write-enabled file. Write access is allowed only if browser supports the PUT feature of the HTTP 1.1 protocol.

- **Directory browsing** - select this checkbox to allow users to see a hypertext listing of the files and subdirectories in the virtual directory.

- **Log visits** - select this checkbox if you want to store the information about visits of the virtual directory.

- **Create application** - select this checkbox to make the web directory an IIS Application. The directory becomes logically independent from the rest of the web-site.

- **Execute permissions** - select the appropriate program execution level allowed for the virtual directory.

  - **None** - allow access only to static files such as HTML or image files.

  - **Scripts only** - allow running scripts only, not executables.

- **Scripts and Executables** - remove all restrictions so that all file types can be executed.

- **ASP Settings** - set specific settings for ASP-based web applications.

- If you are using ASP-based applications that cannot operate correctly under data transfer restrictions currently set by IIS, deselect the **Defined by parent directory** check box corresponding to the field you want to change and type in the required number.

- If you want to enable debugging of ASP applications on the server side, deselect the corresponding **Defined by parent directory** check box and select the **Enable ASP server-side script debugging** check box.

- If you want to enable debugging of ASP applications on the client side, deselect the corresponding **Defined by parent directory** check box and select the **Enable ASP client-side script debugging** check box.

Note that if you are trying to change ASP Settings for the root web directory, the default check box names will be **Defined by IIS**.instead of **Defined by parent directory**.

7 Click **OK** to complete the creation.

➢ *To set access permissions for a virtual directory:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories**.

4 Click the 🔒 icon corresponding to the directory you wish to open, and set the access permissions for this directory and all its files.

Refer to the Setting File and Folder Access Permissions (on page 211) section for more information on setting access permissions.

➢ *To configure ASP.NET for a virtual directory:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories**.

4 Browse to the required directory and enter it.

5 Click **ASP.NET** and set the options accordingly.

Refer to the Configuring ASP.NET for Virtual Directories (on page 151) section for more information on configuring ASP.NET

Changing Virtual Directory Settings

➢ *To change preferences of an existing virtual directory on a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories** in the **Hosting** group.

4 Find the directory which preferences you wish to change, and click ⚙,
 or click **Preferences** in the required directory.

5 Change the preferences of the virtual directory:

- **Name** - specify virtual directory name.

- **Path** - specify the path to the physical directory which virtual directory is linked
 to.

- **Script source access** - select this check box to allow users to access source code
 if either Read or Write permissions are set. Source code includes scripts in ASP
 applications.

- **Read permission** - select this check box to allow users to read files or directories
 and their associated properties.

- **Write permission** - select this check box to allow users to upload files and their
 associated properties to the virtual directory or to change content in a write-
 enabled file. Write access is allowed only if browser supports the PUT feature of
 the HTTP 1.1 protocol.

- **Directory browsing** - select this check box to allow users to see a hypertext listing
 of the files and subdirectories in the virtual directory.

- **Log visits** - select this check box if you want to store the information about visits
 of the virtual directory.

- **Create application** - select this check box to make the web directory an IIS
 Application. The directory becomes logically independent from the rest of the
 web-site.

- **Execute permissions** - select the appropriate program execution level allowed for
 the virtual directory.

  None - allow access only to static files such as HTML or image files.

  Scripts only - allow running scripts only, not executables.

  Scripts and Executables - remove all restrictions so that all file types can be
  executed.

- **Allow to use parent paths** - select this check box to allow using double period in the
 pathname when referring to a folder above the current web 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 path
 directories should not have the **Execute permission** check box selected in their
 preferences, so that applications do not have the ability of unauthorized running
 of programs in the parent paths.

- **Allow application execution in MTA (multi-threaded apartment) mode** - select this check box to allow the application execution in multi-threaded apartment (MTA) mode. Otherwise the application will run in a single-threaded apartment (STA) mode. Using STA, each application pool is executed in a dedicated process. With MTA, several concurrent application pools are executed in one thread which can increase performance in some cases.

- **Use default documents** - select this check box to allow the use of default documents for the current web directory. The default document is sent when users access the directory on the Web without a specific file name (for example, using 'http://www.parallels.com' as opposed to 'http://www.parallels.com/index.html'). If this check box is cleared and the **Directory browsing** check box is selected, the Web server returns a folder listing. If this check box is cleared and the **Directory browsing** check box is cleared as well, the Web server returns an "Access Forbidden" error message.

- **Default documents search order** - specifies the order in which IIS searches for the default document, sending user the first available file it finds. If no match is found, IIS behaves as in the cases when the default content page is disabled.

- **Allow anonymous access** - select this check box if you want to make the directory public so that web users could access it without authentication.

- **Require SSL** - select this check box to enable SSL-only access to the folder.

- **ASP Settings** - set specific settings for ASP-based web applications.

  - If you are using ASP-based applications that cannot operate correctly under data transfer restrictions currently set by IIS, clear the **Defined by parent directory** check box corresponding to the field you want to change and type in the required number.

  - If you want to enable debugging of ASP applications on the server side, clear the corresponding **Defined by parent directory** check box and select the **Enable ASP server-side script debugging** check box.

  - If you want to enable debugging of ASP applications on the client side, clear the corresponding **Defined by parent directory** check box and select the **Enable ASP client-side script debugging** check box.

    Note that if you are trying to change ASP Settings for the root web directory, the default check box names will be **Defined by IIS**.instead of **Defined by parent directory**.

6 Click **OK** to save changes.

> *To change access permissions for a virtual directory:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories**.

4 Click the 🔒 icon corresponding to the directory you wish to open, and change the access permissions for this directory and all its files.

Refer to the Setting File and Folder Access Permissions (on page 211) section for more information on setting access permissions.

➤ *To reconfigure ASP.NET for a virtual directory:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Directories**.

4   Browse to the required directory and enter it.

5   Click **ASP.NET** and change the options accordingly.

> Refer to the Configuring ASP.NET for Virtual Directories (on page 151) section for more information on configuring ASP.NET

Adding and Removing MIME Types

Multipurpose Internet Mail Exchange (MIME) types instruct a Web browser or mail application how to handle files received from a server. For example, when a Web browser requests an item on a server, it also requests the MIME type of the object. Some MIME types, like graphics, can be displayed inside the browser. Others, such as word processing documents, require an external 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. 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.

In this section:

Adding MIME Types

➢ *To add a new MIME type for a virtual directory on a domain:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Directories** in the **Hosting** group.

4   Navigate to the required virtual directory and enter it.

5   Select the **MIME Types** tab.

6   Click **Add New MIME Type**.

- Type the filename extension in the **Extension** field. Filename extention should begin with a dot (.), or a wildcard (*) to serve all files regardless of filename extension.

- Specify the file content type in the **Content** field.

- You can either select the appropriate value from the list or define a new content type. To do this, select **Custom...** and enter the content type in the input box provided.

7   Click **OK** to finish the creation.

Changing MIME Types

➢ *To edit an existing MIME type for a virtual directory on a domain:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Directories** in the **Hosting** group.

4   Navigate to the required virtual directory and enter it.

5   Select the **MIME Types** tab.

6   Select the required MIME type in the list.

- Type the filename extension in the **Extension** field. Filename extention should begin with a dot (.), or a wildcard (*) to serve all files regardless of filename extension.

- Specify the file content type in the **Content** field.

- You can either select the appropriate value from the list or define a new content type. To do this, select **Custom...** and enter the content type in the input box provided.

7   Click **OK** to save changes.

Removing MIME Types

> ➢ *To remove a MIME type for a virtual directory on a domain:*

1 Click the **Domains** shortcut in the navigation pane.
2 Click the required domain name in the list.
3 Click **Web Directories** in the **Hosting** group.
4 Navigate to the required virtual directory and enter it.
5 Select the **MIME Types** tab.
6 Select the checkbox corresponding to the MIME type you wish to remove.
7 Click ✕ **Remove Selected**.
8 Confirm removal and click **OK**.

Setting PHP Version for Virtual Directories

In addition to be able to choose the PHP version you would like to use on each of your domains, you also have the additional ability to specify the PHP version for any given virtual directory on your domains, allowing you to use web applications that require PHP4 as well as PHP5.

> ➢ *To set PHP version for a virtual directory:*

1 Click the **Domains** shortcut in the navigation pane.
2 Click the required domain name in the list.
3 Click **Web Directories** in the **Hosting** group.
4 Click **PHP Settings**.
5 Choose the required version of PHP and click **OK**.

Removing Virtual Directories

> ➢ *To remove an existing virtual directory:*

1 Click the **Domains** shortcut in the navigation pane.
2 Click the required domain name in the list.
3 Click **Web Directories** in the **Hosting** group.
4 Select the checkbox corresponding to the directory you wish to remove.
5 Click ✕ **Remove Selected**.
6 Confirm the removal and click **OK**.

Hosting Personal Web Pages on Your Web Server

You can host on your Web server personal Web pages for individuals who do not need their own domain names. This service is popular with educational institutions that host non-commercial personal pages of their students and staff.

These pages usually have web addresses like http://your-domain.com/~username, however, you can set up personal web pages with alternative web addresses like http://username@your-domain.com, if you like.

➢ *To accommodate a personal web page on your server, allocate a separate web space and set up an FTP account for publishing:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Users** in the **Hosting** group.

4   Click **Preferences**.

5   If you wish to allow execution of scripts embedded in personal web pages, select the **Allow the web users scripting** check box.

6   Click **OK**.

    The settings you have defined at the steps 3 and 4 are common for all personal web pages you might host on your web server. Therefore, you will not need to perform steps 3 and 4 next time you set up a web space for a personal web page.

7   Click **Add New Web User**.

8   Specify a user name and password that will be used for accessing the web space through FTP and publishing the web page.

    You can use only lowercase alphanumeric, hyphen and underscore symbols in user name. The user name should begin with an alphabet character. It cannot contain white spaces. The password cannot contain quotation marks, white space, user's login name, and should be between 5 and 14 characters in length.

9   If you wish to limit the amount of disk space that can be occupied by the Web page content, clear the **Unlimited** checkbox and type the desired value in megabytes into the **Hard disk quota** box.

    When the specified limit is exceeded, the Web page owner will not be able to add files to his or her web space.

10 Select the **Additional write/modify permissions** option if this web user's web applications will use a file-based database (like Jet) located in the root of `httpdocs` or `httpsdocs` folders. Please note that selecting this option might seriously compromise the web site security.

11 Specify the programming languages that should be supported for the Web page.

    For example, if the web page is written in PHP, select the **PHP support** check box.

12 Click **OK**.

        Now you can tell your users the FTP account credentials, so that they can publish their web page.

In this section:

Changing FTP Password for a Web Page Owner

 ➢ *To change FTP password for a web page owner:*

1 Go to **Domains** > *domain name* > **Web Users** > *web user name*.

2 Type the new password into the **New password** and **Confirm password** boxes and click **OK**.

Allocating More Disk Space to the Web Page Owner

 ➢ *To allocate more disk space to the web page owner:*

1 Go to **Domains** > *domain name* > **Web Users**, then click the required web user name.

2 Type the amount of disk space in megabytes into the **Hard disk quota** box and click **OK**.

Removing Web Page Owner's Account

 ➢ *To remove a web page owner's account together with their web page:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Users** in the **Hosting** group.

4 Select a check box to the right of the user name you wish to remove and click ✖ **Remove Selected**.

5 Confirm removal and click **OK**.

Setting Up Anonymous FTP Access to the Server

If you host a site on a dedicated IP address, you can set up a directory within the site, where other users will be able to anonymously download or upload files through FTP. Once anonymous FTP is enabled, the users will be able to log in to the ftp://ftp.your-domain.com with the "anonymous" login name and any password.

➢ *To allow anonymous FTP access:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **FTP Management** in the **Hosting** group.

4   Click the **Anonymous FTP** tab.

5   To activate anonymous FTP service, click **Switch On**.

6   To set up a welcoming message to be displayed when users log in to FTP site, select the **Display login message** check box and type the message text in the input field as desired.

    Note that not all FTP clients display welcoming messages.

7   To allow visitors to upload files to the `/incoming` directory, select the **Allow uploading to incoming directory** check box.

8   To allow users to create subdirectories in the `/incoming` directory, select the **Allow creation of directories in the incoming directory** check box.

9   To allow downloading files from the `/incoming` directory, select the **Allow downloading from the incoming directory** checkbox.

10 To limit the amount of disk space that can be occupied by uploaded files, clear the **Unlimited** check box corresponding to the **Limit disk space in the incoming directory** option, and specify the amount in kilobytes.

    This is the hard quota: the users will not be able to add more files to the directory when the limit is reached.

11 To limit the number of simultaneous connections to the anonymous FTP server, clear the **Unlimited** check box corresponding to the **Limit number of simultaneous connections** option and specify the number of allowed connections.

12 To limit the bandwidth for anonymous FTP connections, clear the **Unlimited** check box corresponding to the **Limit download bandwidth for this virtual FTP domain** option and enter the maximum bandwidth in kilobytes per second.

13 Click **OK**.

➢ *To modify settings for anonymous FTP server or switch it off:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **FTP Management** in the **Hosting** group.

4 Click the **Anonymous FTP** tab.

5 Adjust the settings as required and click **OK**. To switch off the anonymous FTP service, click **Switch Off** in the **Tools** group.

Customizing Web Server Error Messages

When visitors coming to a site request pages that the web server cannot find, the web server generates and displays a standard HTML page with an error message. The standard error messages may inform of problems, but they do not usually say how to resolve them or how to get the lost visitor on his way, and they also look dull.

You may want to create your own error pages and use them on your web server. The following error messages are the ones customized most often:

- 400 Bad File Request. Usually means the syntax used in the URL is incorrect (e.g., uppercase letter should be lowercase letter; wrong punctuation marks).
- 401 Unauthorized. Server is looking for some encryption key from the client and is not getting it. Also, wrong password may have been entered.
- 403 Forbidden/Access denied. Similar to 401; a special permission is needed to access the site – a password and/or username if it is a registration issue.
- 404 Not Found. Server cannot find the requested file. File has either been moved or deleted, or the wrong URL or document name was entered. This is the most common error.
- 500 Internal Server Error. Could not retrieve the HTML document because of server-configuration problems.

➢ *To configure Plesk's web server to show custom error pages for a domain:/*

1 Switch on support for custom error documents through Plesk.

1. Go to **Domains** > domain name > **Setup**.

2. Select the **Custom Error Documents** check box.

3. Click **OK**.

2 Go to **Domains** > **domain name** > **Web Directories** to see the list of error documents for the root web directory (error documents located here are used for all domain web pages). If you want to customize error pages for a certain web directory, go to that directory.

3 Click **Error Documents** tab and click the required error document in the list.

- To use the default document provided by IIS for this error page, select **Default** in the **Type** menu.
- To use a custom HTML document already located in the `error_docs` directory on a domain, select **File** in the **Type** menu and specify the file name in the **Location** field.
- To use a custom HTML document located in directory other than `error_docs` on a domain, select **URL** in the **Type** menu and enter the path to your document in the **Location** field. The path should be relative to the virtual host root (that is, `<vhosts>\<domain>\httpdocs`).

  For example, you have created a file `forbidden_403_1.html` and saved it in the `my_errors` directory located in the `httpdocs`. To use this file as an error document, the following path should be entered in the **Location** filed: `/my_errors/forbidden_403_1.html`.

> **Note.** You can use both FTP and File Manager to upload your custom error
> document to the server. By default, all error documents are stored in the
> `/vhosts/your-domain.com/error_docs/` directory (located in `C:\InetPub`
> by default).

4 Once the web server is restarted, it will start using your error
documents.

Customizing DNS Zone Configuration for Domains

For each new domain name, your control panel automatically creates DNS zone in
accordance with the configuration preset you define. The domain names should work
fine with the automatic configuration, however if you need to perform custom
modifications in the domain name zone, you can do that through your control panel.

➢ *To view the resource records in a DNS zone of a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings** in the **Services** group. A screen will show all resource
records for a given domain.

To learn about modifying resource records in the DNS zone of a domain alias, refer to
the Setting Up Additional Domain Names for a Site (Domain Aliases) (on page 171)
section.

> **Note:** Here you can update the DNS zone with multiple changes in DNS records at
> once, and then confirm the changes by clicking the **Apply** button. Unconfirmed changes
> will not be saved.

In this section:

Adding Resource Records

> ➢ *To add a new resource record to the zone:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **DNS Settings** in the **Services** group.

4   Click **Add New DNS Record** in the **Tools** group.

5   Select a resource record type, and specify the appropriate data:

- For an A record you will need to enter the domain name for which you wish to create an A record. If you are simply defining an A record for your main domain, then you should leave the available field empty. If you are defining an A record for a name server then you will need to input the appropriate entry for the given name server (ie. ns1). Then, you need to enter the appropriate IP address to which to associate the domain name.

- For a NS record, you will need to enter the domain name for which you wish to create the NS record. If you are defining an NS record for your main domain, then you will leave the available field blank. Then enter the appropriate name server name in the field provided. You will need to enter the complete name (i.e. ns1.mynameserver.com).

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

- For a CNAME record, you will need to first enter the alias domain name for which you wish to create the CNAME record. You then need to enter the domain name within which you want the alias to reside. Any domain name can be entered. It does not need to reside on the same server.

- For a PTR record you will first enter the IP address/mask for which you wish to define the pointer. Then enter the appropriate domain name for this IP to be translated to.

- For a TXT record, you will be able to enter an arbitrary text string, which could be a description or an SPF record.

- For a SRV record, you will need to enter the service name, protocol name, port number, and target host. Service and protocol names should start with the underline symbol. You can also specify the priority of service and weight of service in the appropriate fields.

6   Click **OK** to submit the data.

Note: When you are finished with modifying DNS records of the DNS zone, confirm the changes by clicking the **Apply** button on the DNS zone screen (**DNS Settings**). Unconfirmed changes will not be saved.

Modifying Resource Records

➢ *To modify the properties of a resource record for a domain:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **DNS Settings** in the **Services** group.

4   Click the hyperlink in the **Host** column corresponding to the resource record you want to modify.

5   Modify the record as required and click **OK.**

➢ *To modify the entries in the Start of Authority (SOA) record for a domain:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **DNS Settings**.

4   Select the **SOA Records** tab.

5   Specify the desired values:

- **Refresh Interval**. This is how often the secondary name servers check with the primary name server to see if any changes have been made to the domain's zone file. Plesk sets the default value of three hours.

- **Retry Interval**. This is the time a secondary server waits before retrying a failed zone transfer. This time is typically less than the refresh interval. Plesk sets the default value of one hour.

- **Expire Interval**. This is the time before a secondary server stops responding to queries, after a lapsed refresh interval where the zone was not refreshed or updated. Plesk sets the default value of one week.

- **Minimum TTL**. This is the time a secondary server should cache a negative response. Plesk sets the default value of one day.

- **Default TTL**. This is the amount of time that other DNS servers should store the record in a cache. Plesk sets the default value of one day.

6   Click **OK**.

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

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

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

➢ *To change the Start of Authority (SOA) serial number format to YYYYMMDDNN for a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings**.

4 Select the **SOA Records** tab.

5 Select the **Use serial number format recommended by IETF and RIPE** check box.

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

6 Click **OK**.

Modifying Common Access Control List (ACL)

You can modify the common Access Control List (ACL) via Plesk. ACL contains all hosts to which DNS zone transfers for all zones are allowed.

➢ *To modify the common Access Control List (ACL) for a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings** in the **Services** group.

4 Select **Transfer Restrictions** tab.

▪ To add a network to ACL, specify the IP address and mask in the **IP address/mask** field and click **Add Network**.

▪ To delete a network from ACL, select the checkbox corresponding to the required network in the list, click ✖ **Remove Selected**, confirm the removal and click **OK**.

Removing Resource Records

> ➤ *To remove a resource record from the zone:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings** in the **Services** group.

4 Select a check box corresponding to the record you wish to remove.

5 Click ✖ **Remove Selected**.

6 Confirm removal and click **OK**.

Note: When you are finished with modifying DNS records of the DNS zone, confirm the changes by clicking the **Apply** button on the DNS zone screen (**DNS Settings**). Unconfirmed changes will not be saved.

Restoring the Original Zone Configuration

➢ **To restore the original zone configuration in accordance with the server-wide DNS settings:**

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **DNS Settings** in the **Services** group.

4   Click **Restore Defaults**.

5   In the **IP address** drop-down box, select the IP address to be used for restoring the zone and specify whether a www alias is required for the domain.

6   Confirm the restoration and click **OK**. The zone configuration will be recreated.

➢ **To reset the entries in the Start of Authority (SOA) record to default settings:**

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **DNS Settings** in the **Services** group.

4   Select the **SOA Records** tab.

5   Click **Restore Defaults**.

➢ **To restore the default Start of Authority (SOA) serial number format (UNIX timestamp) for a domain:**

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **DNS Settings** in the **Services** group.

4   Select the **SOA Records** tab.

5   Clear the **Use serial number format recommended by IETF and RIPE** check box.

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

6   Click **OK**.

Serving Sites with External Domain Name Servers

If you host web sites on this server and have a standalone DNS server acting as a primary (master) name server for your sites, you may want to set up your control panel's DNS server to function as a secondary (slave) name server.

➢ *To make the control panel's DNS server act as a secondary name server:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings** in the **Services** group.

4 Click **Switch** in the **Tools** group.

5 Specify the IP address of the primary (master) DNS server.

6 Click **Add**.

7 Repeat steps from 1 to 5 for each web site that needs to have a secondary name server on your server.

➢ *To make the control panel's DNS server act as a primary for a zone:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings** in the **Services** group.

4 Click **Switch** in the **Tools** group. The original resource records for the zone will be restored.

If you have external name servers authoritative for some of your web sites, switch off the control panel's DNS service for each site served by external name servers:

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings** in the **Services** group.

4 Click **Switch off** in the **Tools** group. Turning the DNS service off for the zone will refresh the screen, so that only a list of name servers remains.

> **Note:** The listed name server records have no effect on the system. They are only presented on the screen as clickable links to give you a chance to validate the configuration of the zone maintained on the external authoritative name servers.

5 Repeat the steps from 1 to 3 to switch off the local domain name service for each site served by external name servers.

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

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **DNS Settings** in the **Services** group.

4 Add to the list the entries pointing to the appropriate name servers that are authoritative for the zone: click **Add**, specify a name server, and click **OK**.

Repeat this for each name server you would like to test. The records will appear in the list.

5 Click on the records that you have just created.

Plesk will retrieve the zone file from a remote name server and check the resource records to make sure that domain's resources are properly resolved. The results will be interpreted and displayed on the screen.

Serving Domain Names for Sites Hosted on Other Servers (Domain Forwarding)

If you need to serve a domain name or several domain names that point to a web site hosted on another server:

1 Click the **Clients** shortcut in the navigation pane.

2 Click **Add New Domain**.

3 Specify the domain name.

Leave the **www** check box selected if you wish to allow users to access the site by a common and habitual URL like www.your-domain.com. Having the www alias preceding the domain name will allow users to get to the site no matter what they type in their browsers: www.your-domain.com and your-domain.com will both point to the site.

4 Leave the **Create domain without template** option selected in the **Select template** menu.

5 If you have a number of IP addresses to choose from, select the required address from the **Select an IP address** drop-down box.

Bear in mind that e-commerce sites need a dedicated IP address (not shared among other sites) to implement Secure Sockets Layer data encryption.

6 Make sure that there is a check mark in the **Proceed to hosting setup** check box and click **OK**.

7 Choose the forwarding type: select either **Frame forwarding** or **Standard forwarding** option.

With standard forwarding, a user is redirected to the site and the actual site's URL is shown in the user's browser, so the user always knows that he or she is redirected to another URL. With frame forwarding, a user is redirected to the site without knowing that the site actually resides at another location, therefore, **Frame forwarding** should be preferred.

8 Click **OK**.

9 Specify the destination URL: the current web site address that you would like this domain to point to.

10 Click **OK**.

11 Repeat the steps from 1 to 9 to add as many domain forwarders as required.

Renaming Domains

➢ *To rename a domain:*

1 Go to a particular domain's administration page (**Domains** > **domain name**).

2 Click **Rename Domain**.

3 Type a new name for a domain in the **Domain name** field. Leave the **www** check box selected if you wish to allow users to access your site by a common URL like www.your-domain.com.

Having the www alias preceding your domain name will not cost you anything, but it will allow users to get to your site no matter what they type in their browsers: www.your-domain.com and your-domain.com will both point to your site.

4 Click **OK**. The operation might take several minutes, during which all domain services will be stopped.

Since domain renaming involves modifying DNS records, allow up to 48 hours for DNS propagation after the renaming.

Suspending and Unsuspending Domains

➢ *To suspend a domain:*

1 Select the **Domains** shortcut in the navigation pane.

2 Click the domain you need.

3 Click **Switch off**.

The domain will be suspended, its Web, FTP and mail services will no longer be accessible to the Internet users, and domain owner will not be able to log in to the control panel.

➢ *To unsuspend a domain:*

1 Select the **Domains** shortcut in the navigation pane.

2 Click the domain you need.

3 Click **Switch On**.

Removing Domains

➢ *To delete a domain with its content:*

1 Click the **Domains** shortcut in the navigation pane.

2 Select a check box corresponding to the domain name you wish to remove.

3 Click ✖ **Remove Selected**, confirm removal and click **OK**.

➢ *To delete a subdomain with its Web content:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click the **Subdomains** icon in the **Hosting** group.

4 Select the check box corresponding to the subdomain you wish to remove.

5 Click ✖ **Remove Selected**, confirm removal and click **OK**.

Securing Web Sites

In this chapter you will find out how to increase the security of web sites hosted on your server.

In this chapter:

Securing E-commerce Transactions with Secure Sockets Layer Encryption

If your clients are running an e-commerce business, they need to secure transactions between their customers and their site. To prevent the valuable data, such as credit card numbers and other personally identifiable information from being stolen, you should use the Secure Sockets Layer protocol, which encrypts all data and transfers them securely over the SSL connection. And even if someone intercepts the data for malicious intent, they will not be able to decrypt and use them.

To implement the Secure Sockets Layer protocol on your web server, you should purchase an SSL certificate from a reputable certificate vendor (these vendors are called Certificate Authorities), and then install this certificate on your site. To enable SSL protection, you must host your site on a dedicated IP address, which is not shared among other web sites.

There are numerous certificate authorities to choose from. When considering one, pay attention to reputation and credibility of the CA. Knowing how long they have been in business and how many customers they have will help you make the right choice.

Your Plesk control panel provides facilities for purchasing SSL certificates from Comodo, GeoTrust, Inc. and GoDaddy.

In this section:

Obtaining and Installing SSL Certificates from Comodo, GeoTrust, Inc. or GoDaddy

> ➤ *To purchase an SSL certificate through MyPleskCom online store and secure a site:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Certificates** in the **Services** group. A list of SSL certificates that you have in your repository will be displayed.

4   Click **Add New Certificate**.

5   Specify the certificate properties:

- Certificate name. This will help you identify this certificate in the repository.

- Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.

- Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.

- Specify the domain name for which you wish to purchase an SSL certificate. This should be a fully qualified domain name. Example: www.your-domain.com.

- Enter the domain administrator's e-mail address.

6   Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.

7   Click **Buy Cert**. Your private key and certificate signing request will be generated — do not delete them. MyPlesk.com login page will open in a new browser window.

8   Register or login to an existing MyPlesk.com account and you will be taken step by step through the certificate purchase procedure.

9   Choose the type of certificate that you wish to purchase.

10 Click **Proceed to Buy** and order the certificate. In the **Approver E-Mail** drop-down box, please select the correct Approver e-mail.

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

12 Once your certificate request is processed, you will be sent a confirmation e-mail. After you confirm, the SSL certificate will be sent to your e-mail.

13 When you receive your SSL certificate, save it on your local machine or network.

14 Return to the SSL Certificates repository (**Domains** > **domain name** > **Certificates**).

15 Click **Browse** in the middle of the page and navigate to the location of the saved certificate. Select it, and then click **Send File**. This will upload and install the certificate against the corresponding private key.

16 Return to the domain's administration screen (**Domains** > **domain name**) and click **Setup** in the **Hosting** group.

17 Select the SSL certificate that you wish to install from the **Certificate** drop-down box.

> If there is no **Certificate** drop-down box on the screen, this means that you are on a shared hosting account; therefore, you need to upgrade your hosting package and purchase a dedicated IP address from your hosting provider.

18 Select the **SSL support** check box and click **OK**.

Obtaining and Installing SSL Certificates from Other Certification Authorities

➢ *To secure a site with an SSL certificate from other certificate authorities:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Certificates** in the **Services** group. A list of SSL certificates that you have in your repository will be displayed.

4 Click **Add New Certificate**.

5 Specify the certificate properties:

- Certificate name. This will help you identify this certificate in the repository.

- Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.

- Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.

- Specify the domain name for which you wish to purchase an SSL certificate. This should be a fully qualified domain name. Example: www.your-domain.com.

- Enter the domain administrator's e-mail address.

6 Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.

7 Click **Request**. Your private key and certificate signing request will be generated and stored in the repository.

8 In the list of certificates, click the name of the certificate you need. A page showing the certificate properties opens.

9 Locate the **CSR section** on the page, and copy the text that starts with the line **-----BEGIN CERTIFICATE REQUEST-----** and ends with the line **-----END CERTIFICATE REQUEST-----** to the clipboard.

10 Visit the Web site of the certification authority from which you want to purchase an SSL certificate, and follow the links on their site to start a certificate ordering procedure. When you are prompted to specify CSR text, paste the data from the clipboard into the online form and click **Continue**. The certification authority will create an SSL certificate in accordance with the information you supplied.

11 When you receive your SSL certificate, save it on your local machine or network.

12 Return to the SSL Certificates repository (**Domains** > **domain name** > **Certificates**).

13 Click **Browse** in the middle of the page and navigate to the location of the saved certificate. Select it, and then click **Send File**. This will upload and install the certificate against the corresponding private key.

14 Return to the domain's administration screen (**Domains** > **domain name**) and click **Setup** in the **Hosting** group.

15 Select the SSL certificate that you wish to install from the **Certificate** drop-down box.

> If there is no **Certificate** drop-down box on the screen, this means that you are on a shared hosting account; therefore, you need to upgrade your hosting package and purchase a dedicated IP address from your provider.

16 Select the **SSL support** check box and click **OK**.

Creating and Installing Free Self-signed SSL Certificate

If you do not want to purchase SSL certificates, but still need to secure a site, you can create a self-signed certificate and install it on your web server. This will provide data encryption; however, your customers' browsers will show warning messages telling that your certificate is not issued by a recognized authority. Thus, using self-signed certificates is not recommended as it will not instill confidence in customers, and is likely to adversely affect the online sales of your client.

> ➢ *To secure a site with a self-signed SSL certificate:*

1   Go to **Domains** > *domain name* > **Certificates** and click **Add New Certificate**.

2   Specify the certificate properties:

- Certificate name. This will help you identify this certificate in the repository.

- Encryption level. Choose the encryption level of your SSL certificate. We recommend that you choose a value more than 1024 bit.

- Specify your location and organization name. The values you enter should not exceed the length of 64 symbols.

- Specify the domain name for which you wish to generate an SSL certificate. For example: www.your-domain.com.

- Enter the domain owner's e-mail address.

3   Click **Self-Signed**. Your certificate will be generated and stored in the repository.

4   Return to the domain's administration screen (**Domain** > *domain name*) and click **Setup** in the **Hosting** group.

5   Select the self-signed SSL certificate from the **Certificate** drop-down box.

> If there is no **Certificate** drop-down box on the screen, this means that you are on a shared hosting account; therefore, you need to upgrade your hosting package and purchase a dedicated IP address from your hosting provider.

6   Select the **SSL support** check box and click **OK**.

Uninstalling a Certificate from Your Site

➢ *To uninstall a certificate from your site and disable SSL protection:*

1 Make sure that the certificate you want to remove is not used at the moment.

2 Go to **Domains** > *domain name* > **Setup**. The **Certificate** drop-down box indicates which SSL certificate is currently used.

3 If the certificate that you want to remove is currently in use, you should first release it: in the **Certificate** drop-down box, select another certificate and click **OK**.

4 Remove the certificate from repository.

5 To permanently remove the certificate from repository, go to **Domains** > *domain name* > **Certificates** , select a check box corresponding to the certificate that you no longer need and click ✖ **Remove Selected**. Confirm removal and click **OK**.

6 Disable SSL support if you no longer need it.

7 Go to **Domains** > *domain name* > **Setup**.

8 Clear the **SSL support** check box and click **OK**.

Using SSL Certificate Shared By Another Domain (Shared SSL)

Shared SSL is a means of securing the access to a site with SSL (Secure Sockets Layer) without purchasing your own SSL certificate. Websites that employ shared SSL are, in fact, using the certificate shared by another domain. The domain that shares its SSL certificate with others is called Master SSL Domain.

Note. Before your customers can use shared SSL, the Master SSL Domain should be set. Refer to the Configuring Master SSL Domain for Shared SSL (on page 83) section for more information.

➢ *To use SSL certificate of the Master SSL Domain, enabling shared SSL:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Shared SSL** in the **Hosting** group.

4 Select the **Switch on shared SSL** checkbox.

5 Specify the virtual directory name in the corresponding input field. The virtual directory with the supplied name will be created on the Master SSL Domain. This directory will be used for accessing your site through SSL.

   For example, let us suppose that you have a domain named mydomain.com, Master SSL Domain is defined as master_ssl_domain.com, and the virtual directory name you supplied is `my_virtual_dir`. In this case, to access your site through SSL, you need to use the following address: https://master_ssl_domain.com/my_virtual_dir.

   Note. You cannot use your domain name (e.g., mydomain.com) to access your site via SSL if you are using shared SSL.

6 Select the directory where protected content is located on your domain. The documents within specified directory will be accessible only through SSL. You can only choose either `httpdocs` or `httpsdocs` as a target directory.

7 To make your domain accessible via SSL only, select the **Require SSL** checkbox.

8 Click **OK**.

➢ *To stop using SSL certificate of the Master SSL Domain, disabling shared SSL:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Shared SSL** in the **Hosting** group.

4 Clear the **Switch on shared SSL** checkbox.

5 Click **OK**.

Restricting Bandwidth Usage For Domains

To avoid excessive usage of bandwidth, which can lead to resources overage, you can limit bandwidth usage for a domain.

➢ *To limit the bandwidth for a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Performance** in the **Hosting** group.

4 Select the **Switch on bandwidth throttling** checkbox.

5 Input the maximum speed (measured in KB per second) that a domain can share between all its connections in the **Maximum network use (KB/S)** field.

6 Click **OK**.

Restricting the Amount of Simultaneous Web Connections to Domains

To avoid Denial Of Service attacks and to prevent excessive usage of bandwidth, you can set a limit of maximum number of simultaneous web connections your domain can have.

➢ *To limit the maximum number of simultaneous web connections to a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Performance**.

4 Select the **Switch on connections limiting** checkbox.

5 Input the maximum number of simultaneous connections in the **Connections limited to** field.

6 Click **OK**.

Protecting Sites From Bandwidth Stealing (Hotlinking)

Hotlinking (also called file leeching, remote linking, direct linking, bandiwidth stealing or bandwidth banditism) is a term used for describing a situation when a web page of one domain owner is directly linking to images (or other multimedia files) on the web host of another domain owner, usually using an <IMG> tag. If your domains are hotlinked, you may face the problem of excessive bandwidth usage.

➢ *To protect a domain from hotlinking:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Hotlink Protection** in the **Hosting** group.

4   Click **Switch On** to enable the protection from hotlinking.

5   Specify the extensions of files you wish to be protected from hotlinking (e.g. jpg, bmp, etc) in the **Protected files extensions** field. When listing several file extensions, separate them with spaces.

6   Click **OK**.

In this section:

Allowing and Disallowing Domains to Directly Link to Your Domain Files

You can also allow and disallow certain domains to directly link to your domain files.

➢ *To allow a domain directly link to your domain files:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Hotlink Protection**.

4   Input the domain name in the **Friendly domains** field.

5   Click **Add**.

6   Repeat steps 2 and 3 to add other domains, if necessary, and click **OK** when finished.

➢ *To disallow a domain directly link to your domain files:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Hotlink Protection**.

4   Select the domain in the **Friendly domains** field.

5   Click **Remove**.

6   Click **OK**.

Restricting Access to Web Site's Resources with Password Protection

If you have directories in a site that only authorized users should see, restrict access to these directories with password protection.

In this section:

Protecting a Resource

➢ *To password protect a directory in your site and to specify authorized users:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories** in the **Hosting** group.

4 On the **General** tab, click the required name from the Web directories list and select the **Protection** tab. Alternatively, you can click the 🛡 icon corresponding to the directory you want to protect.

5 Click **Protect** to set up a protection.

6 To add authorized users, click **Add New User** in the **Tools** group.

7 Specify the login name and password that will be used for accessing the protected area. The password should be from 5 to 14 symbols in length. Click **OK**.

8 Click **Preferences** to type a a resource description or a welcoming message that your users will see when they visit your protected area in the **Realm access text** input field. Click **OK**.

9 To add more authorized users for this protected resource, repeat the steps 7 and 8.

Adding and Removing Authorized Users

➢ *To add an authorized user of a protected directory:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Directories** in the **Hosting** group.

4   On the **General** tab, click the required name from the Web directories list and select the **Protection** tab. Alternatively, you can click the 🛡 icon corresponding to the required directory.

5   Click **Add New User** in the **Tools** group.

6   Specify the login name and password that will be used for accessing the protected area. The password should be from 5 to 14 symbols in length.

7   Click **OK**.

➢ *To change password for an authorized user of a protected directory:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Directories** in the **Hosting** group.

4   On the **General** tab, click the required name from the Web directories list and select the **Protection** tab. Alternatively, you can click the 🛡 icon corresponding to the required directory.

5   Click the user's name from the Protected URL users list.

6   Specify the new password and confirm it.

7   Click **OK**.

➢ *To revoke a permission to access the protected directory from a user:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Web Directories** in the **Hosting** group.

4   On the **General** tab, click the required name from the Web directories list and select the **Protection** tab. Alternatively, you can click the 🛡 icon corresponding to the required directory.

5   Select a check box corresponding to the user's name.

6   Click ✖ **Remove Selected**. Confirm the operation and click **OK**.

Unprotecting a Resource

> ➢ *To remove password protection and make the resource available to the public:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories** in the **Hosting** group.

4 On the **General** tab, click the required name from the Web directories list and select the **Protection** tab. Alternatively, you can click the icon corresponding to the required directory.

5 Select a check box corresponding to the name of the directory, from which you want to remove protection.

6 Click ✕ **Remove Selected**. The protection will be removed and the contents of the directory will be accessible to the public without restrictions.

Setting File and Folder Access Permissions

Plesk provides setting up file and folder access permissions, including defining special permissions and permissions inheritance, similarly to the way it is presented in Windows interface.

Note. For security reasons, permissions for Administrators, SYSTEM and Plesk Domain Administrator cannot be changed or removed.

In this section:

Setting and Changing Access Permissions for Groups and Users

➢ *To set or change access permissions for a group or user:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **File Manager**.

4 Click 📁 corresponding to the required file or folder.

- To change or remove permissions from a group or user, click the required name in the **Group or user names** list.

- To set permissions for a group or user, which is not in the **Group or user names** list, select the required user/group name from the drop-down box located above the list and click ➕: the user/group appears in the list. Select it.

5 To allow or deny permissions to a selected group/user, select the **Allow** or **Deny** checkboxes corresponding to permissions listed under **Permissions for [user/group name]**.

Note. If check boxes in **Allow** and/or **Deny** columns are shaded, it means that the corresponding permissions are inherited from a parent folder.

- To deny the permission, which are inherited from a parent object as allowed, select the required checkboxes under **Deny**. This will override inherited permissions for this file/folder.

- To allow the permission, which are inherited from a parent object as denied, clear the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** checkbox: this removes the inherited permissions. Then select the required check boxes under **Allow** and **Deny**.

6 Click **OK**.

Removing Access Permissions from Groups and Users

> *To remove access permissions from a group or user:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **File Manager**.

4 Click 📁 corresponding to the required file or folder.

5 Select the required name in the **Group or user names** list and click 🔴 next to it.

Note: The 🔴 icons appear unavailable for entries with permissions inherited from a parent object.

---

6 Select the required entry.

7 Clear the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** checkbox.

8 Select the entry again and click 🔴.

9 Click **OK**.

Setting Up Access Permissions Inheritance for Files and Folders

> *To set up access permissions inheritance for files and folders:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **File Manager** in the **Hosting** group.

4 Click 📁 corresponding to the required file or folder.

5 To make the file/folder inherit permissions from a parent folder (if it does not), select the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** checkbox.

6 To make the files and folders, which are contained in this folder, inherit the folder permissions defined here, select the **Replace permission entries on all child objects with entries shown here that apply to child objects** checkbox.

7 Click **OK**.

Setting, Changing and Removing Special Access Permissions

You can also set, change and remove special permissions including advanced management of folder permissions inheritance. In **Advanced** permissions management mode, several permission entries can be associated with a single group or user, each containing different set of permissions. Also, the list of permissions in **Advanced** mode is more detailed and gives more opportunities for fine-tuning file/folder permissions. It contains permissions that cannot be seen in Microsoft Windows interface, but present combinations of native Microsoft Windows permissions. They are Read Control, Write Control, and Execute Control.

➢ *To set, change or remove file/folder special permissions:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **File Manager** in the **Hosting** group.

4 Click 📁 corresponding to the required file or folder.

5 Click **Advanced**.

- To create a permission entry for a group or user, select the required name from the **Group or user names** list and click ➕.

- To set or change file/folder permissions for a group or user, select the required name from the **Group or user names** list, select the required **Allow** and **Deny** checkboxes corresponding to permissions listed under **Permissions for [group/user name]**.

- To remove a permission entry for a group or user, select the required name from the **Group or user names** list and click ⛔.

- To make child objects of a folder inherit its permissions defined under **Permissions for [group/user name]**, select the **Replace permission entries on all child objects with entries shown here that apply to child objects** checkbox, and select checkboxes in the **Apply onto:** list which correspond to objects you want to inherit the permissions.

6 Click **OK**.

Setting Access Permissions for Virtual Directories

Access permissions can also be applied to virtual (web) directories.

➢ *To set access permissions for a virtual directory:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Web Directories**.

4 Navigate the web site structure and click the required directory.

5 Click **Permissions** in the **Tools** group and set access permissions for this virtual directory, as described in the sections above.

Repairing Access Permissions

If some scripts on your sites stop working, this might be due to the incorrectly defined or corrupted file and folder access permissions. It is advised to run check and repair process to restore proper access permissions, thereby restoring scripts functioning.

➢ *To check and repair access permissions for a domain or a group of domains, restoring scripts functioning:*

1 Click the **Domains** shortcut in the navigation pane.

2 Select the check boxes corresponding to the domain names you want to perform permissions check on.

3 Click 🔒 **Check permissions**.

4 Adjust the settings as required:

- Clear the **Check-only mode** check box to check and repair access permissions. Leave the **Check-only mode** check box selected to run the checking in the read-only mode, when permissions are only checked (with errors reported), but not fixed.

- Leave the **Send notification by e-mail** check box selected to receive check and repair report by e-mail, and specify the required e-mail address in this field.

5 Click **OK**. Plesk will start checking permissions and correcting them, if the corresponding option is set. Please note that this procedure might take a lot of time, depending on the complexity of file and folder structure of your domains.

Transferring Domains Between User Accounts

> ➢ *To transfer a domain or several domains from one user account to another:*

1 Select the **Domains** shortcut in the navigation pane. Alternatively, you can select the **Clients** shortcut in the navigation pane and click on the required client name.

2 Select the check boxes corresponding to the domains you wish to transfer and click 👤 **Change Owner**.

3 Select the destination account you want to transfer selected domains to and click **Next >>**.

Plesk will check if the destination client account can provide the appropriate amount of resources for the transferred domains to function properly. If the destination client account does not have the resources to accommodate the new domains, the lacking resources will be highlighted. To allocate the required amount of resources to the destination client account, go to **Clients** > **client name** > **Limits**, adjust the amount of resources available to the accordingly, and start the domain transfer procedure again.

You can also choose IP addresses for transferred domains by selecting the destination IP address from the **New IP address** menu corresponding to the required domain.

4 Click **Finish** to complete the procedure.

Using E-mail Services

You can use a number of different e-mail services with a single e-mail account. For example, you can have an e-mail address that will accept mail as any standard mailbox, forward to a number of recipients, and send an automatic response to the original message sender.

If you are going to serve mailboxes under a specific domain with an external mail server, follow these steps:

1 Go to **Domains** > *domain name* > **DNS Settings**.

2 In the **Record type** column, locate an MX record, and click the respective link in the **Host** column on the left.

3 In the **Enter mail exchanger** box, type the external mail server's host name, for example, `mailserver.example.com`.

4 Click **OK**.

5 Click **Up Level** to return to the domain management screen.

6 Click **Mail**.

7 Click **Switch Off**.

In this chapter:

Creating Mailboxes

If you wish to have an e-mail address associated with a site, like yourname@domain.com, you should create a mailbox.

> ➢ *To create a mailbox:*

1 Go to **Domains** > *domain name* > **Mail** and click **Add New Mail Account**.

2 Your domain name is shown to the right of @ sign, so you only need to specify the desired name for the mailbox.

   This can be, for example, your first name and last name separated by a dot, a department name, or any other text in Latin symbols. The name should be short enough to remember. It can comprise alphanumeric, dash, dot and underscore symbols.

3 Specify a password that you will use for accessing your mailbox.

4 Make sure that a check mark is present in the **Mailbox** check box, then click **OK**.

Now your mailbox is created on the provider's server, and you can set up your favorite e-mail program so as to receive and send e-mail messages through your new mailbox.

> ➢ *To create mailboxes for other users:*

1 Go to **Domains** > *domain name* > **Mail** and click **Add New Mail Account**.

2 Your domain name is shown to the right of @ sign, so you only need to specify the desired name for the mailbox.

   This can be, for example, user's first name and last name separated by a dot, a department name, or any other text in Latin symbols. The name should be short enough to remember. It can comprise alphanumeric, dash dot and underscore symbols.

3 Specify a password that mailbox owner will use for accessing his or her mailbox.

4 Specify the language and skin for the user's Control Panel.

5 Make sure that a check mark is present in the **Mailbox** check box. If required, limit the amount of disk space that this mailbox and it's autoresponder attachment files can use. To do this, under **Mailbox quota** select the **Enter size** option and type the desired value in kilobytes. Click **OK**.

6 To allow the mailbox owner to log in to Control Panel for managing his or her mail account, click **Permissions**, click the **Select all** shortcut and click **OK**.

Now, the mailbox is created, and a separate e-mail administration panel has been set up in Plesk. To enter it, the mailbox owner should visit the URL https://your-domain.com:8443, type his or her e-mail address into the **Login** box, type the password for the mailbox into the **Password** box, and then click **Login**.

Setting Up Your E-mail Program for Retrieving Mail from Your Mailbox

➢ *To set up Microsoft Outlook Express:*

1 Open Microsoft Outlook Express.

2 Go to **Tools** > **Accounts**.

3 Click the **Mail** tab to open a list of your mail accounts.

4 Click the **Add >** button and select the **Mail ...** item.

5 Enter your name as you want it to appear in any messages you send, and click **Next >**.

6 Type your e-mail address that you created through Plesk (for example, your.name@your-domain.com), and click **Next >**.

7 Select the protocol of your incoming mail server.

8 Specify the mail domain name as the incoming and outgoing mail server (for example: mail.your-domain.com), and click **Next >**.

9 Type your e-mail address in the **Account name** box (for example: your.name@your-domain.com).

10 Type your password. This should be the password that you specified during creation of the mailbox through Plesk.

11 Leave the **Remember password** box checked, if you do not wish to be prompted to enter password each time your e-mail program connects to the mail server to check for new mail, and click **Next >**.

12 To complete setting up your e-mail program, click **Finish**.

➢ *To set up Mozilla Thunderbird:*

1 Open Mozilla Thunderbird.

2 Go to **Tools** > **Account Settings**...

3 Click **Add Account**. The Account Wizard will open.

4 Leave the **Email account** option selected, and click **Next >**.

5 Enter your name as you want it to appear in any messages you send.

6 Type your e-mail address that you created through Plesk.

   For example, your.name@your-domain.com. Click **Next >**.

7 Select the protocol of your incoming mail server.

8 Specify the mail domain name as the incoming and outgoing mail server (for example: mail.your-domain.com), and click **Next >**.

9 In the Incoming User Name box, specify your full e-mail address (for example, your.name@your-domain.com), and click **Next >**.

10 Enter the name by which you would like to refer to this account (for example, Work Account) and click **Next >**.

11 Verify that the information you entered is correct, and click **Finish**.

12 Click **OK** to close the Account Settings wizard.

Accessing Your Mail from a Web Browser

You can read your mail and compose new messages even if you are far from your home or office computer. To do this, you first need to allow access to the Horde Webmail interface that is integrated with your control panel. Then you can work with your mail from any computer that is connected to the Internet and has a Web browser program installed.

➢ *To allow access to the Webmail interface:*

1 Click **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click the **Mail** icon.

4 Click **Preferences**.

5 Choose the required WebMail client software in the **WebMail** menu to enable the ability to read mail through a browser-based WebMail application for users of mailboxes in this domain.

6 Click **OK**.

Note: Activation and deactivation of Webmail for a domain involves modifications in DNS zone, therefore, there is actually a certain delay present when activating and deactivating Webmail due to the speed of DNS registration mechanisms.

➢ *To access your mailbox through Webmail:*

1 Find a computer with Internet connection, for example, in an Internet café.

2 Do any of the following:

- Open a web browser, and type the URL: http://webmail.your-domain.com, where your-domain.com is the name of your domain. Press ENTER. A login screen will open. Type the user name and password that you specified during creation of your mailbox and click **Log in**.

- Open a web browser and type the URL to access your Plesk control panel, for example: https://your-domain.com:8443. Press ENTER. Log in to Plesk, click the domain name you need, and click the **Mail** icon in the **Services** group. Then, click an icon to the right of your e-mail address. A login screen will open and your user name will be prefilled. Type the password that you specified during creation of your mailbox and click **Log in**.

Protecting Mailboxes from Spam

To protect your mailbox from undesirable correspondence, do not publish your e-mail address on Internet forums and switch on the server-side spam filter provided by the SpamAssassin software.

When you need to publish your e-mail address, create a disposable e-mail address - e-mail alias - for your primary e-mail address, and publish it instead. All messages sent to the e-mail alias will come into your mailbox. Once you start getting spam, remove that alias and create another one. If you have a mailbox at another domain or mail server, you may want to set up a disposable e-mail forwarder.

Another efficient measure that can reduce the amount of spam and phishing e-mail messages is DomainKeys. For instructions on setting up spam protection based on DomainKeys, refer to the section Setting Up Spam Protection Based on DomainKeys.

In this section:

Setting Up Additional Disposable E-mail Addresses (Mail Aliases)

➢ *To set up an e-mail alias for a mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail** in the **Services** group.

4 Click the e-mail address you need.

5 Click **Add New Mail Alias**.

6 Type a desired name and click **OK**.

The messages addressed to your additional e-mail address (e-mail alias) will get to your mailbox. You can see the list of currently used mail aliases by clicking 👁 **Show Aliases** on the page that shows a list of mail accounts under the domain.

➢ *To remove an e-mail alias from a mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail** in the **Services** group.

4 Click the e-mail address you need.

5 Select the check box corresponding to the alias that you wish to remove, and click ✖ **Remove Selected**.

Setting Up Spam Filter

If you receive undesirable correspondence to an e-mail address that you cannot or do not want to remove, consider setting up spam filter for your mailbox. To do this,

- Enable SpamAssassin spam filter on the Plesk server, if you installed the SpamAssassin component on the server, and
- Install spam filtering software of your choice to work with e-mail program on your home or office computer.

In this section:

Switching on Spam Filter

> ➢ *To switch on spam filtering for a mailbox:*

1 Click **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail** in the **Services** group.

4 Click the e-mail address you need.

5 Make sure that Spam Filter is enabled: see whether the Spam Filter status shows **On** in the **Info** group. If it shows **Off**, ask your service provider to enable the spam filtering.

6 Click **Spam Filter**.

7 Select **Switch on spam filtering** checkbox.

8 Click **OK**.

9 Click **Up Level** to return to the mailbox management page.

> Now all the incoming mail will be filtered on the server side. By default, spam filter does not delete spam mail, it only adds the "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers to the message, and "*****SPAM*****" text string to the beginning of Subject line of each message recognized as spam. These settings are fine if you prefer to filter mail with a filtering program installed on your local computer – once mail has been retrieved from your mailbox.

> If you rely entirely on the Plesk server's spam filter, you may configure it so as to automatically delete the suspicious messages as they come. To configure the spam filter, follow the instructions below.

Configuring Spam Filter

➤ *To configure the spam filter for a mailbox:*

1 Click **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail** in the **Services** group.

4 Click the e-mail address you need.

5 Click **Spam Filter** in the **Tools** group. Configure the following settings as desired:

- **Use server wide settings**. Select this option if your provider or server administrator has prepared black and/or white lists of e-mail addresses that you would like to use together with your own restrictions. Black list, shown under **Black list** group, includes e-mail addresses of spammers, and White list, shown under **White list** group, includes e-mail addresses of trustworthy correspondents or entities. If the **Use server wide settings** check box is grayed out, i.e. not selectable, this means that there are no preconfigured spam filter settings on the server.

- **Hits required for spam**. This setting adjusts spam filter sensitivity. SpamAssassin performs a number of different tests on contents and subject line of each message. As a result, each message scores a number of points. The higher the number, the more likely a message is spam. For example, a message containing the text string "BUY VIAGRA AT LOW PRICE!!!" in Subject line and message body scores 8.3 points. By default, the filter sensitivity is set so that all messages that score 7 or more points are classified as spam.

- If you receive lots of spam messages with the current setting, to make filter more sensitive, try setting a lesser value in the **Hits required for spam** box; for example, 6.

- If you are missing your e-mails because your spam filter thinks they are junk, try reducing filter sensitivity by setting a higher value in the **Hits required for spam** box.

Note: To further improve spam filter accuracy, you may want to train your spam filter on e-mail messages you receive (see the instructions on improving accuracy of spam detection below).

- **What to do with spam mail**. If you are sure that your spam filter is accurate, you may want to set the filter to automatically delete all incoming messages recognized as spam. To do this, select the **Delete** option. If you wish to filter mail with the software on your local computer, select the **Mark as spam and store in mailbox** option, and then specify how spam filter should mark the messages recognized as spam. "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers are added to the message source by default, and if you want, the spam filter will also include a specific text string to the beginning of Subject line.

6 To save your changes, click **OK**.

7 If you do not want to receive e-mail from specific senders, add their e-mail addresses to the spam filter's black list.

- To add an entry to the black list, under **Black list** group, type an e-mail address into the **E-mail pattern** box. For example: address@spammers.net, *@spammers.net. **An asterisk (**) means any combination of symbols. Click **Add**.

- To remove an entry from the black list, select it and click **Remove**.

8 If you want to be sure that you will not miss e-mail from specific senders, add their e-mail addresses to the spam filter's white list.

- To add an entry to the white list, under **White list** group, type an e-mail address into the **E-mail pattern** box. For example: address@mycompany.com, *@mycompany.com. **An asterisk (**) means any combination of symbols. Click **Add**.

- To remove an entry from the black list, select it and click **Remove**.

9 If you want spam filter to consider some networks to be trusted:

- Select the **Trusted Networks** tab.

- To add an entry to the list, enter a network address into the fields next to **Network/Mask** and click **Add**.

  A network is specified by its starting IP address in the first four fields of the **Network/Mask** field group. The fifth field is for specifying network mask. It should be a number ranging from 1 to 32, which shows how many higher bits set to '1' the mask contains. For example, for the mask 255.255.255.0 you should specify 24 as the fifth parameter.

- To remove an entry from the list, select a network and click **Remove**.

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

Improving Accuracy of Spam Detection

You can improve accuracy of spam detection by training the spam filter on the e-mail messages that you have in your mailbox.

➢ *To improve accuracy of spam detection:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click the **Mail** icon in the **Services** group.

4 Click the e-mail address you need.

5 Click the **Spam Filter** icon in the **Tools** group.

6 Click the **Training** icon in the **Tools** group.

All e-mail messages you have in your mailbox are presented on the screen.

7 Train the spam filter.

In most cases, you can tell if a message is spam by looking at its subject line and sender's name. If they do not give you any clue, try looking inside the message using your e-mail program or webmail interface.

- To mark a message as spam, select the corresponding check box and click '**It's Spam!**'.

- To mark a message as not spam, select the corresponding check box and click '**It's Not Spam**'.

- To remove any information on a given message from the spam filter database, select the corresponding check box and click '**Forget It**'.

8 Once finished with training, you can remove spam e-mails from your mailbox using your e-mail program or Webmail interface.

Clearing Spam Filter's Database

If you have accidentally made your spam filter learn a great number of spam e-mails as non-spam or vice versa, your spam filter will likely produce incorrect results. In this case, clear the spam filter's database and then repeat training.

➢ *To clear spam filter's database:*

1   Click the **Domains** shortcut in the navigation pane.
2   Click the required domain name in the list.
3   Click the **Mail** icon in the **Services** group.
4   Click the e-mail address you need.
5   Click the **Spam Filter** icon in the **Tools** group.
6   Click the **Training** icon in the **Tools** group.
7   Click the **Clear** button.

Switching off Spam Filter

➢ *To switch off spam filtering for a mailbox:*

1   Click **Domains** shortcut in the navigation pane.
2   Click the required domain name in the list.
3   Click **Mail** in the **Services** group.
4   Click the e-mail address you need.
5   Click **Spam Filter** in the **Tools** group, then clear the **Switch on spam filtering** check box.
6   Click **OK** and click **Up Level**.

Protecting Mailboxes from Viruses

To defend your system from viruses, do not open suspicious e-mail attachments, enable anti-virus protection on the server side, and be sure to have a firewall and anti-virus software installed on your personal computer. Keep your operating system up-to-date and timely install security hot fixes and patches.

In this section:

Switching on Antivirus Protection

➢ *To switch on antivirus protection for a mailbox:*

1   Click **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Mail**.

4   Click the e-mail address you need.

5   Click **Antivirus** in the **Tools** group.

6   Choose the desired mail scanning mode. You can switch on scanning for incoming and outgoing mail in the corresponding menus. You can also use default server-wide settings both for incoming and outgoing mail.

7   Click **OK**.

Antivirus will delete all infected messages.

Switching off Antivirus Protection

➢ *To switch off antivirus protection for a mailbox:*

1   Click **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Mail**.

4   Click the e-mail address you need.

5   Click **Antivirus** in the **Tools** group.

6   Choose the **Do not scap for viruses** option in both **Incoming mail** and **Outgoing mail** menus.

7   Click **OK**.

Suspending and Unsuspending Mailboxes

➢ *To temporarily suspend e-mail services for a mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the e-mail address, whose e-mail services you wish to suspend.

5 Click **Mailbox** in the **Tools** group.

6 Clear the **Mailbox** check box.

7 Click **OK**.

➢ *To resume e-mail services for a suspended mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the e-mail address, whose e-mail services you wish to resume.

5 Click **Mailbox** in the **Tools** group.

6 Select the **Mailbox** check box.

7 Click **OK**.

➢ *To temporarily suspend e-mail services for all mailboxes in a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click **Switch off** in the **Tools** group.

➢ *To resume e-mail services for all mailboxes in a domain:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click **Switch On** in the **Tools** group.

Removing Mailboxes

➢ *To remove a mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Select a check box corresponding to the mailbox that you wish to remove.

5 Click ✖ **Remove Selected**.

6 When prompted, confirm removal and click **OK**.

Switching off the Mailbox Service When You Have Decided to Turn Your Account into a Mail Forwarder

If you are going to use your existing e-mail account as a mail forwarder or mailing list, you are recommended to switch off the mailbox service: a mailbox keeps all incoming messages and messages are not removed automatically after being forwarded. Therefore, if you choose to have the "mailbox + mail forwarder" configuration on your account, be sure to clean up the mailbox from time to time.

➢ *To switch off the mailbox service for your account discarding all messages in your mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click the **Mail** icon.

4 Click the required e-mail address.

5 Click the **Mailbox** icon in the **Tools** group.

6 Deselect the **Mailbox** check box.

7 Click **OK**.

Setting Up Mail Forwarding to a Single E-mail Address

➢ *To set up an e-mail address that will accept mail and forward it to another e-mail address:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Mail** in the **Services** group.

4   Click **Add New Mail Account**.

5   Specify the desired name for the mail forwarder next to **Mail account name**.

The domain name is shown to the right of @ sign, so you only need to type the name. This can be, for example, your first name and last name separated by a dot, a department name, or any other text in Latin symbols. The name should be short enough to remember. It can comprise alphanumeric, dash dot and underscore symbols.

6   Clear the **Mailbox** and **Control panel access** check boxes.

7   Click **OK**.

8   Click **Redirect** in the **Tools** group.

9   Select the **Redirect** check box.

10 Type the destination e-mail address to which you would like to forward e-mail.

11 Click **OK**.

➢ *To set up an e-mail address that will accept mail, pass it through the spam filter and then forward it to another e-mail address:*

1   Click the **Domains** shortcut in the navigation pane.

2   Click the required domain name in the list.

3   Click **Mail** in the **Services** group.

4   Click **Add New Mail Account**.

5   Specify the desired name for the forwarder's e-mail address next to **Mail Account Name**.

The domain name is shown to the right of @ sign, so you only need to type the name. This can be, for example, your first name and last name separated by a dot, a department name, or any other text in Latin symbols. The name should be short enough to remember. It can comprise alphanumeric, dash dot and underscore symbols.

6   Make sure that the **Mailbox** check box is selected.

Without a mailbox, you will not be able to apply spam filtering.

7   Specify a password that will be used for accessing the mailbox: You will likely need to clean the contents of mailbox from time to time.

8 Click **OK**.

9 Click **Redirect** in the **Tools** group.

10 Select the **Redirect** check box.

11 Type the destination e-mail address to which you would like to forward e-mail.

12 Click **OK**.

In this section:

Suspending and Unsuspending Mail Forwarders

➢ *To suspend a mail forwarder:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the e-mail address, whose forwarding service you wish to suspend.

5 Click **Redirect** in the **Tools** group.

6 Clear the **Redirect** check box.

7 Click **OK**.

➢ *To unsuspend a mail forwarder:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the e-mail address, whose forwarding service you wish to resume.

5 Click **Redirect** in the **Tools** group.

6 Select the **Redirect** check box.

7 Click **OK**.

Setting Up Mail Forwarding to Multiple E-mail Addresses

➢ *To set up an e-mail address that will accept mail and forward it to multiple other e-mail addresses:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail** in the **Services** group.

4 Click the required e-mail address.

5 Click **Mail Group**.

6 Click **Add New Member**.

   You should add at least one e-mail address before enabling mail forwarding to several e-mail addresses.

7 Enter the desired external e-mail address into the **E-mail** input box or select one or more of the listed mail accounts using check boxes.

8 Click **OK**.

9 Click **Switch On**.

In this section:

Adding and Removing Recipient Addresses

➢ *To add an external e-mail address to the list of mail accounts that receive forwarded e-mail correspondence:*

1 Go to **Domains** > *domain name* > **Mail** > *mail account* > **Mail Group**, then click **Add New Member**.

2 Enter the desired external e-mail address into the **E-mail** input field and click **OK**.

➢ *To remove an external e-mail address from the list of mail accounts that receive forwarded e-mail correspondence:*

1 Go to **Domains** > *domain name* > **Mail** > *mail account* > **Mail Group**.

2 Select the check box corresponding to the mail account you want to remove from the list.

3 Click ✖ **Remove Selected**, confirm removal and click **OK**.

➢ *To add an e-mail address registered on your server to the list of mail accounts that receive forwarded e-mail correspondence:*

1 Go to **Domains** > *domain name* > **Mail** > *mail account* > **Groups**.

2 Select the required multiple e-mail forwarder in the **Available mail groups** list and click **Add >>**, then click **OK**.

An e-mail address registered on your server can also be added to the subscription list using the procedure for adding an external e-mail address (see above).

➢ *To remove an e-mail address registered on your server from the list of mail accounts that receive forwarded e-mail correspondence:*

1 Go to **Domains** > *domain name* > **Mail** > *mail account* > **Groups**.

2 Select the required multiple e-mail forwarder in the **Member of the following mail groups** list and click **<< Remove**, then click **OK**.

An e-mail address registered on your server can also be removed from the subscription list using the procedure for removing an external e-mail address (see above).

Switching off Mail Forwarding to Multiple E-mail Addresses

➢ *To disable the e-mail forwarding to several e-mail addresses:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail** in the **Services** group.

4 Click the required e-mail address.

5 Click **Mail Group**.

6 Click **Switch Off**.

Removing Mail Forwarders

➢ *To remove a mail forwarder:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Select a check box corresponding to the mail forwarder that you wish to remove.

5 Click ✖ **Remove Selected**.

6 When prompted, confirm removal and click **OK**.

Setting Up Automatic Reply

If you are going on vacation and will not be able to check your mail for a while, you may want to leave a vacation notice that will be automatically sent to your correspondents once they send e-mail to your address. This is done with automatic reply facility, also referred to as autoresponder. Aside from vacation notices, organizations can use automatic replies to notify customers that their orders or technical support requests were received and will soon be processed. Automatic replies can include prewritten messages in plain text or HTML format, and they can contain attached files as well.

➢ *To set up automatic reply for a mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the e-mail address, for which you wish to set up an automatic reply.

5 Click **Autoresponders** in the **Tools** group.

6 If you are not going to attach any files to the automatic reply, proceed to the step 6. To attach a file to the automatic reply:

   1. Click **Attachment Files** in the **Tools** group.

   2. Click **Browse** to locate the file, and once selected, click **Send File**.

      The file will be added to the attachment files storage, and you will be able to attach this file to a number of different automatic replies.

   3. Once finished, click ⬆ **Up Level** and proceed to the next step.

7 Click **Add New Autoresponder** in the **Tools** group.

8 Configure the automatic reply:

   1. Type a name for this automatic reply into the **Autoresponder name** box.

      For example, Vacation notice.

   2. If you want this automatic reply to be sent in reply to any incoming e-mail message, in the **Request** group, leave the **always respond** option selected. If you wish to automatically reply only to e-mail messages that contain specific words in the message text or subject line, select the appropriate option, and type the word combination in the **Request text** input box.

   3. By default, the subject line of incoming e-mail will be inserted into the automated reply. To use a custom subject, type it into the **Answer with subject** subject input box.

4. As your correspondents may not figure out that the message they received from you was an automatic response, they may want to respond to your auto-reply. So, you should specify your e-mail address as the **Return address**, otherwise, their messages will be directed at the autoresponder's address.

5. Type your message in the **Reply with text** field.

6. To limit the number of automated responses per day to the same e-mail address, enter the desired number in the **Reply to unique e-mail address not more than** input box under **Limits**.

   The default setting is to respond no more than ten times in one day to the same e-mail address.

7. To reduce mail server load, you may want to limit the number of unique addresses that the autoresponder will remember. To do this, enter the desired number into the **Store up to** box.

8. If you want your incoming mail to be forwarded to another e-mail address while you are away, specify an e-mail address in the **Forward request to e-mail** box.

9. Attach your files, if needed. To do this, click the **Add New Attachment** button, select the check box corresponding to the file that you previously uploaded to the attachment storage, and click **OK**. To remove an attached file from the automatic reply, select the corresponding checkbox, and click ✖ **Remove Selected**.

9 Click **OK**.

10 Click **Switch On** in the **Tools** group.

Switching off Automatic Reply

➢ *To switch off an automatic reply for a mailbox:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the e-mail address, for which you wish to switch off the automatic reply.

5 Click **Autoresponders** in the **Tools** group.

6 Click **Switch off**.

> The automatic reply is now switched off. Its configuration is not deleted from the control panel, so the next time you need to use this automatic reply, repeat the above procedure, clicking **Switch On** on the last step.

➢ *To delete an automatic reply configuration that you no longer need:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the e-mail address you need.

5 Click **Autoresponders** in the **Tools** group.

6 Select a check box corresponding to the configuration name, and click ✖ **Remove Selected**.

Setting Up Site-Wide Preferences for Handling Mail to Nonexistent Users (Mail Bounce)

When somebody sends an e-mail message to an e-mail address that does not exist under your domain, the mail server, by default accepts mail, processes it, and when it finds out that there is no such a recipient under the domain, it returns the mail back to sender with the "this address no longer accepts mail" notice. You can choose to:

- Continue returning all such mail back to senders (**Bounce** option),
- Forward all such mail to the specified e-mail address (**Catch to address** option),
- Forward all such mail to another mail server with the specified IP address (**Redirect to external mail server with IP address** option),
- Reject such mail without accepting it and without notifying senders (**Discard** option).

    This setting can decrease mail server load caused by a large amount of spam, which is often sent to randomly generated user names. However, for spammers, this can somewhat speed up scanning your mail server for valid e-mail addresses.

➢ *To configure the site-wide settings for handling mail to nonexistent users:*

1   Click the **Domains** shortcut in the navigation pane.
2   Click the required domain name in the list.
3   Click **Mail**.
4   Click **Preferences**.
5   Choose a desired option and specify the information as required.
6   Click **OK**.

Introducing Similar Changes to a Number of Mail Accounts at Once

To save time and effort, you can change the settings of multiple mail accounts at once. This feature is called group operations.

➢ *To perform group operations on multiple mail accounts:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail** in the **Services** group.

4 Select the check boxes corresponding to the mail accounts whose settings you want to change.

5 Click **Group Operations**.

6 Adjust the settings as necessary:

- Select **Switch on** to enable the corresponding option for the selected mail accounts.

- Select **Switch off** to disable the corresponding option for the selected mail accounts.

- Leave **Do not change** selected if you don't want to change the corresponding option.

7 Click **OK**.

C H A P T E R 9

Sending E-mail Notices to Multiple Customers at Once

When you need to inform your customers of scheduled server maintenance, or to introduce new service offerings, you can use the Mass E-mail function (**Server > Mass E-mail Messages**) to send notices to all of your customers at once.

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

Read this chapter to learn how to:

Create message templates for further use (on page 241)

Send e-mail to multiple customers (on page 243)

In this chapter:

Creating, Editing and Removing Message Templates

> *To create a new message template:*

1 Go to **Server** > **Mass E-Mail Messages** and click **Add Mass E-Mail Template**.

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

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

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

4 Select the recipients for your e-mail message:

- If you want clients to receive your message, select the **Clients** check box and select the required scope of recipients: **All** to send message to all clients, **Selected only** to send message only to the clients you select manually, **All except selected** to send message to all clients except the ones you select manually.

- To select several clients, click **Select Addresses** to the right of the **Clients** check box (note that this button is not available if **All** mode is selected), select the required clients in the **Available clients** field and click **Add >>**. To remove clients from the list of selected clients, select the required clients in the Selected clients field and click **<< Remove**.

- If you want domain administrators to receive your message, select the **Domain Administrators** check box and select the required scope of recipients: **All** to send message to all domain administrators, **Selected only** to send message only to the domain administrators you select, **All except selected** to send message to all domain administrators except the ones you select.

- To select several domain administrators, click **Select Addresses** to the right of the **Domain Administrators** check box (note that this button is not available if **All** mode is selected), select the required domain administrators in the **Available domain administrators** field and click **Add >>**. To remove domain administrators from the list of selected domain administrators, select the required domain administrators in the **Selected domain administrators** field and click **<< Remove**.

   You can see your choice of selected clients and domain administrators anytime by clicking the respective **Show/Hide Selected** button.

- If you want a copy of the message to be sent to your mailbox, select the **Plesk Administrator** check box.

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

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

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

> *To edit a message template:*

1   Go to **Server** > **Mass E-Mail Messages** and click the required template in the list.

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

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

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

4   Select the recipients for your e-mail message:

   ▪   If you want clients to receive your message, select the **Clients** check box and select the required scope of recipients: **All** to send message to all clients, **Selected only** to send message only to the clients you select manually, **All except selected** to send message to all clients except the ones you select manually.

   ▪   To select several clients, click **Select Addresses** to the right of the **Clients** check box (note that this button is not available if **All** mode is selected), select the required clients in the **Available clients** field and click **Add >>**. To remove clients from the list of selected clients, select the required clients in the Selected clients field and click **<< Remove**.

   ▪   If you want domain administrators to receive your message, select the **Domain Administrators** check box and select the required scope of recipients: **All** to send message to all domain administrators, **Selected only** to send message only to the domain administrators you select, **All except selected** to send message to all domain administrators except the ones you select.

   ▪   To select several domain administrators, click **Select Addresses** to the right of the **Domain Administrators** check box (note that this button is not available if **All** mode is selected), select the required domain administrators in the **Available domain administrators** field and click **Add >>**. To remove domain administrators from the list of selected domain administrators, select the required domain administrators in the **Selected domain administrators** field and click **<< Remove**.

   You can see your choice of selected clients and domain administrators anytime by clicking the respective **Show/Hide Selected** button.

   ▪   If you a copy of the message to be sent to your mailbox, select the **Plesk Administrator** check box.

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

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

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

➢   *To remove a message template:*

1   Go to **Server** > **Mass E-Mail Messages**.

2   Select the check box corresponding to the mass e-mail message template you want to remove and click ✖ **Remove Selected**. Confirm the removal and click **OK**.

Sending E-mail Notices

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

1 Click **Server** in the navigation pane, then click **Mass E-Mail Messages.**

2 If you want to use a message template that you previously created (as described in the Creating, Editing and Removing Message Templates (on page 241) section), click the respective 🔻 icon in the **Create message** column. If you want to send a custom message, click **Send Mass E-Mail**.

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

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

4 Select the recipients for your e-mail message:

▪ If you want clients to receive your message, select the **Clients** check box and select the required scope of recipients: **All** to send message to all clients, **Selected only** to send message only to the clients you select manually, **All except selected** to send message to all clients except the ones you select manually.

▪ To select several clients, click **Select Addresses** to the right of the **Clients** check box (note that this button is not available if **All** mode is selected), select the required clients in the **Available clients** field and click **Add >>**. To remove clients from the list of selected clients, select the required clients in the Selected clients field and click **<< Remove**.

▪ If you want domain administrators to receive your message, select the **Domain Administrators** check box and select the required scope of recipients: **All** to send message to all domain administrators, **Selected only** to send message only to the domain administrators you select, **All except selected** to send message to all domain administrators except the ones you select.

▪ To select several domain administrators, click **Select Addresses** to the right of the **Domain Administrators** check box (note that this button is not available if **All** mode is selected), select the required domain administrators in the **Available domain administrators** field and click **Add >>**. To remove domain administrators from the list of selected domain administrators, select the required domain administrators in the **Selected domain administrators** field and click **<< Remove**.

You can see your choice of selected clients and domain administrators anytime by clicking the respective **Show/Hide Selected** button.

▪ If you want to send a copy of this message to your e-mail, select the **Plesk Administrator** check box.

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

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

7 If you want to save this message (both the text itself and information about its recipients) as a template for further use, select the check box to the left of **Save text to a new template named** field and specify the template name in this field.

8 Click **Send** to send the message. If you have chosen to save the message contents as a template, a template will be created and placed in the list of available templates.

Maintaining Mailing Lists

If you wish to deliver offers and promotions to your customers, run a newsletter, or inform visitors of your site of recent updates, you should set up a mailing list on your site and subscribe your users to it or invite them to subscribe themselves.

Mailing list is a convenient way to reach a number of readers at once: it contains a list of subscribers' e-mail addresses, which are combined under a single e-mail address, to which you post your information or a newsletter. Mailing lists are provided by the GNU Mailman software, which may or may not be installed on your server.

In this section:

Setting Up a Mailing List

> ➢ *To create a mailing list:*

1 Go to **Domains** > *domain name* > **Mail** > **Mailing lists** tab and click **Add New Mailing List**.

2 Specify the desired name for the mailing list.

This can be, for example, a department name, a topic of the mailing list, or any other text in Latin symbols. The name should be short enough to remember. It can comprise alphanumeric, dash, dot and underscore symbols.

3 Specify the mailing list administrator's e-mail.

If you need to change the mailing list administrator's e-mail later, go to **Domains** > *domain name* > **Mail** > **Mailing lists** tab > *mailing list name* > **Preferences** and specify the new e-mail address.

4 Leave the **Notify administrator of the mailing list creation** check box selected.

You will receive instructions on using and managing the mailing list at the administrator's e-mail you specified. Keep that message for your records.

5 Click **OK**.

You will be taken to the page where you can subscribe users to your new mailing list. Refer to the Subscribing and Unsubscribing Users section for more information.

Subscribing and Unsubscribing Users

➢ *To subscribe one user to a mailing list:*

1   Go to **Domains** > *domain name* > **Mail** > **Mailing lists** tab > *mailing list name* and click **Add New Member**.

2   Specify subscriber's e-mail address in the **E-mail** field and click **OK**.

➢ *To subscribe several users to the mailing list:*

1   Create a list of user e-mail addresses you want to add and save it on your computer. The list should be in plain text format and contain one e-mail address per line.

2   Go to **Domains** > *domain name* > **Mail** > **Mailing lists** tab > *mailing list name* and click **Add New Member**.

3   Select **Add from a text file (one e-mail address per line)** option and click **Browse**. In the opened window find your list of user e-mail addresses on your computer and click **OK**.

4   Click **OK** to subscribe the users in your list of user e-mail addresses to the mailing list.

➢ *To unsubscribe users from mailing list:*

1   Go to **Domains** > *domain name* > **Mail** > **Mailing lists** tab > *mailing list name*.

2   Select a check box to the left of the user's e-mail address.

3   Click ✖ **Remove Selected**. Confirm removal and click **OK**.

Exporting The List Of Subscribed Users

➢ *To export the list of users subscribed to a mailing list:*

1   Go to **Domains** > *domain name* > **Mail** > **Mailing lists** tab.

2   Click the 💾 icon corresponding to the required mailing list.

3   Select the place you want to save the list of subscribed users to and click **OK**.

Posting to Your Mailing List

To post a newsletter issue or other information to the mailing list, send it by e-mail to the mailing list's e-mail address. All subscribed users will receive it.

Removing Mailing Lists

> ➢ *To remove a mailing list from site:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the required domain name in the list.

3 Click **Mail**.

4 Click the **Mailing lists** tab.

5 Select a check box corresponding to the mailbox that you wish to remove.

6 Click ✖ **Remove Selected**.

7 When prompted, confirm removal and click **OK**.

Viewing Trouble Tickets in Your Help Desk

➢ *To view the problem reports you have in the Help Desk:*

1 Click the **Help Desk** shortcut in the navigation pane.

2 If you need to view the problem reports submitted by users of this server, go to step 4.

3 If you need to view problem reports submitted to Help Desk on another server you manage using the Master function (as described in the section Using Centralized Access to Your Numerous Plesk Servers (on page 279)), in the **Global Help Desk** group, click **Servers**, then select the server you need.

4 To view new problem reports, in the **Local Tickets** group, click **New**. To view all reports, click **All**. To view all opened and not resolved problem reports, click **All Opened**. To view the tickets the users reopened because they found that their issues were not resolved, click **Reopened**. To review the closed tickets, click **Closed**.

5 The tickets will be listed and the following supplementary information will be displayed:

- **Id**: identification number assigned by the system upon submission,

- **Ticket Subject**: a summary entered by the ticket reporter,

- **Ticket Status**: new, reopened, closed,

- **Reporter Type**: a type of control panel user account or an e-mail address the ticket came from - a client, domain administrator, e-mail user with access to control panel, or user submitted a ticket by e-mail,

- **Reporter Name**: a name of person who submitted the ticket, domain names for tickets submitted by domain owners, or e-mail addresses for tickets submitted by e-mail,

- **Modified**: the date the ticket was modified - a comment appended, or status changed,

- **Queue**: the order in which the problem reporters would prefer their issues to be resolved,

- **Priority**: the severity of a problem estimated by the problem reporter,

- **Category**: the category to which the ticket is related.

6 To see what is inside a ticket, click a ticket id or ticket subject.

Commenting and Closing Trouble Tickets

➢ *To close a ticket when the issue was resolved or to post your comment:*

1 Click the **Help Desk** shortcut in the navigation pane. If you need to visit Help Desk on another server you manage, in the **Global Help Desk** group, click **Servers**, then select the server you need.

2 Locate the ticket you need and click its subject or identification number.

3 To close, reopen or post a comment to the ticket, select the operation you would like to perform from the **Ticket Event** drop-down box, and type a new comment into the **New Comment** input field if required. Click **OK** to submit.

Migrating User Accounts, Domain Names and Web Sites from Other Hosting Platforms

Migration of user accounts, domain names and web sites from other hosting platforms to Plesk control panel is performed by Plesk Migration Manager, created for easy and fast migration from other, competitive control panels to Plesk, and also for migration from different platforms of Plesk.

At the present moment you can migrate the following platforms to Plesk for Windows:

- Helm, Version 3.1.x
- Helm, Version 3.2.x
- Ensim Pro, Version 3.6, 4.0.1
- Plesk for Unix, Version 2.5.x, 5.x, 6.x, 7.1 – 7.5.4

To learn more about performing the migration, refer to the Plesk Migration Manager guide.

Backing Up And Restoring Your Data

With the current version of backup and restore utilities installed with your control panel, you can:

Back up individual domains (Web sites). The backup archive will include all data related to domain administrator account, domain (web site) and mail services, including the contents of mailboxes, anti-spam and anti-virus settings.

Schedule backups. You can schedule the backup of your domains.

Restore your data from backup archives.

Your customers granted with the permission to use the backup and restore facilities can back up and restore their own account settings and Web sites through the control panel. Your customers will find shortcuts to their backup repositories on their Home pages (**Home** > **Backup**).

To backup and restore clients data and server data, you need to use external backup/restore utilities provided with Plesk. To learn more, refer to the Backup/Restore Utilities guide.

In this chapter:

Backing Up Individual Domains (Web Sites)

➢ *To back up a domain (web site):*

1 Click **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Backup** in the **Domain** group.

4 Click **Create Backup** in the **Tools** group.

5 Select the backup method from the **Backup method** list.

  ▪ Select the **create backup file and store in repository** option to create and store the backup file on the Plesk server.

  ▪ Select the **do not store the backup file in repository, only download it** option to store the backup file on the local machine.

  ▪ To create and save the backup file on FTP server, select the **create the backup file and store on FTP server** option, and follow these steps:

  1. Specify the FTP server name in the **FTP server** text input field.

  2. Type the name of the FTP server directory where the domain backups are stored in the **Base directory on FTP server** text input field.

  3. Enter the FTP server login in the **FTP Login** text input field.

  4. Enter the FTP password in the **FTP Password** text input field.

  5. If required, select the **Use passive mode** checkbox.

  Note. The **FTP server**, **Base directory on FTP server**, **FTP Login** and **FTP Password** fields will be automatically filled if the FTP account settings have been previously specified (at **Domains** > Domain name > **Back up** > **FTP Account Properties**).

6 Specify the **Backup file name**.

7 Type your comments in the **Comments** text input field.

8 Select the **Suspend domain** checkbox, if you wish to suspend all domain activity during the backup. Note that suspended domains aren't available to the visitors.

9 Select the **Notify by e-mail** checkbox and enter the e-mail address if you wish to receive notifications of backup procedures start and completion.

10 Click **Back Up**. The process of backing up will start.

  Note. If you have selected the **do not store the backup file in repository, only download it** option, the **File Download** dialog window will appear. Specify the location on your local machine where the backup file should be stored and then click **Save**.

11 Upon completion of the backup process you will be shown a window displaying the backup results, including errors, if they were encountered. Click **OK**.

Backing Up Your Databases

Plesk allows you to back up and subsequently restore the databases used by domains hosted on your server, including their users and content. You can:

- Back up your domain databases with all data and users
- Restore databases from backup files
- Download, upload and remove database backup files
- Recover users who became orphaned after the restoration.

In this section:

Backing Up Databases

➢ *To back up a database:*

1   Go to **Domains** > *domain name* > **Databases** > *database name* and click **Back Up Now**.

2   Specify the name of the backup file and click **OK**.

3   If you want to download the resulting backup file, click the file name on the next page after the backup process was finished. Specify the location where you want to save the file and click **Save**.

4   Click **OK**.

➢ *To back up all databases on your domain:*

1   Go to **Domains** > *domain name* > **Back Up** > **Database Backup Repository**, make sure that **All domain repositories** is selected in the **Database** field, and click **Back Up Now**.

2   Specify the name of the backup file and click **OK**.

3   If you want to download the resulting backup file, click the file name on the next page after the backup process was finished. Specify the location where you want to save the file and click **Save**.

4   Click **OK**.

Restoring Databases

➢ *If the database already exists and you only need to restore its contents:*

1 Go to **Domains** > *domain name* > **Databases** > *database name* > **Database Backup Repository**, select the required backup file from the list and click **Restore Selected**.

If you do not have the backup file on your server, you can upload the backup file to the server repository from your local machine. Refer to Uploading Database Backup Files To Server (on page 257) section for more information.

2 Confirm the restoration by selecting the corresponding check box and click **OK**.

If you are restoring MS SQL database, there is a possibility that some database users will be orphaned. In order to provide the ability to access and use the database for these users, you need to repair them. Refer to Recovering Orphaned Database Users (on page 258) section for more information.

➢ *If the database does not exist and you need to recreate it from scratch:*

1 Go to **Domains** > *domain name* > **Databases** and click **Add New Database**.

2 Specify the database name, type and server for the database you are restoring.

> **Note.** You can specify a new database name, but you must choose the correct database type: for example, if you are trying to restore a MySQL database, choose MySQL database type.

3 Select the **Restore database from backup file** check box.

4 Specify the location of the database backup file. You can upload a backup file from your local machine or specify a file located on the server.

5 Provide the default username and password for the restored database.

6 Click **OK**.

If you are restoring MS SQL database, there is a possibility that some database users will be orphaned. In order to provide the ability to access and use the database for these users, you need to repair them. Refer to Recovering Orphaned Database Users (on page 258) section for more information.

Maintaining Database Backup Files Repository

Your database backup files are stored in your own database backup repository, accessible by going to **Domains** > *domain name* > **Backup** > **Database Backup Repository** on your home page. Each database has its own backup files repository. To see backup files for a specific database, select the required database from the **Database** menu. By default, the database backup repository shows backup files for all databases on a domain.

In the database backup repository you can:

- Upload database backup files stored on another computer
- Download database backup files to another computer

Remove redundant database backup files from database backup repository

In this section:

Uploading Database Backup Files To Server

➢ *To upload a backup file to backup repository:*

1   Go to **Domains** > *domain name* > **Backup** > **Database Backup Repository** and
    click **Upload Backup File**.

2   Select the database in which repository you want to upload the
    backup file to in the **Database name** menu.

3   Click **Browse...** and select the required backup file.

4   Leave the **Restore database backup immediately upon uploading** check box
    selected if you want the database contents to be restored immediately
    after the backup file is uploaded.

5   Click **OK**.

   The database backup file will be uploaded to the backup repository of the
   specified database.

Downloading Database Backup Files From Server

➢ *To download a backup file from backup repository:*

1   Go to **Domains** > *domain name* > **Backup** > **Database Backup Repository.**

2   Select the database which backup files you want to browse in the
    Database menu. Leave **All domain databases** selected if you want to browse
    backup files of all databases on a domain.

3   Click 🖫 icon corresponding to the database backup file you want to
    download

4   Select the location where you want to save the backup file and click
    Save.

The backup file will be downloaded from the backup repository.

Removing Database Backup Files From Server

➢ *To download a backup file from backup repository:*

1   Go to **Domains** > *domain name* > **Backup** > **Database Backup Repository.**

2   Select the database which backup files you want to browse in the
    Database menu. Leave **All domain databases** selected if you want to browse
    backup files of all databases on a domain.

3   Select a check box corresponding to the database backup file you
    wish to remove. Click ✖ **Remove Selected**, confirm removal and click **OK**.

Recovering Orphaned Database Users

If you are restoring MS SQL database, there is a possibility that some database users will be orphaned. In order to provide the ability to access and use the database for these users, you need to repair them.

➢ *To check if a database has orphaned users:*

1   Go to **Domains** > *domain name* > **Databases** > *database name*.

2   If you see a warning saying that there are several orphaned users that should be repaired in order to function properly, you have orphaned users who need to be repaired.

➢ *To repair orphaned users:*

1   Go to **Domains** > *domain name* > **Databases** > *database name* and click **Repair now** button corresponding to the orphaned user you want to repair.

2   Provide a password for this user and click **Repair**.

If a user is supposed to be a sysuser without a password, run repair with empty password field.

3   Repeat steps 1-2 as necessary to repair all orphaned users.

Scheduling Backups

➢ *To schedule backup of a single domain (web site):*

1 Click **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Backup** in the **Tools** group.

4 Click **Scheduled Backup Settings** in the **Tools** group.

5 Specify when and how often to perform backup.

6 Select the backup repository files location:

- **Domain dumps** - backup files are stored on Plesk server.

- **FTP** - backup files are stored on the remote FTP. If you select this option, you need to specify the path to the FTP server, FTP credentials (login and password) and base FTP directory in the corresponding fields on the **FTP Account Properties** page. If required, select the **Use passive mode** checkbox (**Domains** > **domain name** > **Backup** > **FTP Account Properties**).

7 Specify the maximum number of stored backup files in the corresponding field.

8 Specify the combination of symbols that backup file names should begin with. This will help you distinguish between backup files.

9 Select the **Suspend domain** checkbox, if you wish to suspend all domain activity during the backup. Note that suspended domains aren't available to the visitors.

10 Click **Switch On** in the **Tools** group.

11 Click **OK**.

Restoring Data from Backup Archives

> ➢ *To restore a domain (Web site):*

1 Click **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Backup** in the **Tools** group.

4 Click the backup file name you need.

5 Select the **Suspend domain** checkbox, if you wish to suspend all domain activity during the restore. Note that suspended domains aren't available to the visitors.

6 Select the **Nofity by e-mail** checkbox and specify the e-mail, if you want to be notified about the restore.

7 Click **Restore**.

8 Upon completion of the restoring process you will be shown a window displaying the restoration results, including errors, if they were encountered.

9 Click **OK**.

Maintaining Backup Files Repository

Domain backups are usually stored in separate backup repositories for each domain hosted on your server. They are accessed by clicking **Domains** shortcut, clicking the required domain name and clicking **Backup**. You can manage these backup repositories by:

- Uploading backup files stored on another computer
- Downloading backup files to another computer
- Removing redundant backup files from backup repository

In this section:

Uploading Backup Files to Server

➢ *To upload backup file to the backup repository:*

1 Click **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Backup** in the **Tools** group.

4 Click **Browse...** and select the required backup file.

5 Click **Upload**.

6 Click **OK**.

The backup file will be uploaded to the backup repository.

➢ *To upload backup file to the backup repository from FTP:*

1 Click **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Backup** in the **Tools** group.

4 Click **FTP Account Properties**.

5 Specify the path to the FTP server, FTP credentials (login and password) and base FTP directory in the corresponding fields.

6 Click **OK**. This will return you to the previous screen.

7 Click **Browse...** and select the required backup file.

8 Click **FTP Upload**.

9 Click **OK**.

The backup file will be uploaded to the backup repository.

Downloading Backup Files from Server

➢ *To download backup file from the backup repository:*

1 Click **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Backup** in the **Tools** group.

4 Click the 🖫 icon corresponding to the backup file you wish to download.

5 Select the location where you wish to save the backup file and click **Save**.

The backup file will be downloaded from the backup repository.

Removing Backup Files from Server

➢ *To remove backup file from the backup repository:*

1 Click **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Backup** in the **Tools** group.

4 Select a checkbox corresponding to the backup file you wish to remove.

5 Click ✕ **Remove Selected**.

6 Confirm removal and click **OK**.

C H A P T E R   1 2

Viewing Statistics

> ➢ *To view the information on server usage:*

1 Click the **Server** shortcut in the navigation pane.

2 Click **Statistics** in the **System** group.

The following information will be presented:

- Processor information.
- Plesk version and build number.
- Operating system and its kernel version.
- Plesk license key number.
- Server uptime.
- Processor load averages for the last 1 minute, 5 minutes and 15 minutes.
- The amount of RAM installed and used.
- The amount of swap space used.
- Hard disk usage by partitions and directories.
- The connected (mounted) storage and network storage devices.
- The number of hosted domains: **active** shows the domains that are online; **problem** shows the domain that have exceeded the disk space and bandwidth allotments but still online; **passive** shows the domains that are offline because they were suspended by you or your resellers.

3 Click **Refresh** to update the server statistics with the latest data.

> ➢ *To view the information on software components installed on your server and managed by the Plesk control panel:*

1 Click the **Server** shortcut in the navigation pane.

2 Click **Components Management** in the **System** group.

3 Click **Refresh** to update the information.

> ➢ *To view a consolidated report on a user account and user's sites:*

1 Click the **Clients** shortcut in the navigation pane.

2 Click the user name you need.

3 Click **Report** in the **Tools** group.

➢ *To view a detailed report on server resources and hosting features used by a specific domain name/web site:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Report**.

➢ *Common operations on reports:*

▪ To get more details, select the **Full Report** option from the **Report** drop-down menu.

▪ To adjust the amount of information presented in a report, click 🔧 **Customize**, and then modify an existing report template (to do this, click a report template name) or create a new report template (to do this, click **Add New Layout**). Next, specify how much information you want in each section of the report: select **None** if you do not want any information, select **Summary** if you want a concise overview, or select **Full** if you need a detailed report. Select the **Use as default report** check box and click **OK**. To delete a custom report layout, select the checkbox corresponding to the report layout name and click ✖ **Remove Selected**.

▪ To print the report, click 🖨 **Print**. A report will open in a separate browser window. Select the **File** > **Print** option from the browser's menu to print the report.

▪ To send the report by e-mail, type the recipient's e-mail address into the input box located to the right of the Report group and click 📧 **Send by E-mail**. If you are the recipient, then you do not need to specify an e-mail address: the system assumes by default that you are the report recipient and specifies your e-mail address registered with your control panel account.

▪ To have the reports automatically generated and delivered by e-mail on a daily, weekly, or monthly basis, click **Report Delivery** and follow the instructions supplied in the "Automating report generation and delivery by e-mail" section.

➢ *To find out how many people visited a site, from what countries, and what pages of the site they viewed:*

1 Click the **Domains** shortcut in the navigation pane.

2 Click the domain name you need.

3 Click **Report**.

4 View the statistics for the web pages or files downloaded from or uploaded to specific areas of your site:

▪ To view the statistics for web pages transferred from your site over hypertext transfer protocol (HTTP), click **Web Stats**.

▪ To view the statistics for web pages transferred from your site over secure hypertext transfer protocol (HTTPS), click **Web Stats SSL**.

▪ To view statistics for files transferred over file transfer protocol (FTP), click **FTP Stats**.

▪ To view the bandwidth usage by months, click **Traffic History**.

▪ To view the bandwidth usage by FTP, Web and mail services in this domain, click **Traffic**.

Alternately, you can view the Web statistics for a site by visiting the following URL: https://your-domain.com/plesk-stat. When prompted for username and password, specify the FTP account credentials.

In this chapter:

Viewing Kaspersky Antivirus and Spamassassin Statistics

> ➢ *To view the information about viruses detected and removed by Kaspersky Antivirus:*

1 Go to **Server** > **Mail** > **Statistics** tab and click **Virus Statistics**.

2 Select the period for which you want to view virus statistics.

> If you want to view more detailed information about viruses, or e-mail addresses of e-mail senders or recipients, click the respective tab.

> ➢ *To view the information about spam messages detected and filtered by Spamassassin:*

1 Go to **Server** > **Mail** > **Statistics** tab and click **Spam Statistics**.

2 Select the period for which you want to view spam statistics.

> If you want to view more detailed information about spam message recipients, click the **Recipients** tab.

Automating Report Generation and Delivery by E-mail

> ➢ *To receive consolidated reports on one or several user accounts on a regular basis:*

1 Go to **Clients** > *client name* > **Report** > **Layouts** > *report type* > **Report Delivery** > **New Delivery Schedule**.

2 To receive the report to your e-mail address registered with the system, select the **the server administrator** value from the **Deliver to** drop-down menu. To receive the report to another e-mail address, select the **the e-mail address I specify** option and type the e-mail address. To send the reports to the client, select the **the client** option. To send the client reports to all respective clients, select the **Report on all clients** option.

3 Select the delivery interval from the **Delivery frequency** drop-down menu and click **OK**. You can have the report delivered each day, each week, or each month.

> ➢ *To change the delivery schedule for an account status report:*

1 Go to **Clients** > *client name* > **Report** > **Layouts** > *report type* > **Report Delivery**.

2 Under the **Frequency** column, click a hyperlink corresponding to the delivery schedule you would like to change.

3 Adjust the settings as required and click **OK**.

➢ *To stop receiving the account status reports:*

1 Go to **Clients** > *client name* > **Report** > **Layouts** > *report type* > **Report Delivery**.

2 Select a check box corresponding to the delivery schedule and click ✖ **Remove Selected**. Confirm removal and click **OK**.

➢ *To receive detailed reports on one or several domains/web sites on a regular basis:*

1 Go to **Domains** > *domain name* > **Report** > **Layouts** > *report type* > **Report Delivery** > **New Delivery Schedule**.

2 To receive the report to your e-mail address registered with the system, select the server administrator value from the **Deliver to** drop-down menu. To receive the report to another e-mail address, select the **e-mail address I specify** option and type the e-mail address. If this domain name/web site belongs to another user, you may want to send the report to that user: select the **client** or **domain administrator** option.

3 To receive a report on a given domain/web site, leave **this domain** option selected. To receive detailed reports on each domain that belongs to a given user account, select the **all domains of this client** option. To receive reports on all domains hosted on the server, select the **all domains** option.

4 Select the delivery interval from the **Delivery frequency** drop-down menu and click **OK**. You can have the report delivered each day, each week, or each month.

➢ *To change the delivery schedule for a detailed domain/web site report:*

1 Go to **Domains** > *domain name* > **Report** > **Layouts** > *report type* > **Report Delivery**.

2 Under the **Frequency** column, click a hyperlink corresponding to the delivery schedule you would like to change.

3 Adjust the settings as required and click **OK**.

➢ *To stop receiving the domain reports:*

1 Go to **Domains** > *domain name* > **Report** > **Layouts** > *report type* > **Report Delivery**.

2 Select a check box corresponding to the delivery schedule and click ✖ **Remove Selected**. Confirm removal and click **OK**.

Viewing Log Files and Configuring Recycling of Log Files

All connections to the Web server and requests for files that were not found on the server are registered in log files. These log files are analyzed by the statistical utilities running on the server, which then present graphical reports on demand. You may want to download these log files to your computer for processing by third-party statistical utilities, or view their contents for web server debugging purposes.

➢ *To prevent these log files from growing too large, you should enable automatic cleanup and recycling of log files:*

1 Go to **Domains** > *domain name* > **Log Manager** > **Log Rotation** and click **Switch On**. If you see only **Switch off** there, this means that log recycling is already switched on.

2 Specify when to recycle log files and how many instances of each log file to store on the server. Also specify whether they should be compressed and sent to an e-mail address after processing. Click **OK**.

➢ *To view the contents of a log file or download it to your computer:*

1 Go to **Domains** > *domain name* and click **Log Manager** in the **Hosting** group. A list of log files will show.

- To specify the number of lines from the end of the log file that you would like to view, type a number into the input box under the **Preferences** group.

- To view the contents of a log file, click its file name.

- To download a file to your computer, click an icon 💾 corresponding to the file you need.

- To remove a processed log file from the server, select a corresponding check box and click ✖ **Remove Selected**. Confirm removal and click **OK**.

Monitoring Connections to Control Panel, FTP Services and Plesk Server

In this chapter:

Monitoring Connections to Control Panel

> ➢ *To find out who of your customers is logged in to the control panel at the moment:*

1 Click **Sessions** in the navigation pane. All sessions including yours will be presented and the following details will be displayed:

- **Type**. A type of control panel user who established the session:

  for server administrator.

  for client.

  for domain or Web site owner.

  for mailbox owner.

- **Login**. The login name the user is logged in as.

- **IP address**. The IP address from which the control panel is accessed.

- **Logon time**. The date and time when the user logged in to the control panel.

- **Idle time**. The time that user was not doing anything in the control panel while being logged in.

2 To refresh the list of user sessions, click **Refresh**.

3 To end a user session, select the respective check box and click ✖ **Remove Selected**, then confirm removal and click **OK**.

Monitoring Connections to FTP Service

> ➢ *To find out who is connected to your server via FTP, in what directories they currently are and what files they are uploading to or downloading from the server:*

1 Click **Sessions** in the navigation pane.

2 Click the **FTP Sessions** tab. All sessions including yours will be presented and the following details will be displayed:

- **Type**. The type of user who established the session:

  for users not registered with the control panel.

  for anonymous FTP users.

  for domain or web site administrators.

  for subdomain administrators.

  for web users (owners of personal web pages without individual domain names).

- **Status**. The current status of FTP connection.

- **FTP user login**. The login name used for access to FTP account.

- **Domain name**. The domain the FTP user is currently connected to.

- **Current location**. The directory the FTP user is currently at.

- **File name**. The file name being operated on.

- **Speed**. Transfer speed in kilobytes.

- **Progress, %**. The file transfer operation progress in percentage.

- **IP address**. The IP address from which the FTP account is accessed.

- **Logon time**. The time lapsed since the moment user logged in.

- **Idle time**. The time that user was not doing anything while being connected to the server through FTP.

3 To refresh the list of FTP sessions, click **Refresh**.

4 To end a session, select the respective check box and click ✖ **Remove Selected**.

Monitoring Terminal Session Connections to Your Server

> ➢ *To find out who of your customers is logged in to the server via Terminal Server session at the moment:*

1 Click **Sessions** in the navigation pane and click the **TS Sessions** tab. All sessions including yours will be presented and the following details will be displayed:

- **S**. The status of the terminal session:

  ⚠ - for server administrator.

  ✅ - client is connected and logged in, using valid login and password.

  ▶ - client is connected, but not logged in.

  ❌ - client is disconnected.

- **Name**. The name of this terminal session.

- **User**. The name of the terminal session user.

  You can see the session details by clicking the session name in the list.

2 To refresh the list of terminal sessions, click **Refresh**.

3 To disconnect a terminal session, select the respective check box and click 🔌 **Disconnect**, then confirm disconnection and click **OK**.

4 To log out a terminal session, select the respective check box and click 🔑 **Log Out**, then confirm disconnection and click **OK**.

Accessing The Server Via Remote Desktop (RDP)

The remote desktop (RDP) access feature allows you to remotely login to the Plesk server and interact with it via standard Microsoft Windows desktop interface.

> ➢ *To access the server via Remote Desktop interface:*

1 Click **Server** in the navigation pane.

2 Click **Remote Desktop** in the **Services** group.

3 Set up screen resolution for the session in the **Screen resolution for terminal session** menu.

Note: Higher resolutions are more taxing for your connection, decreasing the interaction speed and spending more bandwidth.

---

4 Choose the connection method according to your browser:

- **Microsoft RDP ActiveX** - recommended to use with Internet Explorer browser, since it may not work with other browsers. When you use this method for the first time, your browser will automatically install the required ActiveX component, if Internet Explorer security settings permit this. If your browser displays security alerts, try to temporarily lower security measures in the browser options.

- **properoJavaRDP** - recommended to use with Netscape, Mozilla, or Firefox browsers, since it may not work with Internet Explorer. Only 8.0 and higher versions of Opera are supported. This component requires Java Runtime Environment (JRE) to be installed on your system. If you do not have JRE, you can download it from http://java.sun.com/j2se/1.5.0/download.jsp (version 1.4 and higher) and install it before using the remote desktop feature.

Note: You don't need to install JDK (Java Development Kit) in order for the RDP feature to work.

If you use Internet Explorer or Mozilla, you should open the Terminal Services Configuration console in the Microsoft Windows (**Start** > **Administrative Tasks**), and set the **Licensing** option to **Per user** on the **Server Settings** screen.

5 Click **OK**. A new window will open with an area where your interaction with the server's desktop will take place.

6 Log in to the system. By default, Plesk uses the domain's FTP/Microsoft FrontPage login. You can supply any valid login and password.

7 After logging in to the system you can start working with it as with regular Windows desktop.

To finish your Remote Desktop session:

- Close the browser window with the remote desktop session. This way, the session you had will be detached from your desktop, but it will keep running on the server, so when you log in there next time, you will see the remote desktop in the state you left it,

  or

- Select **Start** > **Log off** if you want to quit the session permanently (all running sessions consume the server's resources).

Logging Actions Performed by Your Customers in the Control Panel

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

- Administrator information changed
- System service restarted, started, or stopped
- IP address added, removed, changed
- Login settings (allowed period of inactivity for all user sessions in the control panel) changed
- Client account created, deleted, personal or system information changed
- The status of client account changed (suspended/unsuspended)
- Client's interface preferences changed
- Client's IP pool changed
- Site applications were added to or removed from a client's pool
- The limit on disk space is reached for a client account
- The limit on traffic usage is reached for a client account
- A Desktop preset was created, deleted, or modified
- The limit on disk space is reached for a domain
- The limit on traffic usage is reached for a domain
- Domain administrator account properties changed
- Domain created, deleted, settings changed
- Domain owner changed
- Domain status changed (suspended/unsuspended)
- DNS zone updated for a domain
- Subdomain created, deleted, settings changed
- Domain alias created, deleted, settings changed
- DNS zone of the domain alias changed
- Client account limits (resource allotments) changed
- Client's permissions changed
- Domain limits (resource allotments) changed
- Users logged in and out of the control panel
- Mail accounts created, deleted, changed
- Mailing lists created, deleted, settings changed
- Physical hosting created, deleted, changed
- Standard or frame forwarding hosting accounts were created, deleted, reconfigured

- Web user account created, deleted, changed
- Site application installed, reconfigured, uninstalled
- Site application package installed, uninstalled, updated
- License key expired or updated
- Database server created, deleted, updated
- Database created or deleted
- Database user account created, deleted, updated
- Client's GUID updated
- Domain's GUID updated
- Plesk component was updated or added

In this chapter:

Setting Up Action Logging

> *To set up action logging:*

1 Select the **Server** shortcut in the navigation pane.

2 Click **Action Log** in the **Control Panel** group.

3 In the **Logged actions** group, select the actions to be logged using the check boxes.

4 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.

5 To retain all action log records, select the **Do not remove records** option.

6 To apply all the changes made, click **OK**.

Downloading the Action Log

➢ *To download the action log to your machine:*

1 Go to **Server** > **Action Log**.

2 In the **Log files** section, select the time period using the drop-down boxes, and click **Download**.

   The dialog window will open, prompting you to select the location for the downloaded log file to be saved to.

3 Select the location, and click **Save**.

Clearing the Action Log

➢ *To clear the action log:*

1 Go to **Server** > **Action Log**.

2 In the **Log files** section, click **Clear Log**.

Using Event Tracking Mechanism

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

In this section:

Adding Event Handlers

> ➢ *To add 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\parallels\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 **Event Manager** in the **Control Panel** group.

3 Click **Add New Event Handler**. The event handler setup page appears:

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

5 Select the priority for handler execution, or specify a custom value. To do this, select custom in the **Priority** drop-down list and type in the value.

   When assigning several handlers to a single event you can specify the handler execution sequence, setting different priorities (higher value corresponds to a higher priority).

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

7 In the **Command** input field, specify a command to be executed upon the selected event. In our example it is `c:\program files\parallels\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**.

Note: In the command we have specified the parameters in the angle brackets `<new_contact_name>` and `<new_login_name>`. Before executing the handler, they will be replaced with name and login of the created client respectively. The entire list of available parameters is provided below. You should keep in mind that with the removal operations, the parameters of type new_xxx contain an empty string. And with creation operations the parameters of type old_xxx contain an empty string.

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

To learn more about the events that can be processed by the Event Handler, please refer to Plesk for Windows Advanced Administration Guide.

Removing Event Handlers

➢ *To remove an event handler:*

1 Select the **Server** shortcut in the navigation pane.

2 Click **Event Manager** in the **Control Panel** group.

3 Select the corresponding check boxes in the list of handlers and click ✖ **Remove selected**.

Using Centralized Access to Your Numerous Plesk Servers

If you have a number of Plesk-managed servers, you can use the control panel on one of your servers for accessing and managing the other servers. To check if this feature is available within your control panel, see if there is the **Master** shortcut in the navigation pane.

What the Master function can do for you is remember your credentials for accessing other Plesk-managed servers (almost like your Web browser's password manager): When you need to log in to control panel on any of your servers, you will need to get to the list of your slave servers in the control panel and click an icon. The control panel running on another server will open in a new browser window.

In addition to giving you a single point of entry to a number of servers, the Master function can also poll other servers you specify, retrieve information on state of system services and resource usage, and display this information in your control panel.

As you can see, the Master function can only save you a little time and a few clicks, that is all it really does. If you have numerous servers and need truly centralized server management, you should use Plesk Expand or Parallels Business Automation solutions by Parallels.

In this chapter:

Adding a Server Record

> ➢ *To add a record on a Plesk-managed server to your control panel:*

1 Go to **Master** > **Add New Server**.

2 Enter the hostname and port number (8443) in the respective fields, specify 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** check box, if you do not want the detailed server information to be retrieved and presented at that time.

3 Click **Set**.

4 To upload an SSL certificate that will be used for secure connection to that server's control panel, click the **Certificate** button. Click **Browse...** to locate your certificate file or paste the certificate contents from the clipboard. After that, click the **Send File** or **Send Text** button respectively to upload the certificate to the slave server.

When you need to modify a server record, click the **Master** shortcut in the navigation pane, and then click the host name you need.

Viewing Server Information and Logging in to a Server

> ➢ *To view information on a server and to log in to the server's control panel:*

1 Click the **Master** shortcut in the navigation pane.

The following information is displayed for all servers you added:

- Status icon in the **S** column:

    ✅ - the server is in operable state and there is no resource overage,

    ⛔ - some system service is down,

    ⚠️ - there is at least one user account that exceeded resource (disk space or bandwidth) allotments,

    ❌ - the server is down or inaccessible,

    ❓ - the server was not polled for its status.

- **Hostname**.

- **Description** you specified.

2 To view a detailed server report, click the hostname you need.

3 To log in to the server's control panel, click the respective 🟨 icon.

Removing a Server Record

➢ *To remove a server record:*

1 Click the **Master** shortcut in the navigation pane.

2 Select the check box corresponding to the record you wish to remove.

3 Click ✖ **Remove Selected**. Then, confirm removal and click **OK**.

Upgrading Your Control Panel

You can easily install the necessary updates and even upgrade your control panel to the latest available release using the Updater function within your control panel.

➢ **To update your Plesk control panel:**

1 Click the **Server** shortcut in the navigation pane.

2 Click **Updater** in the **Services** group.

   The control panel connects to the Parallels official Plesk Update server at URL http://autoinstall.plesk.com, retrieves information on the available releases, then analyses the components installed in the system and displays the lists of available releases and component updates. For each release a brief description of available operations is displayed.

   > **Note.** To see the list of the already installed updates, click the **Installed Updates** tab.

3 Select the check boxes corresponding to the updates you wish to install and click **Install**. A confirmation screen appears.

4 Specify your e-mail address. You will be sent a notice by e-mail once update is completed. To confirm installation of the selected updates, select the check box and click **OK**. The updates you selected will be downloaded and automatically installed in the background mode.

You can also install all necessary updates by using external Plesk Auto Updater utility.

➢ **To upgrade your Plesk control panel via Plesk Auto Updater utility:**

1 Open the **Start** menu > **All Programs** > **Parallels** > **Plesk** > **Plesk Auto Updater**. Plesk Auto Updater will connect to Parallels Web site and retrieve the list of available updates.

2 After Plesk Auto Updater retrieves the list of available updates from Parallels Web site, select the check boxes corresponding to the components you wish to install.

3 Click **Install**.

   Your selected updates will be first downloaded and then installed. Follow the instructions of the Installation Wizard that will guide you through the installation process.

   Depending on the importance of installed updates, Plesk might prompt you to restart your server. It is highly recommended to restart the server, otherwise your control panel might not work properly.

   Notes on updating procedures:

When upgrading to a new control panel version, you will be notified by e-mail of upgrade procedure start and end. The notification message will include the event log and a list of installed components, if upgrade is successful. However, you may not receive any error notice if your mail server fails. In this case you can check for errors in the autoinstaller.log file located on the server hard drive.

All control panel operations are suspended during the installation of control panel components that affect the control panel's core functionality.

If you need to install a new license key after upgrade, refer to the Upgrading Your License Key (on page 26) section. If you experience any problems with installing a license key, please contact sales@parallels.com (sales@parallels.com).

In this chapter:

Setting Up Plesk Auto Updater to Notify You About Control Panel Updates

You can configure Plesk to notify you that updates for your Plesk control panel are available, so that you know it is time to update your Plesk server.

➢ *To make Plesk Auto Updater notify you when Plesk updates are available:*

1 Go to **Server** > **Updater**.

2 Click the **Automatic Update** tab.

3 Select the **Switch on automatic update of Plesk** check box.

4 In the **Check for updates** and **at** fields select date and time when Plesk Auto Updater should connect to Parallels Web site and check for updates.

5 Select what should Auto Updater do when it finds that Plesk updates are available:

- **Notify that updates are available for download. Do not download and install any updates automatically** - a notification is sent to you when updates are available, so that you can update Plesk manually.

- **Download the updates automatically. Notify that updates are downloaded and ready to be installed** - updates are downloaded automatically in the background; notification is sent to you so that you can update Plesk manually without downloading the updates.

6 Select notification options in the **Notification settings** section:

- **To e-mail** - specify the e-mail address to which Plesk Auto Updater should send the notifications.

- **From e-mail** - specify the e-mail address from which Plesk Auto Updater should send the notifications.

- **Subject** - specify the subject of notification e-mails. The default subject is "The Plesk Auto Updater notification".

7 Click **OK**.

You can also configure Plesk Auto Updater utility to notify you that updates for your Plesk control panel are available, so that you know it's time to update your Plesk server.

➢ *To make Plesk Auto Updater utility notify you when Plesk updates are available:*

1 Open the **Start** menu > **All Programs** > **Parallels** > **Plesk** > **Configure Auto Updater**.

2 Select the **Switch on automatic update of Plesk** check box.

3   In the **Check for updates** and **at** fields select date and time when Plesk Auto Updater should connect to Parallels Web site and check for updates.

4   Select what should Auto Updater do when it finds that Plesk updates are available:

- **Notify that updates are available for download. Do not download and install any updates automatically** - a notification is sent to you when updates are available, so that you can update Plesk manually.

- **Download the updates automatically. Notify that updates are downloaded and ready to be installed** - updates are downloaded automatically in the background; notification is sent to you so that you can update Plesk manually without downloading the updates.

5   Select notification options in the **Notification settings** section:

- **To e-mail** - specify the e-mail address to which Plesk Auto Updater should send the notifications.

- **From e-mail** - specify the e-mail address from which Plesk Auto Updater should send the notifications.

- **Subject** - specify the subject of notification e-mails. The default subject is "The Plesk Auto Updater notification".

6   Click **Apply**.

Configuring Automatic Updates of Your Control Panel

If you do not want to install updates manually, you can configure Plesk Auto Updater to download and install updates without your intervention, keeping Plesk up-to-date automatically.

➢ *To make Plesk Auto Updater automatically update your Plesk control panel:*

1 Go to **Server >** **Updater**.

2 Click the **Auto Updater Settings** tab.

3 Select the **Switch on automatic update of Plesk** checkbox.

4 In the **Check for updates** and **at** fields select date and time when Plesk Auto Updater should connect to Parallels Web site and check for updates.

5 Select the **Download and install the updates automatically. Notify that updates were downloaded and installed** option. The updates will be downloaded and installed automatically, and two notifications will be sent to you, letting you know that updates were downloaded and installed correspondingly.

6 Select notification options in the **Notification settings** section:

   ▪ **To e-mail** - specify the e-mail address to which Plesk Auto Updater should send the notifications.

   ▪ **From e-mail** - specify the e-mail address from which Plesk Auto Updater should send the notifications.

   ▪ **Subject** - specify the subject of notification e-mails. The default subject is "The Plesk Auto Updater notification".

7 Click **OK**.

If you do not want to install updates manually, you can configure Plesk Auto Updater to download and install updates without your intervention, keeping Plesk up-to-date automatically.

➢ *To make Plesk Auto Updater utility automatically update your Plesk control panel:*

1 Open the **Start** menu > **All Programs** > **Parallels** > **Plesk** > **Configure Auto Updater**.

2 Select the **Switch on automatic update of Plesk** checkbox.

3 In the **Check for updates** and **at** fields select date and time when Plesk Auto Updater should connect to Parallels Web site and check for updates.

4 Select the **Download and install the updates automatically. Notify that updates were downloaded and installed** option. The updates will be downloaded and installed automatically, and two notifications will be sent to you, letting you know that updates were downloaded and installed correspondingly.

5 Select notification options in the **Notification settings** section:

- **To e-mail** - specify the e-mail address to which Plesk Auto Updater should send the notifications.

- **From e-mail** - specify the e-mail address from which Plesk Auto Updater should send the notifications.

- **Subject** - specify the subject of notification e-mails. The default subject is "The Plesk Auto Updater notification".

6 Click **Apply**.

Note. You may receive a notice in the notification message saying that a certain update couldn't be installed in silent mode. If you receive such a notice, please update Plesk manually using the Plesk Auto Updater.

Setting Up a Custom Updates Server for Plesk Updates

If you maintain a great number of Plesk servers, to reduce bandwidth usage, you may want to set up a mirror of the official Plesk Update server inside your network, and then configure your Plesk servers to use it.

You can set up a mirror on any networked computer with Linux or Windows operating system and Web server installed. The following instruction provides the steps for setting up a mirror on Windows-based servers:

1 Download the `MirrorManager.exe` utility from Parallels site at www.parallels.com.

2 Copy or move the utility to the server where you want to set up the mirror.

3 Run the utility. The utility retrieves a list of available updates from Parallels server, and shows it in the **Server Configuration File** window.

4 To create a new blank configuration file, click **New file**. Note that you can also make a copy of the configuration file retrieved from Parallels Updates server (shown in the **Server Configuration File** window), and then remove the unwanted updates from the list. To make a copy of the original configuration file, from the **File** menu, select **Duplicate Server Configuration**.

5 To arrange conveniently the windows on the screen, from the **Window** menu, select **Tile Vertically**.

6   Decide which updates you would like to make available from your mirror server, select them in the **Server Configuration File** window, and click **Download**. When prompted, specify the Web server's directory where you want to place updates, such as `C:\Inetpub\vhosts\default\htdocs\Updates`. Click **OK**.

7   From the **Server Configuration File** window, drag the selected updates to the new window on the left.

8   Do the following for each selected update:

   a   Click an update's name in the window to the left.

   b   In the **Packet properties** window, double-click the **Source URL** entry.

   c   Type the URL to your mirror server (for example, http://example.com/Updates/) and click **OK.**

   d   Double-click the **Readme URL** entry.

   e   Type the URL to your mirror server (for example, http://example.com/Updates/) and click **OK.**

9   Click **Save As** and save the configuration file to the Web server's directory C:\Inetpub\vhosts\default\htdocs\Updates.

10 Define the MIME types appropriately:

   a   Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager > Web Sites**, right-click the domain name, select **Properties**, click the **HTTP Headers** tab, and then click the **MIME Types** button.

   b   Click **New**. In the **Extension** box, type `.xml`, in the **MIME type** box, type `application/octet-stream`. Click **OK.**

   c   Click **New**. In the **Extension** box, type `.crc`, in the **MIME type** box, type `application/octet-stream`. Click **OK**.

   d   Click **New**. In the **Extension** box, type `.msp`, in the **MIME type** box, type `application/octet-stream`. Click **OK**.

   e   Click **New**. In the **Extension** box, type `.msi`, in the **MIME type** box, type `application/octet-stream`. Click **OK**.

   f   Click **OK** and close the **Internet Information Services (IIS) Manager**.

11 Log in to Plesk and go to **Server > Updater > Automatic Update** tab.

12 Select the **Automatically update Plesk** check box, type the network address of your mirror server and click **OK**.

Appendix A. Advanced Features

In addition to operations available via control panel, Plesk software provides several advanced management capabilities, available to the administrator from the command line. The administrator can:

- Monitor the status of vital Plesk services without logging it to control panel
- Change the Plesk server's host name
- Customize the text shown on Plesk title bar
- Change DNS zone serial number format
- Use event tracking mechanism to organize data interchange between Plesk and external systems
- Change Tomcat connector ports
- Restore Plesk mail configuration
- Change Tomcat connector ports
- Manage various Plesk entities bypassing Plesk GUI

To learn more about advanced features, please refer to Plesk for Windows Advanced Administration Guide.

For more information about command line utilities usage refer to Plesk for Windows Command Line Utilities Administrator Guide.