Simplify Your Server Management

Plesk Server Administrator 2.0
Users Manual

Plesk Inc.
Ph.: 1-703-815-5670
Fx.: 1-703-815-5675
http://www.plesk.com

Rev. 2001-10-16

1. BEFORE YOU GET STARTED

1.1 About Plesk, Inc.

Founded by a team of Internet entrepreneurs, UUNET veterans, and Cisco Systems Inc. professionals, Plesk Inc. was incorporated in September 1999 in Northern Virginia. The company produces software applications that exploit the power of the World Wide Web as a common user interface. Plesk seeks to develop server management applications that are easy to use, require minimal training, and offer maximum value. The target audience of the company includes Web hosting companies, Internet service providers (ISPs), server hardware manufacturers, application service providers (ASPs), small to mid-sized businesses and individual site owners.

In November 1999 Plesk released the Plesk Server Administrator, or PSA in beta. PSA is a software tool designed to make server management faster, easier and more accessible to both administrators and end-users. PSA allows users to perform administrative functions through an easy-to-use GUI, which makes it possible for even non-technical individuals to administer sites. Functions such as creating domains, managing email accounts and obtaining SSL certificates can all be performed through the PSA interface. This manual is to be used with Plesk Server Administrator, and is updated in accordance with the release of Version 2.0.

To find out more about Plesk, such as product information, partnership opportunities, and contact information, please visit www.plesk.com.

Plesk, Inc. currently has offices located in Chantilly, Virginia and Novosibirsk, Russia.

1.2 About The Plesk Server Administrator

The flagship product of Plesk is the Plesk Server Administrator, or PSA. This server management software makes use of a graphical user interface (GUI) which allows users to perform a wide array of administrative tasks simply and easily. With PSA, a user does not require advanced knowledge of the operating system or hours of work to create domains, add e-mail accounts or check site statistics. Instead, PSA makes server management accessible and easy for the average computer user. This manual deals with PSA 2.0.

1.2.1 Who Should use the Plesk Server Administrator

The Plesk Server Administrator (PSA) is designed to be used both by experienced administrators and users with little or no server administration or programming experience. Typical users and customers include:

- **Web Hosting Companies**
  PSA can dramatically reduce a Web hosting company or an ISP's support workload. Customers or "clients" no longer need to call their support staff to perform various routine or complicated tasks; PSA makes those tasks accessible to the customers enabling them to support themselves. Clients are empowered by PSA to manage their own accounts, allowing the hosting companies to focus on more complex issues. Because the Plesk database is structured around a customer (not a domain), PSA lets a hosting company run its reseller programs immediately after installing the software. PSA increases customer satisfaction and reduces the support workload.

- **Server Hardware Manufacturers**
  Server manufacturers can include PSA as a pre-installed feature to add value to its products and to diversify its product lines. When PSA is installed, the server is ready for immediate use; it only needs to be networked.

- **Small Businesses**
  Many small businesses do not have a full-time system administrator to maintain their company's Internet server. Limited technical skills or the high cost of outsourced hosting need not limit a business's online presence. PSA empowers a business's existing staff to manage all email and hosting requirements; the web-based interface empowers the average computer user.

1.2.2 Plesk Server Administrator Capabilities

Plesk Server Administrator (PSA) PSA provides three tiers of administration: admin, client, and domain. All can perform tasks at remote locations via any standard Internet browser. The following capabilities exist for each type of user:

System Administrator - Admin

- System Management
    - Hardware Reboot and/or Shutdown
    - Manage IP aliases
    - Set system time
    - Check server level statistics
- Services Management
    - Set up server wide mail limits
    - Set up allowable mail relay capabilities and mail blockers
    - Set up DNS server default zone template
- Control Panel Management
    - Co-brand using company logo and link
    - Set up control panel access security
    - Allow discounted domain registration and SSL certificate purchasing
    - Set up screen paging options
    - Set control panel language; currently limited to English only
- Client Management
    - Create, edit, and delete system clients
    - Allow reseller capabilities
    - Set up client level limits on domain creation
- My.Plesk.Com Service Management
    - Access to purchase additional server tools

Client Administrator

- Multiple Domain Management
    - Create, edit, and delete domains and/or hosting accounts
    - Set up FTP and/or anonymous FTP services
    - Set up web server allowances

        - Traffic limits
        - Scripting – PHP, SSI, CGI, mod_perl, and/or Apache ASP
        - FrontPage server extensions
        - SSL support
    - Set up domain level limits
        - Disk space
        - Mail accounts
        - User accounts
        - Databases
    - Manage DNS zones
    - Set up domain tools
        - Webalizer
        - IMP webmail
- My.Plesk.Com Service Management
    - Domain registration and management services
    - SSL Certification purchasing and management services
    - Access to purchase additional domain tools
- Control Panel Management
    - Co-brand using company logo and link
    - Set up screen paging options
    - Set control panel language; currently limited to English only

Domain Administrator

- Mail Account Management
    - Create, edit, and delete POP3 mail boxes / quotas
    - Create, edit, and delete mail redirects
    - Create, edit, and delete mail groups
    - Create, edit, and delete multiple configurable autoresponders

    - Utilize IMP webmail service
- Domain Report Management
    - Review domain services
    - Access domain statistics
- Web User Management
    - Create, edit, and delete domain web users
    - Set up scripting capabilities for web users
- Protected Directory Management
    - Create, edit, and delete protected directories
    - Set up access with SSL or standard http
    - Manage directory users
- SSL Certificate Management
    - Create CSR or self-signed certificate
    - Install SSL certificate
- FTP Service Management
    - Change passwords
    - Utilize anonymous FTP service
- Database Management
    - Create, edit, and delete multiple databases
    - Manage database users
    - Direct access to databases through PhpMyAdmin

1.2.3 Compatible Operating Systems

The Plesk Server Administrator (PSA) 2.0 is available for the following platforms:

- FreeBSD® 4.0, 4.1, 4.2
- Red Hat® Linux 6.2 and 7.1

NOTE: In theory, PSA should work on all versions of Linux (e.g. Caldera OpenLinux, Debian Linux, et cetera), but Plesk Inc. has not tested the software on all versions and cannot guarantee the product's performance. The current release runs on Red Hat® Linux. Future releases of PSA may run on other Linux versions.

1.2.4 System Requirements

These are the system requirements for each platform that runs with Plesk Server Administrator 2.0.

Server side:
Red Hat® Linux
Red Hat® Linux version 6.2 or 7.1
Pentium 166 MHz or better w/ 32MB Ram and 80 MB of disk space.
or
FreeBSD®
FreeBSD® versions 4.0, 4.1, and 4.2
Pentium 166 MHz or better w/ 32 MB Ram and 80 MB of disk space.

Client side:
Netscape 4.x+ or Microsoft Internet Explorer 4.x+

NOTE: By default PSA installs everything into the /usr/local/psa directory. It is important to partition the hard drive accordingly.

1.2.5 Additional Benefits

Ease of Use

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

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

Security

The Plesk Server Administrator (PSA) uses extensive security measures to assure your system of the highest possible integrity and protection. It should be noted however that this is limited to PSA and the software it installs. The security of the server operating

system is considered the responsibility of the system administrator and is not part of the PSA installation and/or set up:

- PSA uses the secure HTTP (HTTPS) protocol. All documents and communications between users and the server are fully encrypted and secure.
- PSA provides a generic secure socket layer (SSL) certificate that enables secure transactions between a remote user and PSA. However, this certificate will not be recognized by the web browser as being valid for your control panel URL, which results in warning messages. Certifications can be purchased directly through the PSA control panel or by contacting a certificate-signing authority directly.
- When creating an FTP account on the server, the login shell is set to **/bin/false**, preventing any Telnet-like programs from accessing the account.
- When creating physical hosting with PHP support, you are unable to start an external program from the PHP script. It is impossible to read or write files above the user's home directory.
- PSA uses the suexec feature of the Apache web server for secure CGI operation.
- On FreeBSD and Linux systems, PSA uses the chroot feature on the FTP server, preventing clients from changing their home directories to another directory.
- PSA applies a chroot to the named process to eliminate any possibility of gaining system access through named.
- PSA has chosen the Qmail mail system and ProFTPd ftp system both of which maintain the highest security standards in their respective fields of service.
- Firewalls are not currently supported, but may be added in a future release.

1.3 Getting Help

Plesk Server Administrator (PSA) is designed with the concepts of simplicity and functionality in mind, so that non-technical individuals can use it with ease. However, times may arise when a user needs assistance in using the product, configuring the system, or obtaining advanced information. For users' convenience, Plesk Inc. maintains several sources of information.

1.3.1 How to Use This Manual

This manual is written to provide instructions and information on how to use PSA. It is intended for system administrators, clients, and domain owners using PSA. Certain sections apply only to a system administrator, there is one section each for client administration and domain administration, and other sections are for general use.

- System Administrator
    - Downloading the Plesk Server Administrator Software
    - Installing the Plesk Server Administrator on Your System
    - System Administration: Managing the Server
    - System Administration: Managing Clients
    - System Administration: Managing Domains
- Client
    - Client-Level Administration
- Domain User
    - Domain-Level Administration
- General Information
    - About Plesk Inc.
    - About the Plesk Server Administrator
    - Getting Help
    - Glossary of Terms
    - Index

NOTE: Information prefaced with "**NOTE:**" is a note, tip or warning. Notes provide special messages about the function you are reviewing. Also be sure to notice the red asterisk which indicates a **Required Field** on certain screens. An error or warning

message will appear if you do not properly enter information in any required field.

1.3.2 Other Forms of Help

There are several ways to obtain answers for any questions you might have, or problems you might encounter:

- **Website**
  You can read more about Plesk Inc. and our products at www.plesk.com. The website contains information about the company, details on purchasing Plesk Server Administrator, information on downloading software, **FAQs** about Plesk and its products, an **online forum** for customers to post questions/comments to other users, and information on hosting partners, reseller arrangements and contacts.

  NOTE: We strongly encourage you to consult the **online forum** and/or **FAQ** section of our website when encountering problems or questions concerning PSA. Our Technical Support staff continuously updates the FAQ section to reflect and address common problems and important issues reported to us by our users.

- **Online Software Demos**
  If you would like to demo or use the Plesk Server Administrator before you actually install it, there are two demos available at www.plesk.com. The interactive demo allows you to perform and try out all of the various features of PSA online, giving you hands-on experience with every function. The Flash Demo is a short (5-6 minute) presentation showcasing PSA's different features, allowing you to see PSA in action.

  NOTE: If you'd like to install and try out PSA before purchasing it, the fully functional one-domain version is available for free download at www.plesk.com.

- **Help File**
  The Plesk Server Administrator software comes with a comprehensive help file. The help file is context-sensitive, providing step-by-step assistance and tips relating to the function currently in use. To access the help file, click the **HELP** button on any Plesk Server Administrator page.

- **Email Access**
  If you have an inquiry or comment that you would like a Plesk Inc. staff-member to address, or if you require additional information about our products, please e-mail us at one of the following addresses:

  - To purchase software: sales@plesk.com
  - For technical support: support@plesk.com

- For billing questions: accounting@plesk.com
- To report software problems: bugreport@plesk.com
- For general information (including customer service inquiries): info@plesk.com

- **Technical Support**
  Support covers questions and problems directly relating to the Plesk product you purchased. It does NOT cover alterations of Plesk products to include functionality and/or features not currently supported; nor does it cover the transferring of domains and/or websites from an existing server. Plesk Inc. offers various levels of technical support:
  - **First 30 Days: Free Email Support**
    For the first 30 days following the purchase and installation of your Plesk product, you receive email support, available at support@plesk.com.
  - **Plesk Premium Support**
    Plesk Inc. offers a one-year premium support package for $499 USD. It offers phone support for a maximum of 25 incidents from 9am to 5pm (EST) and unlimited email support at support@plesk.com. This service can be purchased online at www.plesk.com or directly through a Plesk Inc. sales representative at 1-703-815-5670.
  - **Per/Incident Support**
    We also offer phone support from 9am to 5pm (EST) at $30 USD per incident. To access this service, call Plesk Inc. at 1-703-815-5670.
  - **Unlimited Email Support**
    You can purchase a 1-year unlimited email support package for $249 USD. This service can be purchased online at www.plesk.com or directly through a Plesk Inc. sales representative at 1-703-815-5670.
  - **Installation Service**
    Have your PSA product remotely installed by a Plesk Inc. technician for a fee of $150 USD. Please contact a Plesk Inc. sales representative at 1-703-815-5670 or make arrangements through Plesk's online store.

2. GETTING STARTED

2.1 Downloading The Plesk Server Administrator Software

Once you purchase Plesk Server Administrator (PSA), you will be emailed your key information. This key enables you to activate the software for the purchased number of domains. Prior to installing the key, you must download and install the PSA software. This can be done directly from the Plesk website.

1. Go to www.plesk.com/downloads to download the PSA software.
2. You will be prompted to login. If you are not an already registered customer in our system, you are a new customer, and need to register before you can proceed with downloading the product. If you are already registered as a Plesk customer, enter your user ID and password to proceed.
3. In the frame on the right you will be able to select the appropriate PSA release version. This will take you to the main download page for the respective release.
4. Click on the appropriate PSA version. Keep in mind when selecting your version that selection is not only limited to the operating system (OS) being used. There are two separate installation methods available for the RedHat OS. You can either select the PSA RPM or the standard PSA Self-Extracting install which includes the complete install of all your system services. For typical PSA users it is recommended to use the PSA Self-Extracting install as this simplifies the process of install significantly.
5. Once you have selected the appropriate PSA version, you will be prompted to choose a location on your computer to which to download the software.
6. After indicating the download location, click the "OK" button in the **DOWNLOAD** file box and the download will begin.
7. When the download is complete, the Plesk Server Administrator is ready to be installed on your server.

NOTE: We strongly recommend that you download the installation instructions from www.plesk.com/download, or follow the instructions on the Installing Plesk Software page. Review of and careful attention to the installation instructions will help ensure proper and complete installation of the software.

2.2 Installing the Plesk Server Administrator on Your System

- Before You Install the Plesk Server Administrator
- What Happens During Install?
- Installing the Plesk Server Administrator
- Error Messages
- Installing the License and SSL Certificate

2.2.1 Before You Install Plesk Server Administrator

Only install the Plesk Server Administrator (PSA) on a clean server that serves as one dedicated server. Plesk Inc. will not be held liable for any damages occurring as a result of installing PSA on a server that has been installed with anything other than a fresh installation of the operating system for which the PSA installation was intended. You must have root privileges to install PSA on your server.

The PSA Self-Extracting install includes the following components:

- Admin server
- Web server
- MySQL database
- Mail server
- DNS server
- FTP server

The PSA RPM install is designed in general to treat all packages separately. For detailed information on all the packages included in the distribution and what packages PSA can work with see Installing the Plesk Server Administrator later in this section.

NOTE: PSA requires that the network components including inetd/xinetd be properly installed on the system before installation of the PSA software.

2.2.2 What Happens During Install?

This section reviews the functions performed as well as the structure created on the server as it is configured during PSA installation.

PSA Self-Extracting Install

The following services run under PSA:

- named – BIND 9.1-REL
- MySQL – 3.23.36
- Qmail – 1.03
- Apache – 1.3.19 Ben-SSL/1.42
- ProFTP – 1.2.1
- stunnel – 3.14

NOTE: Additional services controllable under Apache are mod_throttle 2.11, mod_perl 1.24_01, PHP 4.0.4pl1, apache::asp 2.09, and Frontpage 4.0.

Directory Structure

PSA creates the directory **/usr/local/psa/** as its root software directory. The location of this directory is defined within the /etc/psa/psa.conf file. Several subdirectories are also created, including:

- /usr/local/psa/admin/...
- /usr/local/psa/apache/...
- /usr/local/psa/mysql/...
- /usr/local/psa/ftpd/...
- /usr/local/psa/named/...
- /usr/local/psa/stunnel/...
- /usr/local/psa/frontpage/...
- /usr/local/psa/qmail/...
- /usr/local/psa/courier-imap/…
- /usr/local/psa/webalizer/…
- /usr/local/psa/home/…
- /usr/local/psa/rc.d/…
- /usr/local/psa/var/…

- /usr/local/psa/bin/…
- /usr/local/psa/tmp/…
- /usr/local/psa/etc/…

Accounts and Groups

PSA creates accounts for Apache, MySQL and qmail pseudo-users. These pseudo-users do not have shells in which to operate, alleviating security concerns involving the users.

Services

The following changes in cervices take place:

- PSA disables the sendmail service and replaces it with qmail.
- PSA replaces your **named** database and configuration files. Then PSA restarts the **named daemon**.
- PSA also edits the **inetd/xinetd** configuration file and comments out the **comsat** service record.
- PSA adds the POP3 service, using qmail to handle it. If you had a previous POP3 service on the server, PSA comments out the old version and uses the new POP3 version.
- PSA adds a sendmail service record, handled by the qmail daemon. If you had a previous sendmail service record, PSA comments it out and replaces it with the new version.
- The inetd/xinetd daemon restarts to read its new configuration file.

Using an External DNS Server

You can use an external DNS service with PSA, but you should follow these manual configuration steps:

1. During installation, a remote DNS server can be specified. Or after installation, the remote DNS can be specified in the **/etc/resolv.conf** file.
2. The line **search localdomain** must be removed from the **/etc/resolv.conf** file on the Plesk server.
3. Any DNS configurations on the local PSA server must be reflected on the external DNS server.

Other Changes

PSA creates some links to the MySQL libraries in the **/usr/lib** subdirectory and adds the **@clients** string to **/etc/ftpchroot**.
Also, it adds a string to the file /etc/shells:

/bin/false
or
/usr/bin/false

If the POP3 service record is not in **/etc/services**, PSA adds it. PSA moves the sendmail binary file to **sendmail.plesk**. The PSA startup script is placed in the appropriate location to start PSA; this script will enable PSA to start each time the server is booted up.

PSA RPM Install

The following services will be controllable under PSA:

- named – BIND 9.1-REL
- MySQL – 3.23.36
- Qmail – 1.03
- Apache – 1.3.19 Ben-SSL/1.42
- ProFTP – 1.2.1
- stunnel – 3.14

NOTE: Additional services controllable under Apache are mod_throttle 2.11, mod_perl 1.24_01, PHP 4.0.4pl1, apache::asp 2.09, and Frontpage 4.0.

Directory Structure

PSA creates the directory **/usr/local/psa/** as its root software directory. The location of this directory is defined and changeable within the /etc/psa/psa.conf file. Several subdirectories are also created, including:

- /usr/local/psa/admin/...
- /usr/local/psa/bin/…
- /usr/local/psa/etc/…

Accounts and Groups

PSA creates accounts for Apache, MySQL and qmail pseudo-users. These pseudo-users do not have shells in which to operate, alleviating security concerns involving the users.

Using an External DNS Server

You can use an external DNS service with PSA, but you should follow these manual configuration steps:

1. During installation, a remote DNS server can be specified. Or after installation, the remote DNS can be specified in the **/etc/resolv.conf** file.
2. The line **search localdomain** must be removed from the **/etc/resolv.conf** file on the Plesk server.
3. Any DNS configurations on the local PSA server must be reflected on the external DNS server.

Other Changes

PSA creates some links to the MySQL libraries in the **/usr/lib** subdirectory and adds the **@clients** string to **/etc/ftpchroot**.
Also, it adds a string to the file /etc/shells:

/bin/false
or
/usr/bin/false

If the POP3 service record is not in **/etc/services**, PSA adds it. PSA moves the sendmail binary file to **sendmail.plesk**. The PSA startup script is placed in the appropriate location to start PSA; this script will enable PSA to start each time the server is booted up.

IMPORTANT: You must install Plesk Server Administrator on a clean server; specifically only the operating system should be installed. Plesk Inc. will not be held liable for damages as a result of installing the PSA on a server with anything other than a fresh installation of the operating system for which the PSA installation was intended.

2.2.3 Installing the Plesk Server Administrator

PSA Self-Extracting Install Procedure

Download the PSA software file to your server from www.plesk.com/downloads.

1. Log in as “root” and change your working directory to the directory where the Server Administrator install script resides; for example:
   #cd /home/admin/psa

2. Run the install script, for example:
   #sh.<psa_install_file_name.sh>

3. If you have a previous version of Plesk Server Administrator installed in the /usr/local/psa directory, the install script will detect it and will ask if you want to delete it. If you answer No, the installation will not continue. If you answer Yes, the entire contents of the /usr/local/psa directory will be deleted. WARNING: This action is not reversible. If you’re attempting to upgrade a previous version of Plesk Server Administrator, you need to stop, and obtain a special upgrade script from Plesk.

4. You will see several messages as the install script prepares for the installation.

5. Next the script will display a series of messages showing the progress of the installation. At this time all of the components of Plesk Server Administrator will be installed and properly configured on the server. Depending on the speed of the server, there may be times when the installation seems to be stuck. The entire install procedure should take only a few minutes. Do not attempt to cancel the install script. The installation logs all of the changes made to the system in the /tmp/ directory. The install script will backup any system configuration files before making the changes.

6. When the installation is complete, you will receive a message notifying you that psa is now running on your server. You will be able to use the Plesk Server Administrator on your host at:
   https://< machine.domain.name or IP-Address>:8443/
   The default username is ‘admin’ and the default password is ‘setup’. Both are case sensitive. For security reasons this password should be changed upon initial login.
7. Upon initial login to Plesk Server Administrator you will be required to complete the final steps in the installation process.
8. You will first be asked to accept the Plesk, Inc. End User License Agreement. Select the appropriate checkbox at the end of the agreement and select **ACCEPT**. Note: You have the option to leave the license agreement active on the server if you wish.
9. You will then be asked to verify the IP-address to be used for name-based hosting and the hostname and domain name associated with your server. These fields will be populated based on items already defined within your server parameters. Edit this information appropriately and select **UPDATE**.
10. You will then be asked to fill in the appropriate Administrator information. Once you have completed this, you will be able to utilize the full functionality of Plesk Server Administrator.

PSA RPM Install Procedure

The PSA 2.0 RPM installations require either RedHat Linux 7.1 or RedHat Linux 6.2 already installed on your system. We recommend using the Linux RedHat 7.1 even though PSA 2.0 has been fully tested and is compatible with both versions. If possible RedHat Linux 7.1 should be used, however PSA 2.0 may be installed for RedHat Linux 6.2 accompanied by full upgrade of the required components. Keep in mind that installation of any new product for older Linux versions always requires more time and efforts from the Administrator.

Installing PSA 2.0 for Linux RedHat 7.1:

1. You will first need to log in as 'root' to your system.

2. Before the installation, make sure that all the required libraries are installed.

   You can check whether a particular rpm is already installed by entering the following command:
   'rpm -q <rpmname>'.

   For example:

   bash$ rpm -q pam
   pam-0.74-22

   You can also use our script 'query_rpm_for_prod.sh -vvv' to check the complete configuration of the system.

   Following is the list of required libraries and packages. You can check for their presence in the system:

   bash$ rpm -q db1 db3 freetype gd gdbm glibc krb5-libs libjpeg libpng libstdc++ libtermcap ncurses pam readline sharutils xinetd zlib

   If one or more of these libraries are not installed in the system it can be installed from the system installation CD or downloaded from ftp://ftp.redhat.com or from any of its mirrors and installed by entering the following command:
   'rpm -Uvh <rpm_name>.rpm'

3. Install the rpm's of indicated versions or higher from the RedHat 7.1 disc:

   apache-1.3.19-5.i386.rpm
   bind-9.1.0-10.i386.rpm
   bind-utils-9.1.0-10.i386.rpm
   binutils-2.10.91.0.2-3.i386.rpm
   mod_perl-1.24_01-2.i386.rpm
   mod_ssl-2.8.1-5.i386.rpm

mysql-3.23.36-1.i386.rpm
mysql-devel-3.23.36-1.i386.rpm
mysql-server-3.23.36-1.i386.rpm
ntp-4.0.99k-15.i386.rpm
openssl-0.9.6-3.i386.rpm
openssl095a-0.9.5a-1.i386.rpm
perl-5.6.0-12.i386.rpm
perl-DBI-1.14-10.i386.rpm
perl-DBD-MySQL-1.2215-1.i386.rpm
php-4.0.4pl1-9.i386.rpm
php-imap-4.0.4pl1-9.i386.rpm
php-mysql-4.0.4pl1-9.i386.rpm
shadow-utils-20000826-4.i386.rpm
textutils-2.0.11-7.i386.rpm

From PowerTools disc:

perl-libnet-1.0703-5.i386.rpm
webalizer-2.01_06-5.i386.rpm

All of these rpm's are available on the RedHat 7.1 installation CDs, at ftp://ftp.redhat.com or any of its mirrors, or from the directory “std.rh-7.1” in your PSA archive (PSA-RPMS-full-rh7.1.buildXXXXXX.tar), or from the “Downloads” section at: http://www.plesk.com/

For installation use the following command:
'rpm -Uvh <rpm_name>.rpm'

4. Install the base PSA rpm's from the directory “base” in your PSA archive (PSA-RPMS-<…>-rh7.1.buildXXXXXX.tar), or from the “Downloads” section at: http://www.plesk.com/

   courier-imap-1.3.5-<…>psa.rh7.1.i586.rpm
   psa-qmail-1.03-rh7.1.build<…>.i586.rpm
   psa-courier-imap-add-2.0.0-rh7.1.build<…>.i586.rpm
   psa-proftpd-1.2.1-rh7.1.build<…>.i586.rpm
   psa-proftpd-xinetd-1.2.1-rh7.1.build<…>.i586.rpm
   psa-2.0.0-rh7.1.build<…>.i586.rpm

   For installation use the following command:
   'rpm -Uvh <rpm_name>.rpm'

5. In order for your Apache to support FrontPage extentions and Apache::ASP it is necessary to install rpm's from the directory “opt” in your PSA archive (PSA-RPMS-<…>-rh7.1.buildXXXXXX.tar), or from the “Downloads” section at:

http://www.plesk.com/
However these packages are not required for PSA to function properly.

6. When the installation is finished, Plesk Server Administrator will have started automatically. In order to complete the PSA initial configuration, you need to login to PSA on your host at:
https://< machine.domain.name or IP-Address>:8443/
The default username is 'admin' and the default password is 'setup'. Both are case sensitive. For security reasons this password should be changed upon initial login.

Installing PSA 2.0 for Linux RedHat 6.2:

1. You will first need to log in as 'root' to your system.

2. Utilizing RedHat 6.2 requires the upgrade of many rpm's included in the system. The final updates are available at ftp://updates.redhat.com or at any mirror of this site. It is also possible to a partial update (updating only the needed libraries and components that are required for PSA 2.0) by installing all the rpm's from the directory "std.rh-6.2" in your PSA archive (PSA-RPMS-full-rh6.2.buildXXXXXX.tar), or from the "Downloads" section at:
http://www.plesk.com/

   Below is the list of the needed rpm's:

   bash2-2.03-8.i386.rpm
   db3-3.1.17-4.6x.i386.rpm
   db3-utils-3.1.17-4.6x.i386.rpm (optional)
   freetype-1.3.1-5.i386.rpm
   gd-1.3-6.i386.rpm
   glibc-2.1.3-22.i386.rpm
   inetd-0.16-7.i386.rpm
   krb5-configs-1.1.1-27.i386.rpm
   krb5-libs-1.1.1-27.i386.rpm
   libjpeg-6b-10.i386.rpm
   ncurses-5.0-12.i386.rpm
   openssl-0.9.5a-2.6.x.i386.rpm
   pam-0.72-20.6.x.i386.rpm
   rpm-4.0.2-6x.i386.rpm
   xntp3-5.93-15.i386.rpm
   xpm-3.4k-2.i386.rpm

   You can check whether a particular rpm is already installed by entering the following command:
   'rpm -q <rpmname>'.

For example:

bash$ rpm -q pam
pam-0.72-20.6.x

You can also use our script 'query_rpm_for_prod.sh -vvv' to check the complete configuration of the system.

For installation use the following command:
'rpm -Uvh <rpm_name>.rpm'

Following is the list of required libraries and packages. You can check for their presence in the system:

bash$ rpm -q db3 freetype gd gdbm glibc krb5-libs libjpeg libpng libstdc++ libtermcap ncurses pam readline sharutils zlib xpm rpm inetd openssl xntp3 bash2 perl

Some packages require the rpm to be of version 4.0 or higher, therefore it is best to have it installed as version 4.0 from the beginning. To do that, you will need to enter this sequence of commands:

bash$ rpm --rebuilddb
bash$ rpm -Uvh rpm-4.0.2-6x.i386.rpm db3-3.1.17-4.6x.i386.rpm
bash$ rpm --rebuilddb
bash$ rpm -q rpm
rpm-4.0.2-6x

3. After you have made sure that all the necessary libraries and packages from the distributive have been included and all the updates to RedHat 6.2 are installed, proceed to installation of all rpm's from the directory “ std.rh-7.1_to_6.2” in your PSA archive (PSA-RPMS-<…>-rh6.2.buildXXXXXX.tar), or from the “Downloads” section at: http://www.plesk.com/

   Below is a list of the needed rpm’s:

   apache-1.3.19-5.i386.rpm
   apache-manual-1.3.19-5.i386.rpm
   bind-9.1.0-10psa.rh6.2.i386.rpm
   bind-utils-9.1.0-10psa.rh6.2.i386.rpm
   mod_perl-1.24_01-2.rh6.2.i386.rpm
   mod_ssl-2.8.1-5.i386.rpm
   mysql-3.23.36-1.rh6.2.i386.rpm
   mysql-server-3.23.36-1.rh6.2.i386.rpm
   php-4.0.4pl1-9.rh6.2.i386.rpm
   php-imap-4.0.4pl1-9.rh6.2.i386.rpm

php-manual-4.0.4pl1-9.rh6.2.i386.rpm
php-mysql-4.0.4pl1-9.rh6.2.i386.rpm
webalizer-2.01_06-5.rh6.2.i386.rpm

These rpm's are to be downloaded Only from our site as they are built specifically for RedHat 6.2 running with PSA 2.0.

For installation use the following command:
'rpm -Uvh <rpm_name>.rpm'

It is possible to personally generate any of the mentioned rpm's or compile and install any of them from the source, but this not recommended and requires a very high level of rpm knowledge and experience.

4. Install the base PSA rpm's from the directory “base” in your PSA archive (PSA-RPMS-<…>-rh6.2.buildXXXXXX.tar), or from the “Downloads” section at: http://www.plesk.com/

   courier-imap-1.3.5-<...>psa.rh6.2.i586.rpm
   psa-qmail-1.03-rh6.2.build<...>.i586.rpm
   psa-courier-imap-add-2.0.0-rh6.2.build<...>.i586.rpm
   psa-proftpd-1.2.1-rh6.2.build<...>.i586.rpm
   psa-proftpd-inetd-1.2.1-rh6.2.build<...>.i586.rpm or psa-proftpd-xinetd-1.2.1-rh6.2.build<..>.i586.rpm
   psa-2.0.0-rh6.2.build<...>.i586.rpm

   For installation use the following command:
   'rpm -Uvh <rpm_name>.rpm'

   Comments:
   If you are using inetd (part of the RedHat 6.2 distribution) then you should install psa-proftpd-inetd; if you are using xinetd (part of other RedHat-base distributions, but is not truly tested) then you should install psa-proftpd-xinetd.

   Before installation of the base rpm’s make sure that inetd (or xinetd) is already started.

   For example:
   bash$ ps -ax|grep inetd
   4377 ? S 0:00 inetd

   If you do not find it working, start it yourself:
   bash$ service inet start

5. In order for your Apache to support FrontPage extentions and Apache::ASP it is necessary to install rpm's from the directory “opt” in your PSA archive (PSA-

RPMS-<…>-rh6.2.buildXXXXXX.tar), or from the “Downloads” section at: http://www.plesk.com/
However these packages are not required for PSA to function properly.

6. When the installation is finished, Plesk Server Administrator will have started automatically. In order to complete the PSA initial configuration, you need to login to PSA on your host at:
https://< machine.domain.name or IP-Address>:8443/
The default username is ‘admin’ and the default password is ‘setup’. Both are case sensitive. For security reasons this password should be changed upon initial login.

2.2.4 Error Messages

You may receive the following error message when installing the Plesk Server Administrator:

===> Installing MySQL Server
Checking for the group 'mysql'...
ERROR:
"It seems that there is group "mysql" in your system. PSA uses the same group name but with another group ID ("3306"). Sorry, but this situation is not properly handled yet. Please contact support@plesk.com"

This situation indicates that whomever is installing the Plesk Server Administrator is probably installing it remotely via Telnet. If this error occurs, the "su-" (superuser) command was not executed. Please contact us at support@plesk.com or 1-703-815-5670 for technical assistance.

2.2.5 Uninstalling the Plesk Server Administrator

The process of uninstalling Plesk Server Administrator for systems that run under **RedHat® Linux** slightly differs from the one for systems that run under **FreeBSD®**. One of the following sections will guide you through the process of uninstalling PSA depending on the type of Operating System you are running.

NOTE: Exercise extreme caution. The whole PSA directory will be deleted without confirmation. This action is not reversible. Make sure you have anything you want to save placed safely somewhere else before you run the uninstall function, as it will return your server to the state that it was in before PSA was installed. HTML documents, log files, outstanding email, and mySQL databases will all be deleted.

Uninstalling PSA for RedHat® Linux

1. First, log in through telnet and change to super-user with the “su –“ command if you have local access, log in as root.
2. Run /usr/local/psa/admin/bin/deinstall.sh deinstall. This will remove PSA 2.0 from the system.
3. Delete /etc/psa directory.
4. Delete PSA users and groups from:

   - /etc/ftpchroot
   - /etc/ftpusers
   - /etc/passwd
   - /etc/shadow
   - /etc/group

   PSA System Users:

   - bind
   - mysql
   - apache
   - psaadm
   - psaftp
   - qmaild
   - qmaill
   - qmailp
   - qmailq
   - qmailr
   - qmails
   - popuser
   - +all users with group=psacln (ftpusers and webusers)

   PSA System Groups:

- psaftp
- qmail
- popuser
- psaadm
- psacln

5. Delete PSA startup scripts located in /etc/rc.d/init.d/
6. Delete PSA services ftp, and smtp from /etc/inetd.conf or /etc/xinetd.conf and /etc/xinetd.d directory, restart xinetd.
7. Delete /etc/sysconfig/named
8. Restore link to you sendmail /usr/lib/sendmail and /usr/sbin/sendmail
9. Delete link /etc/named.conf
10. Delete /tmp/.state directory
11. Install PSA 1.3.1 as a clean installation
12. Restore all data from PSA 1.3.1 you backed up.

NOTE: The two final steps (11 and 12) are needed only in case if you have upgraded your previously used PSA 1.3.1 to PSA 2.0 and now wish to restore PSA 1.3.1.

Uninstalling PSA for FreeBSD®

1. First, log in through telnet and change to super-user with the “su –“ command if you have local access, log in as root.
2. Run /usr/local/psa/admin/bin/deinstall.sh deinstall. This will remove PSA 2.0 from the system.
3. Delete /etc/psa directory.
4. Delete psa users and groups from

- /etc/ftpchroot
- /etc/ftpusers
- /etc/passwd
- /etc/master.passwd
- /etc/group

PSA System Users:

- bind
- mysql
- apache
- psaadm
- psaftp
- qmaild
- qmaill
- qmailp
- qmailq
- qmailr
- qmails
- popuser
- +all users with group=psacln (ftpusers and webusers)

PSA System Groups:

- psaftp
- qmail
- popuser
- psaadm
- psacln

5. Delete PSA startup scripts located in /usr/local/etc/rc.d/.
6. Delete PSA services ftp, and smtp from /etc/inetd.conf, restart inetd.
7. Delete /etc/sysconfig/named
8. Restore link to your sendmail /usr/lib/sendmail and /usr/sbin/sendmail
9. Delete link /etc/named.conf
10. Delete /tmp/.state directory.

11. Install PSA 1.3.1 as a clean installation.

12. Restore all data from PSA 1.3.1 you backed up.

NOTE: The two final steps (11 and 12) are needed only in case if you have upgraded your previously used PSA 1.3.1 to PSA 2.0 and now wish to restore PSA 1.3.1.

2.2.6 Installing the Key License

To activate PSA for the purchased number of domains, you must install the key license that is sent to you in an email. Key installation instructions are as follows:

1. Transfer the key file to the server.
2. Change to super-user with the “su –“ command.
3. Access the directory where you transferred the key file.
4. Execute the key file shell script plesk_key.sh.

   “sh plesk_key.sh”
5. The script will automatically restart the Plesk server with the new key.

2.3 Logging Into and Off the Server Administrator

2.3.1 Accessing your Control Panel

For security purposes, Plesk Server Administrator (PSA) uses SSL, so both clients and administrators need to access the control panel through their browser, using **HTTPS:** secure protocol. To bring up the control panel for PSA 2.0, follow these steps:

1. Open your web browser.
2. Administrators and Clients can access the control panel from different **urls**.
    - Administrators - HTTPS://<Primary IP>:8443 (Primary IP refers to the primary IP address of your server – any IP address on your server will work)
    - Clients - HTTPS://<Client Domain>:8443 (Client Domain refers to any active domain that resolves to the server)

    NOTE: These are the preferred ways of accessing the control panel. However, the Administrator can access the control panel using any IP or name associated with the server.
3. The control panel login screen with the username and password fields should appear.
4. Proceed with the logging in process.

NOTE: By default, PSA comes with a self-signed certificate that will not be recognized by your browser as a valid certificate. You can still access your control panel, but you will receive a warning message. If you purchase a valid certificate, you will not receive this warning.

2.3.2 Logging In

When you access the Plesk Server Administrator (PSA) control panel, you must enter your login name and password for security purposes.

1. Enter your PSA login name in the first text box.
2. Enter your password in the second box. As you type your password, the letters are masked by asterisks for security purposes.
3. Click **LOGIN** to proceed.

4. Upon your initial log in as administrator you will first be required to accept the PSA product license agreement before being able to utilize PSA.

5. Also upon your initial log in PSA will need confirmation on the IP-Address to be used for name-based hosting as well as the hostname and domain name for the server. PSA will attempt to properly populate these fields from information found on the server.

It is **very** important to note the following:

- As a system administrator, you can log in for the first time with the default login name **admin** and password of **setup** (both are case sensitive - lower case). Be sure to change the password the first time you administer your server.

- Every PSA page has a **HELP** button in the bottom right hand corner. Click **HELP** for detailed information relating to using the current page.

- When you log in as a system administrator, you enter the system on the *Clients List page*. When you log on as a client, you enter into your domain list. When you log on as a domain owner, you enter into that domain's main administration page.

2.3.3 Logging Out

You can leave the PSA interface at any time.

1. Every screen has a **LOG OUT** button in the top right hand corner. Click **LOG OUT** to leave PSA.

2. The PSA asks you to confirm that you really want to leave the system: Click **OK** to leave, or **Cancel** to continue.

3. ADMIN-LEVEL ADMINISTRATION

3.1 Managing the Server

As an administrator using the Plesk Server Administrator (PSA) software, you can perform a variety of server management tasks in a few clicks. When you are logged on as an administrator, click the **SERVER** button located at the top of the screen to bring up the *Server Management page*. From this page, you can access the following functions:

- 3.1.1 System Management
    - Rebooting the System
    - Shutting Down the System
    - IP Aliasing Management System
    - Setting System Time
    - Accessing System Statistics
- 3.1.2 System Services
    - Mail System Management
    - DNS Zone Templates Management
- 3.1.3 Control Panel Management
    - Logo Setup
    - Sessions Management
    - Control Panel Certificate Management
    - Interface Preferences
    - Additional Services Management
- 3.1.4 Admin Information Management
    - Editing Admin Information
    - Setting the Admin Password

3.1.1 System Management

Rebooting the System

Rebooting simply means restarting the server. If users are logged on to the system, you should not reboot the server until you have informed all the users that the server must be

shut down temporarily; however, sometimes an emergency necessitates immediate rebooting of a server to correct a problem that cannot be fixed any other way. To reboot your system, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. Click the **REBOOT** button.
3. PSA warns you that the system will be restarted and asks you to confirm your choice, for safety purposes. Click **OK** to reboot, or **Cancel** to keep the server up.

NOTE: Rebooting the server via the PSA interface also reboots the operating system and anything else running on the server.

Shutting Down the System

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

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. Click the **SHUTDOWN** button.
3. PSA warns you that the system will be shut down and asks you to confirm your choice, for safety purposes. Click **OK** to turn the server off or **Cancel** to keep the server active.

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

IP Aliasing Management System

The *IP Aliasing page* enables the administrator to control IP Aliasing on system network interfaces. This function is specifically for servers that have more than one IP address or are on more than one interface. From this page, the user can:

- Choose the network interface for which he/she wishes to add or remove IP aliases.
- Add an IP alias by entering the appropriate IP address and Subnet Mask.
- Remove one or more IP Aliases from the server.

To add or remove IP Aliases on a server with PSA, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. Click on **IP ALIASING**. The IP Aliasing screen appears.
3. To choose which network interface the IP Aliases will be added to or removed from, select the appropriate **Interface** from the drop down box.
4. To add an IP Alias, enter the appropriate IP address and Subnet Mask in the text boxes provided. Click **ADD** to submit. Once submitted, the new address remains on the screen to facilitate the entry of multiple addresses.
5. To remove one or more IP Aliases from the network interface, first select the necessary **Interface**, and then select the IP Alias from the list you want to delete. Click **REMOVE**.
6. A warning message appears. Click **OKAY** to delete the IP address.
7. Click **UP LEVEL** to return to the *Server Management page.*

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

Setting System Time

As the administrator you are able to manage your server date and time through the interface. From the *System Time page*, you can review and edit the time and date manually. You can also synchronize your server time with the Network Time Protocol (NTP) server. To set the system time, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. To manually set the System Date and Time, in the area beneath **System Date and Time** click in any of the given fields (i.e. Year, Month, Day, Hour, Minute, Seconds) and adjust the information as needed.
3. Click the **SET** button to submit your settings and update the system time.
4. To synchronize your server time with that of a server running the Network Time Protocol, click in the checkbox next to **Synchronize system time**. Once there is a check in this box, this function will be enabled.
5. Enter a valid IP address and click the **SET** button to synchronize.
6. In order for this function to work, you must enter an IP address, which points to a valid NTP server.

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 IP address you enter for synchronization is a valid NTP server. If not, this function will not work and your server will continue to run with its current settings for time.

Accessing System Statistics

Plesk Server Administrator (PSA) compiles statistics on server usage. You can access this information at any time, for viewing or printing. The report is especially helpful if the server is slow or is experiencing performance problems; the report may help you diagnose and correct such problems.

The report lists several informative statistics:

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

Version: This provides with the version of PSA you are running as well as the kernel number.

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

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

Load Averages for the last minute, 5 minutes, and 15 minutes: The average number of processes waiting in the scheduler queue for execution in the last time frame

Hard Disk Usage:

- **Total** - How many bytes of server disk space are on the server
- **Used** - How many bytes of server disk space are being used
- **Available** - How many bytes of server disk space are presently unused and available for use
- **Capacity** - The percentage of disk space presently being used

Domains:

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

To access the *Server Statistics page*, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. Click **STATISTICS**. The server report appears.
3. Click **REFRESH** to update the server statistics with the latest data.

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

3.1.2 System Services

Mail System Management

The *Mail System Management page* allows the administrator to set the parameters for various mail services on the server. The following settings can be adjusted from this page:

- **Max letter size** - this field can be used to set the maximum allowable size of any email received on the server. If this field is left empty, or zero is entered, then the maximum allowable size is "unlimited."
- **Mailbox quota template** – this field can be used to set the default value for mailbox quota for every new domain.
- **Relaying** - these fields are used to set the mail system relay mode. Relaying affects only the sending of mail; it does not in any way change how mail is received on the server. Mail relaying can work in one of three modes: open relay, closed relay and relay with authorization.
    - Open relay - selecting this allows any host computer to utilize the mail services of any domain on the server, to send and/or receive mail. In this mode, no password is required.
    - Closed relay - selecting this only allows mail to be sent and received locally (to and from domains residing on the server). The only exception would be hosts specified as allowable relay hosts in the **White list**.
    - Require authorization - selecting this allows any host computer to utilize the mail services of a domain on the server provided that a valid username and password are used to authenticate the mail user.
        - **POP3** - requires a POP3 login before sending mail. The **lock time** field sets the allowed time given for sending mail after login. During the lock time, any email sent from the initial IP address will be accepted without requiring a password to be re-entered.
        - **SMTP** - smtp authentication (the PSA mail system supports LOGIN, CRAM-MD5 and PLAIN methods of smtp authorization) requires a password every time you send an email.
- **White List** - the White list is a list of IP-addresses with masks from which mail is always accepted.
- **Blockers** - Mail blockers are used to identify mail domains from which you do not allow mail to be received.

In order to manage mail system settings, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. To set the maximum letter size allowed on the server, click in the **Max letter size** text box and enter your desired size in KBytes. Click **SET** to submit.
3. To set the default value of the mailbox quota, click in the Mailbox quota template text box and enter the desired size in Kbytes. Click **SET** to submit.
4. To set the mail system relay mode, click on the radio button next to your desired mode to select it:
    - For open relaying, click on the **Open** button.
    - For closed relaying, click on the **Closed** button.
    - For relaying which requires authorization, click on the **Requires authorization** button. You must then select an authorization type, which can be POP3, SMTP or both.
        - **POP3** - Click a check in the check box next to **POP3** to enable this mode of authorization. You must then set the **lock time**; the default setting is 20 minutes.
        - **SMTP** - Click a check in the check box next to **SMTP** to enable this authorization mode.
    - Click on **SET** to submit.
5. To add an IP address/mask to the White List, type in the appropriate IP Address and mask in the fields provided. Click the **ADD** button to submit. The address selected will appear in the IP list.
6. To remove an IP address/mask from the White List, select the IP address you wish to delete from the IP list. Click the **REMOVE** button.
7. To add a mail blocker, click in the text box next to **Enter domain name** and enter the domain name from which you want to block mail. Click the **ADD** button to submit. The domain you selected will appear in the blocked domain list.

To remove a mail blocker, select the domain you wish to remove from the list of blocked domains. Click the **REMOVE** button.

DNS Zone Templates Management

This page allows you to create the default DNS Zone Templates. Such templates make it easier to set up the DNS records for a freshly created new domain. This feature provides you with a number of DNS records that are more or less standard for a DNS zone.

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

1. Access the server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click on the **DNS** button. The *DNS Zone Template page* appears.

3. Select the type of the record you wish to add from the **Record type** drop down box and click the **ADD** button. The *DNS Zone Template Records Edit page* appears.

4. Fill in the required information into the provided input fields (the type of the information required varies depending on the type of the DNS record selected).

5. Click the **UPDATE** button to submit the entered data and add the new record to the template. If you decide to not add the record, simply click the **UP LEVEL** button. Both will take you back to the *DNS Zone Template page*, one adding the record and the other one skipping any modifications.

NOTE: It is possible not to enter the precise name of the new domain or the IP address. Instead, the following substitutions are made available: **<domain>**, which is then replaced with the domain name, and **<ip>**, which is replaced by the primary IP address.

3.1.3 Control Panel Management

Logo Setup

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

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click the **LOGO SETUP** button. The *Logo Setup page* appears:

3. Click in the **Choose new Logo file** text box and enter the name of the logo file you wish to use. Or, click the **BROWSE...** button and choose a file.

   NOTE: You should use a GIF or a JPEG file format for your logo, preferably no larger than 100 kilobytes to minimize download time. Plesk resizes the logo to fit in the banner area. If you don't want your logo to be resized, you should edit the logo to the exact banner size, which is **558 X 81** pixels.

4. Click **SEND LOGO** to place your logo in the banner area. This may take some time to upload.

5. You have the option to create a hyperlink that activates when a user clicks on your logo. The link may take the user to a corporate URL or other website. Click in the **Enter new Logo link** box. Enter in the URL.

6. Click **SEND LINK** to activate the hyperlink.

7. If you change your mind about a logo, and wish to revert back to the PSA logo, click **DEFAULT LOGO**.

When you have finished defining a local logo and hyperlink, click **UP LEVEL** to return to the *Server Management page*.

Sessions Management

The *Sessions Management page* allows for the set up of different PSA security parameters. The following parameters can be set from this screen:

- **Session idle time** - allowable idle time for any session in PSA. PSA does not allow two sessions using the same login name to run simultaneously; however, should a user session remain idle for a length of time exceeding that specified as the **Session idle time**, then PSA allows that user name to login from a different location, thus ending the idle session.

- **Invalid login interval** - interval between two invalid login attempts within which the invalid login attempts counter is increased. If the time between two invalid login attempts exceeds this value, then the invalid login counter is reset back to 0.

- **Invalid login attempts** - maximum quantity of invalid login attempts allowed. Once a user has exceeded this value, they are locked out for the time specified in the **Invalid login lock time** text box.

- **Invalid login lock time** - lockout time for a user once the invalid login attempts counter has exceeded its maximum limit. During this time, correct attempts will not be accepted. Upon completion of the lockout time, the invalid login attempts counter is reset to "0" and the user is again given the ability to login to PSA.

In order to change the settings for the sessions parameters, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click on the **SESSIONS** button. The *Sessions Management page* appears.

3. To set the **Session idle time**, click in the field provided to the right, and enter the selected time.

4. To set the **Invalid login interval**, click in the field provided to the right, and enter the selected interval.

5. To set the number of **Invalid login attempts**, click in the field to the right, and enter the selected number of attempts.

6. To set the **Invalid login lock time**, click in the field to the right, and enter the selected lock time.

7. Click the **UPDATE** button to submit your settings.

Click the **DEFAULTS** button to return the settings to their default amounts.

Control Panel Certificate Management

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

Notes on Certificates:

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

To generate a self-signed certificate or a certificate-signing request, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click the **CERTIFICATE** button. The *SSL certificate setup page* appears.

3. The **Certificate Information:** section lists information needed for a certificate Request, or a Self-Signed certificate.

4. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop down box next to **Bits:.**

5. To enter the information into the provided text input fields (**State or Province**, **Locality**, **Organization Name** and **Organization Unit Name** (optional)) click in the text boxes and enter the appropriate names.

6. To enter the Domain Name for the certificate, click in the text box next to **Domain Name:** and enter the appropriate domain.

7. The domain name is a required field. This will be the only domain name that can be used to access the Control Panel without receiving a certificate warning in the browser. The expected format is www.domainname.com or domainname.com.

8. Click on either the **SELF-SIGNED** or **REQUEST** button.

9. Clicking **SELF-SIGNED** results in your certificate being automatically generated and posted to your certificate directory. Selecting **REQUEST** results in the sending of a certificate-signing request to the email provided.

When you are satisfied that the SSL certificate has been generated or the SSL certificate request has been correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

To purchase a certificate through the My.Plesk.com, first complete the steps given in the items 1 – 7 of the previous instruction (generating a self-signed certificate or a certificate-signing request) and then proceed to:

8. Click on the **BUY CERTS** button to gain access to the certificate management interface on My.Plesk.com. The *MPC Gate page* appears.

9. This page allows you to create account (the **CREATE ACCOUNT** button) and access (the **LOG IN** button) to MPC from where you are able to purchase and manage the certificates.

10. In case you already have an existing account on MPC but forgot the password for it, there is a button provided especially for such occasions: **FORGET PASSWORD?**. Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your Server Administrator profile.

NOTE: if you do not wish to purchase certificates at this time but do wish to view the certificates currently owned by you, you may proceed directly to the *MPC Gate page* by clicking the **VIEW CERTS** button. At that you will not be prompted to fill in the details at the *SSL Certificate setup page*.

To upload a file containing the certificate authorized by the Certificate Signing Authority:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click the **CERTIFICATE** button. The *SSL certificate page* appears.

3. If you wish to upload a Certificate File authorized by the Certificate Signing Authority, click the **BROWSE…** button under the **Upload previously bought Certificate File (without private key)** section to select the file (the file must be in .txt format)

4. Then, click **SEND FILE** to copy the certificate to the server.

To upload a new certificate:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click the **CERTIFICATE** button. The *SSL certificate page* appears.

3. If you wish to upload a certificate file from a local computer, under the **Uploading Certificate File** section, click the **BROWSE…** button to select the file (the file must be in .txt format).

4. Then, click **SEND FILE** to copy the certificate to the server. Or, if you want to type in the text of the certificate without uploading a specific file, click in the text box and enter and paste the certificate information.

5. Click **SEND TEXT** to implement the text on the server.

   NOTE: Ensure that the private key text block is included along with the SSL certificate text block when using the **SEND FILE** or **SEND TEXT** options.

6. When you upload the certificate to the server, PSA checks for errors. If an error is detected, PSA restores the old version of the SSL certificate, and PSA warns you to update the certificate. At this point, you can try again to enter text or to upload the certificate file.

7. When you are satisfied that the SSL certificate is correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

If you are using a certificate that has been signed by an authority other than Thawte or Verisign then it is likely that this will require the use of a rootchain, or CA, certificate. To install a rootchain certificate for the domain:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click the **CERTIFICATE** button. The *SSL certificate setup page* appears.

3. The icon next to **Use rootchain certificate for this domain** appears on this page.

4. If the icon is **[ON]** then the rootchain certificate will be enabled for this domain. If the icon is **[X]** this function will be disabled.

5. To change the status of the rootchain certificate, click the **ON/OFF** button.

6. To upload your rootchain certificate, first make sure that it has been saved on your local machine or network. Use the **Browse** button to search for and select the appropriate rootchain certificate file.

7. Then click the **SEND FILE** button. This will upload your rootchain certificate to the server to assure proper authentication of the certificate authority.

Interface Preferences

PSA is intended to provide an option of choosing the interface language. For this moment only English is available. This page also allows you to set a number of lines displayed on the pages containing the lists (i.e.: Domains List, Clients List, etc.).

To change the number of lines displayed per page:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click the **PREFERENCES** button. The *Control Panel Preferences page* appears.

3. Click in the **Enter display lines per page** input box and enter the number of lines you want to see displayed on the pages.

4. Click the **UPDATE** button or the **UP LEVEL** button to return to the *Server Management page*. One will commit the changes; the other one will leave the settings unchanged.

To change the control panel interface language:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.

2. Click the **PREFERENCES** button. The *Control Panel Preferences page* appears.

3. Select the desired language from the drop down box (currently only English is available).

4. Click the **UPDATE** button or the **UP LEVEL** button to return to the *Server Management page*. One will commit the changes; the other one will leave the settings unchanged.

Additional Services Management

This page allows you to manage a few additional services available through My.Plesk.com (MPC). The current services are Domain Registration, Certificate Purchasing and Extras (general MPC access).

To activate (or deactivate) a certain service, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. Click the **ADD SERVICES** button. The *Additional Services Management page* appears.
3. Check (or uncheck) the checkbox corresponding to the service you wish to activate (or deactivate).
4. Click the **UPDATE** button or the **UP LEVEL** button to return to the *Server Management page*. One will commit the changes; the other one will leave the settings unchanged.

3.1.4 Admin Information Management

Editing Admin Information

This page allows you to enter contact information for the administrator. The email address to which the administrator receives messages from users was set when you installed the PSA software. You can change this email address at any time. To enter or edit Admin information, follow these steps:

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. Click the **EDIT** button. The *Edit Administrator Information page* appears.
3. Click in any of the desired fields and enter the admin information.
4. All the required fields are marked with asterisks.
5. You can return to this page and edit this information at any time.
6. Click the **UPDATE** button to submit your information.

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

Setting the Admin Password

You can change the administrative password at any time. Regularly changing the administrative password is a good idea for security purposes.

1. Access server management functions by clicking on the **SERVER** button at the top of the PSA interface. The *Server Management page* appears.
2. Click the **CHANGE PASSWORD** button. The *Change Server Administrator Password page* appears.
3. Click in the **Old password** text box and enter your current password.

4. Click in the **New password** text box and enter the password that you wish to change to.
5. Click in the **Confirm password** text box and re-enter the new password, exactly as you entered it in the **New password** text box.
6. Click the **UPDATE** button opposite the **Confirm** text box.

NOTE: The default password is "setup" and is established during the installation process. Because of this, you cannot "create" a password, rather you can only change it.

3.2 Managing Clients

As an administrator using the Plesk Server Administrator (PSA) software, you can perform a variety of server management tasks in a few clicks. When you are logged on as an administrator, click the **CLIENTS** button located at the top of the screen to access client management. This will take you to the *Client List page*, from which you can perform the following client management functions:

- 3.2.1 Client List Page
    - Client List
    - Searching the Client List
    - Creating a Client
    - Additional Services (Extras)
- 3.2.2 Client Home Page
    - Activating or Deactivating a Client
    - Editing a Client Information
    - Accessing a Client Status Report
    - Editing the Preferences for the account
    - Create a New Domain
    - Registering and Managing the Domain via MPC.
    - Additional Services (Extras)
    - Domain List
    - Searching the Domain List

3.2.1 Client List Page

When you log on as an administrator, you access the Clients List page. This page lists all of your clients currently registered in the PSA system as well as their status.

NOTE: when you first log on to PSA, this page will be blank until you, the admin, create clients.

As an administrator, you can also access this page from anywhere in the PSA system, by clicking the **CLIENTS** button.

From this page, you can access all the administrative functions that enable you to manage your server and to create domains and clients. You can choose how clients are sorted. You can create a new client by clicking on the **NEW CLIENT** button and entering the client information. The **EXTRAS** button allows the access to the external services provided by out company and available through My.Plesk.com. Click on any client name in the client list, and you access the *Client Home page* where you can perform a number of client management functions.

Possible Clients may include, for example:

- Customers accessing the server of a Web hosting company
- Users of the server on the intranet of a small business
- Companies accessing a remote Internet server
- Customers of an Internet Service Provider

NOTE: As an administrator, you can create as many clients as you need, with any type of name. The amount of the clients you are allowed to create can be limited only by the key you have installed.

Client List

Each client entry lists the client's status, creation date and name. The client's status is represented by two icons to the left of the client's name:

[OK][ON]

The first status icon indicates the system status of the client:

[OK] means that the client's account is operating within defined disk space and traffic parameters.
[!] means that the client has exceeded allocated disk space or traffic limitations in at least one of the client's domains. The PSA system evaluates disk space and traffic every 24 hours.

The second icon indicates if the system administrator has activated this client:

[ON] means that the client is activated.
[X] means that this client is presently deactivated or turned off. If the client is turned off, all of the client's domains are deactivated and inaccessible.

When a new client is created, a corresponding new entry is added to the Client List. The Client List also allows you to remove clients (clients' accounts) from the system. To remove one or more clients, follow these steps:

1. Check the checkboxes in the **Del** column of the Client List corresponding to the clients you wish to remove.
2. Click on **REMOVE SELECTED**. The *Client Removal page* appears.
3. For every client you chose to remove the Client Name and the Domain Names that belong to this client will be displayed.
4. If you are certain that the displayed information is correct and wish to proceed with deleting, check the "Yes, I have read, understood, and agree to remove these clients and all their domains" checkbox. Then click **SUBMIT**. If you decide to not delete these clients or wish to modify the list of clients chosen for deletion, click the **CANCEL** button.
5. Both buttons will return you to the *Client List page*, one committing the changes, the other one leaving everything unchanged.

Searching the Client List

PSA allows you to search the Client List for a certain pattern. It may help you in case you have a great number of clients in the system and you need to work with a particular one. To search in the Client List:

- Select the input field and type in the pattern string.
- Click the **SEARCH** button.
- If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Client List.
- If no matches were found it will be so stated.
- The button SHOW ALL will revert to displaying the whole list of PSA clients.

There is also another way to ease the process of working with a large list of clients. An option of sorting the list by several various parameters is made available to you. You can sort the Client List by **Problem State**, **Status**, **Creation Date** and **Client Name**. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Creating a Client

As an administrator, your first step in setting up a server system is to create the clients who are access the server. If you are in a hurry, you can create clients by initially entering their login names, passwords and company contact names. You can always add detailed information to client record at a later time:

1. Access the client management functions by clicking on the **CLIENTS** button at the top of the Plesk Server Administrator (PSA) interface. The *Client List page* appears.

2. Check the list of current clients to see if the client you wish to create already exists. If no client exists with the name you wish to create, then click the **NEW CLIENT** button.

   NOTE: If a client record already exists, click on the client's name to edit the record. See Editing a Client Record for step-by-step instructions for updating an existing client.

3. PSA displays the *New Client page*. It prompts you to enter all the information required to create a new client.

4. Enter all the data for your new client in the text boxes. Click in a specific text box to enter data, or use the TAB key to move from one text box to the next. The following data fields are required:

   - **Contact Name** - This is the name that appears in the **CLIENTS** list as well as when you select a client to add a new domain. The contact name must be unique in order to work with in the PSA system.

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

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

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

5. The last text box is a two-part entry. First, enter the client's domain name in the text box. Second, make sure a check mark appears in the WWW check box. Selecting this enables users to include the WWW prefix to access this domain. If WWW is not required (typically because this domain is for local use only), make sure the WWW checkbox remains unchecked.

NOTE: You must officially register the domain and Internet address before you can create a domain and internet address in the PSA. Use any Internet registration service to do this.

6. Review the entered information. Edit data in any text box by clicking and editing the specific word or phrase.
7. When you are satisfied that the information is complete and correct, click **UPDATE**.
8. The PSA notifies you if you are missing data in any required fields. If data is missing, return to the client record and complete the necessary fields.
9. Click **UPDATE** to save the revised information.

NOTE: You can leave the Client function at any time without saving your work. Click **UP LEVEL** to discard all entries you have made and to return to the main page.

Additional Services (Extras)

From the *Client List page* you can access external services (other than registering domains and managing domains registration) provided through My.Plesk.com. To do that, click the **EXTRAS** button.

3.2.2 Client Home Page

The *Client Home page* allows the administrator to perform various client management functions, such as:

- Activating or Deactivating a Client
- Editing a Client's Information
- Accessing a Client Status Report
- Editing the Preferences for a Client’s account
- Creating a New Domain for a Client
- Registering and Managing the Domain Registration via MPC
- Additional Services (Extras)
- Domain List

- Searching the Domain List

To access this page:

1. Access the client management function by clicking on the **CLIENTS** button at the top of the PSA interface. The *Client List page* appears.
2. Click on the client name that you wish to update. The *Client Home page* appears.

Activating or Deactivating a Client

There are times when the administrator may need to deactivate all of a client's domains. To do this, you turn a client OFF. You must be logged on as a system administrator in order to turn a client **ON/OFF**.

1. Access the client management function by clicking on the **CLIENTS** button at the top of the PSA interface. The *Client List page* appears.
2. Click on the client name that you wish to change. The *Client Home page* appears:

   The client's current status is listed in two status icons, such as:

   [OK][ON]

   The first status icon indicates the system status of the client:

   [OK] means that the client's account is operating within the defined disk space and traffic parameters.
   [!] means that the client has exceeded allocated disk space or traffic limitations in at least one of the client's domains. The PSA system evaluates disk space and traffic every 24 hours.

   The second icon indicates if the system administrator has activated this client:

   [ON] means that the client is activated.
   [X] means that this client is presently deactivated or turned off. If the client is turned off, all of the client's domains are deactivated and inaccessible.

3. Click **ON/OFF** to change the client's status.
4. PSA will ask you to confirm that you want to change the status of the client. Click **OK** to change the status, or **Cancel** to keep the current client status.

Editing a Client Information

Occasionally, you may need to change the information in a client's record (e.g. if the company needs to change its contact information). Changing a client on a PSA managed server is simple:

1. Access the client management function by clicking on the **CLIENTS** button at the top of the PSA interface. The *Client List page* appears.
2. Click on the name of the client whose information you wish to edit.
3. The *Client Home page* appears, listing the client status and the domains that the client owns (if any). To update the client data, click **EDIT**.
4. PSA displays the full client data page. Click in any text box to change or edit the information. Four data fields are required: **Contact Name**, **Control Panel login name**, **Control Panel password** and **Confirm password**. Be sure to complete these fields before saving the record.
5. When you are done, click **UPDATE** to save the revised information. The changes are activated immediately.

NOTE: You can exit the client editing function without saving your changes at any time. Click **UP LEVEL** to discard the changes you have made to this record and to revert to the most recent version of the client record.

Accessing a Client Status Report

The Plesk Server Administrator (PSA) keeps a summary of important data for every client on the Plesk system. As an administrator you can view this information at any time. The client report includes the following information:

- PSA build number
- Client status
- Company name
- Control Panel login name
- Creation date
- Phone
- Fax
- E-mail
- Street address
- City
- State/Province
- Postal/ZIP code
- Country
- Interface language

To access the client status report, follow these steps:

1. Access the client management function by clicking on the **CLIENTS** button at the top of the PSA interface. The *Client List page* appears.
2. Click on the name of the client on which you wish to receive a report.
3. The *Client Home page* appears.
4. Click the **REPORT** button to see the client's report.
5. From here, you can do these things:
    - Email the report to the client or other individual administrators. You may want to do this, for example, if your client has forgotten his/her login information or if the client has exceeded account limitations and you want to remind him/her of an inactive status.
    - Enter the email address of the desired recipient of the report in the provided text box. Click the **SEND AS E-MAIL** button to send the report.
    - Return to the client record. Click **UP LEVEL** to close the report and to return to the *Client Home page*.
    - Print a copy of the report. Select File/Print in your browser to print a paper copy of the report you are viewing.

Editing the Preferences for the account

When a client is added to the PSA system, in order to become a legitimate user this client needs to have the necessary permissions, privileges, quotas and limits set by the administrator. Click the **PREFERENCES** button on the *Client Home page* to access the page with two buttons: **PERMISSIONS** and **LOGO SETUP**.

- The **PERMISSIONS** button takes you to the *Client Permissions page*. This page allows you to enable or disable the client to perform certain functions within his/her account and to manage the resource allocated to the client.
- The **LOGO SETUP** button takes you to the *Client Logo Setup page*. This page allows you to set up the logo preferences for the client’s account.

To set up or modify the Permissions for the client, follow these steps:

1. Access the client management function by clicking on the **CLIENTS** button at the top of the PSA interface and then click on the name of the client in the Client List at the *Client List page*. The *Client Home page* appears.
2. Click the **PREFERENCES** button, and then, when the *Client Preferences page* appears, click **PERMISSIONS**. The *Client Permissions page* appears.

3. Check the **Client can create domains** checkbox if you wish to allow this particular client to be able to do that.

4. A list of features available for setting limits follows. It includes:

   - Maximum number of domains the client can have
   - Total disk space
   - Total amount of traffic
   - Maximum number of mailboxes
   - Maximum mailbox quota
   - Maximum number of redirects
   - Maximum amount of mail groups
   - Maximum number of autoresponders
   - Maximum number of web users the client can create
   - Maximum number of databases

5. To set the value of each of these items, check the corresponding checkbox placed to the left of the feature name, click in the text input field and enter the limiting value for this particular feature.

6. To allow the client to create IP-based hosting accounts check the corresponding checkbox and select the set of available IP by choosing between **All available IP** and **List available IP**. For the latter, you can add or remove available IP using the **ADD** and **REMOVE** buttons and the IP-list.

NOTE: All the above features may be edited only if the **Client can create domains** checkbox is activated, which means that the Administrator authorizes the Client to perform certain functions concerning creating new and managing existing domains. Otherwise, the Administrator is responsible for handling all such matters.

7. Also you can allow or forbid the client to **manage DNS zone** and **log rotation** as well as set the number of lines displayed on the page containing the lists (i.e.: Domains List, Clients List, etc.).

8. Click the **UPDATE** button to submit the entered data. If you decide to not change the settings this time, simply click the **UP LEVEL** button. Both will take you back to the *Client Preferences page,* one submitting the changes and the other one skipping any modifications.

To set up or modify the logo preferences for the client, follow these steps:

1. Access the client management function by clicking on the **CLIENTS** button at the top of the PSA interface and then click on the name of the client in the Client List at the *Client List page*. The *Client Home page* appears.

2. Click the **PREFERENCES** button, and then, when the *Client Preferences page* appears, click **LOGO SETUP**. The *Client Logo Setup page* appears.

3. To submit a logo you must have the desired graphics file on your local machine. Choose the file from your local machine and click on **SEND LOGO**. (*.GIF and *.JPG files only, 558x81 recommended).

4. To submit a link, type the desired URL in the field provided and click on **SEND LINK**.

5. The **DEFAULT LOGO** button will revert the logo back to the default Server Administrator logo on default language.

6. Click **UP LEVEL** to return to the *Client Preferences page*.

Create a New Domain

When you create a new client record, you assign a domain to the client. Sometimes, you may need to add additional domains to a client's account. You can create a new domain for a client at any time.

1. Access the client management function by clicking on the **CLIENTS** button at the top of the PSA interface. The *Client List page* appears.

2. Click on the client name that you wish to update. The *Client Home page* appears.

3. Click the **NEW DOMAIN** button.

4. The *Client Domain Creation page* appears containing the client information.

5. To create the new client domain, click in the **New domain name** text box and enter the name.

6. Make sure a check mark appears in the WWW check box if users must include the WWW prefix to access this domain. If WWW is not required (typically because this domain is for local use only), click to clear the WWW check box so that it is unchecked.

   NOTE: You must officially register a domain and Internet address before you create it in PSA. Use any Internet registration service to do this.

7. Click **UPDATE** to add the domain to the client's account. Repeat these steps to add additional domains.

NOTE: You can exit the domain creation function without saving your changes. Click **UP LEVEL** to discard all changes you have made to this record and to revert to the most recent version of the client record.

Registering and Managing the Domain via MPC.

When a new domain is created it must be officially registered. There are a number of Internet services where you can register your domain but there is one that is offered by Plesk Inc.

To register a new domain, follow these steps:

1. Access the *Client Management page* by clicking on the **CLIENTS** button at the top of the PSA interface. The *Client List page* appears.

2. Click on the name of the client whose domain you wish to register. The *Client Home page* appears.

3. Click the **REGISTER** button to access the *MPC Gate page*.

4. From *MPC Gate page* you can access the services provided to you by My.Plesk.com. To do that, enter the **MPC Login** and **MPC Password** into the provided corresponding text input fields and click **LOG IN**.

   NOTE: You can do that if you already have an account at MPC. If you do not, you can create one by clicking **CREATE ACCOUNT**.

5. You can check the **Remember account** checkbox to have you login and password remembered by the system. This way the next time you wish to access MPC, you will be taken directly to My.Plesk.com and will not be prompted to enter your login and password.

   NOTE: This feature will save the login and password for anyone that accesses this Client record. This function is intended for use by the Client, and is not recommended for the Administrator of the server.

6. In case you forgot the password, there is a button provided especially for such occasions: **FORGET PASSWORD?** Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your Server Administrator profile.

7. You can return to the *Client Home page* by clicking **UP LEVEL**.

To manage already existing domains, follow these steps:

1. Access the *Client Management page* by clicking on the **CLIENTS** button at the top of the PSA interface. The *Client List page* appears.

2. Click on the name of the client whose domain you wish to manage. The *Client Home page* appears.

3. Click the **MANAGE** button to access the *MPC Gate page*.

4. From *MPC Gate page* you can access the services provided to you by My.Plesk.com. To do that, enter the **MPC Login** and **MPC Password** into the provided corresponding text input fields and click **LOG IN**.

5. You can check the **Remember account** checkbox to have you login and password remembered by the system. This way the next time you wish to access MPC, you will be taken directly to My.Plesk.com and will not be prompted to enter your login and password.

   NOTE: This feature will save the login and password for anyone that accesses this Client record. This function is intended for use by the Client, and is not recommended for the Administrator of the server.

6. In case you forgot the password, there is a button provided especially for such occasions: **FORGET PASSWORD?** Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your Server Administrator profile.

7. You can return to the *Client Home page* by clicking **UP LEVEL**.

Additional Services (Extras)

From the *Client Home page* you can access external services (other than registering domains and managing domains registration) provided through My.Plesk.com. To do that, click the **EXTRAS** button.

Domain List

Each domain entry lists the domain status, creation date and name. The domain status is represented by three icons to the left of the domain name:

[OK][ON][ON]

The first status icon indicates the status of the domain:

[OK] if the domain is operated within the disk space and traffic limitations.
[!] if the domain has exceeded disk space or traffic limitations. The PSA system evaluates disk space and traffic every 24 hours.

The second icon indicates whether the domain has been turned **ON** or **OFF** by the Administrator:

[ON] means that the domain is activated.
[X] means that this domain is presently turned off and presently deactivated or inaccessible. If the domain is turned **OFF**, no service will be rendered to the given domain.

The third icon indicates whether the domain has been turned **ON** or **OFF** by the client:

[ON] means that the domain is activated.
[X] means that this domain is presently turned off and presently deactivated or inaccessible. If the domain is turned **OFF**, no service will be rendered to the given domain.

When a new domain is created, a corresponding new entry is added to the Domain List. The Domain List also allows you to remove domains from the system. To remove one or more domains, follow these steps:

1. Check the checkboxes in the **Del** column of the Domain List corresponding to the domains you wish to remove.
2. Click on **REMOVE SELECTED**. The *Domain Removal page* appears.
3. For every domain you chose to remove the Domain Name will be displayed.
4. If you are certain that the displayed information is correct and wish to proceed with deleting, check the "Yes, I have read, understood, and agree to remove these domains" checkbox. Then click **SUBMIT**. If you decide to not delete these domains or wish to modify the list of domains chosen for deletion, click the **CANCEL** button.
5. Both buttons will return you to the *Client Home page*, one committing the changes, the other one leaving everything unchanged.

Searching the Domain List

PSA allows you to search the Domain List for a certain pattern. It may help you in case you have a great number of domains in the system and you need to work with a particular one. To search in the Domain List:

- Select the input field and type in the pattern string.
- Click the **SEARCH** button.
- If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Domain List.
- If no matches were found it will be so stated.
- The button **SHOW ALL** will revert to displaying the whole list of domains.

There is also another way to ease the process of working with a large list of domains. An option of sorting the list by several various parameters is made available to you. You can sort the Domain List by **Problem State**, **Status (Admin)**, **Status (Client)**, **Creation Date** and **Domain Name**. To sort the list by a certain parameter in ascending or

descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

3.3 Managing Domains

As an administrator using the Plesk Server Administrator (PSA) software, you can perform a variety of server management tasks in a few clicks. When you are logged on as an administrator, click the **DOMAINS** button located at the top of the screen to access Domain Management. This will take you to the *Domains List page*, from which you can perform the following domain management functions:

- 3.3.1 Domains List Page
    - Searching the Domain List
    - Deleting Domains
    - Creating a Domain
    - Editing a Domain
- 3.3.2 Domain Administration Page
    - Turning a Domain On or Off
    - Domain Preferences
    - Domain Report
    - Managing Mail
        - Mail Names Page
        - Mail Name Properties Page
            - Managing Mailbox Accounts
            - Managing Mail Redirects
            - Managing Mail Groups
            - Managing Mail Autoresponders
    - Customize DNS Settings
        - DNS Settings Page
        - Changing DNS Settings
        - DNS Example Setups
    - Changing Hosting Account Settings
        - Physical Hosting Configuration

        - Standard Forwarding Configuration
        - Frame Forwarding Configuration
    - Web User Management
    - Protected Directories
        - Creating a Protected Directory
        - Changing a Protected Directory
        - Searching the Protected Directories List
        - Removing a Protected Directory
    - SSL Certificate Management
        - Generate a Self-signed Certificate or Certificate Signing Request
        - Purchase an SSL Certificate
        - Upload Existing Certificate w/o Private Key
        - Upload a New Certificate w/ Private Key
        - Uploading the Rootchain Certificate
    - Anonymous FTP
    - Database Management
        - Searching the Database List
        - Creating a New Database
        - Editing an Existing Database
    - Domain User

3.3.1 Domains List Page

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

Domains are identified by their familiar Internet URL (uniform resource locator) addresses. Syntactically, a domain name is a string of names or words separated by

periods. For example, www.plesk.com is the name of the domain where Plesk's information resides on its servers. A domain must belong to one client. For example, John Smith may be a programmer whose domain is aceprogrammer.com; the ABCDE, Inc. company may own a domain by the name of abcde.com. All domains must be assigned to clients.

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

Domain Status Icons

Each domain entry lists the domain's status, creation date, and name. The domain status consists of three icons:

[OK][ON][ON]

The first status icon indicates the system status of the domain:

[OK] means that the account is operating within defined disk space and traffic parameters.
[!] means that the account has exceeded allocated disk space or traffic limitations within that domain. The PSA system evaluates disk space and traffic every 24 hours.

The second icon indicates whether the system administrator has turned a domain on or off:

[ON] means that the domain is activated.
[X] means that the domain is presently deactivated or turned off. The domain is inaccessible.

The third icon indicates if the client has turned the domain on or off:

[ON] means that the domain is activated.
[X] means that the domain is turned off and presently inaccessible.

Searching the Domain List

PSA allows you to search the Domain List for a certain pattern. It may help you in case you have a great number of domains in the system and you need to work with a particular one. To search in the Domain List:

1. Select the input field and type in the pattern string.
2. Click the **SEARCH** button.

3. If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Domain List.

4. If no matches were found it will be so stated.

5. The button **SHOW ALL** will revert to displaying the whole list of domains.

There is also another way to ease the process of working with a large list of domains. An option of sorting the list by several various parameters is made available to you. You can sort the Domain List by **Problem State**, **Status (Admin)**, **Status (Client)**, **Creation Date** and **Domain Name**. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Deleting Domains

To delete existing domains select the domains that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. Care should be taken when performing this action as this will delete all content related to the domain, and the action is not reversible. You will be asked for confirmation prior to final deletion of the domains.

Creating a Domain

You can create a domain in three different ways:

- Use the **NEW CLIENT** function from the *Client List page*. When you create a client, you can, at the same time, add a domain name to the record.

- Use the **NEW DOMAIN** function from the *Domain List page*. When you create a domain, you can create its client at the same time or choose from the existing clients.

- Use the **NEW DOMAIN** function from the *Client Home page* to create a domain for the already existing client.

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

To create a new domain and fully configure its services, follow these steps:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Check the list of current domains to see if the domain you wish to create already exists. If the domain you wish to create does not exist, then click the **NEW DOMAIN** button.

   NOTE: If a record already exists for the domain, click on the domain's name to

edit the record. See Editing a Domain for step-by-step instructions for updating an existing domain.

3. PSA displays the *New Domain page*. It prompts you for all the information you need to create a new domain.
4. Enter all the data for the new domain in the text boxes. Use the TAB key to move from one text box to the next one or just click inside a specific text box to enter information. The following data fields are required:
    - **Domain Name** - Enter a valid domain name (e.g. mycompany.com) that is unique to the system. If you enter a domain name that already exists, PSA will ask you to change it. The **New Domain Name** field also has a prompt for the WWW tag. The WWW checkbox, when checked, indicates that the WWW prefix can be used when addressing the domain as well as the domain name by itself. If the box is unchecked, then the domain can only be referenced by its name without the WWW prefix.
    - **Client** – Select the appropriate client from the list of existing clients or create a new client by filling in the appropriate fields below. When creating a new client you must fill in, as a minimum, the Contact name, Control Panel login name, and Control Panel Password. See Section 3.2.1 for more information on creating clients.
5. If you are creating a domain for a client who already exists in the system, PSA enters the client name in the Contact Name field, and adds the information from the client record to this domain record.
6. You can edit data in any text box by clicking and editing a specific word or phrase.
7. When you are satisfied that the information is complete and correct, click **UPDATE**.
8. PSA informs you if any required entries are missing. If data is missing, then return to the domain record and complete the necessary fields. Click the **UPDATE** button to save the revised information.

NOTE: You can leave the new domain function at any time without saving your work. Click **UP LEVEL** to return to the main page and to delete all data entered in this new domain record.

Editing a Domain

Occasionally, you may need to change the information in a domain's record. This may occur if the company has changed its name, address, phone numbers et cetera. Since the information in a domain record is actually the data from the owning client's record, you edit domain record data by editing the client record.

1. Access the client list by clicking the **CLIENTS** button at the top of the PSA interface.
2. Click on the name of the client who owns the domain you wish to edit.
3. The client summary page appears, listing the domains that the client owns. To update the client data, click **EDIT**.
4. PSA displays the full client data page. Click in any text box to edit the information.
5. When you are done, click **UPDATE** to save the revised information. The changes take place immediately.

NOTE: At any time you can exit the client editing function without saving your changes. Click **UP LEVEL** to discard changes made to the record and to revert to the most recent version of the client and domain records.

3.3.2 Domain Administration Page

This page gives you access to several domain administration functions. From this screen, you can:

- Turn the Domain ON or OFF.
- Access Domain Preferences.
- Access a Domain Report.
- Manage Mail for a Domain.
- Customize DNS settings.
- Register a Domain
- Set-up Hosting.
- Create Web Users.
- Create Protected Directories.
- Manage the Domain SSL Certificate.
- Set-up Anonymous FTP
- Manage Databases
- Set-up the Domain Level Control Panel Login

Turning a Domain On or Off

If you need to deactivate a domain, you may do so. Administrators may deactivate any domain on a PSA server, whereas clients may deactivate any of their domains.

Each domain entry lists the domain's status, creation date and name. The domain status consists of three icons:

[OK][ON][ON]

The first status icon indicates the system status of the domain:
[OK] means that the account is operating within defined disk space and traffic parameters.
[!] means that the account has exceeded allocated disk space or traffic limitations within that domain. The PSA system evaluates disk space and traffic every 24 hours.

The second icon indicates whether the system administrator has turned a domain on or off:

[OK] means that the domain is activated.
[X] means that the domain is presently deactivated or turned off. The domain is inaccessible.

The third icon indicates if the client has turned the domain on or off:

[OK] means that the domain is activated.
[X] means that the domain is turned off and presently inaccessible.

To turn a domain ON/OFF, follow these steps:

1. Access the Domains function by clicking the **DOMAINS** button.
2. Click on the domain name that you wish to change. The *Domain Administration page* appears.
3. Click **ON/OFF** button to change the domain's status.
4. PSA asks you to confirm that you want to change the status of the domain. Click **OK** to change the status, or **Cancel** to keep the current client status.

NOTE: If you are an administrator deactivating a domain, you should inform the client as to why the domain's status has changed.

Domain Preferences

This page allows the administrator to set domain level limitations for total disk space, the maximum number of mailboxes and the mailbox quota, mail redirects, mail groups,

autoresponders, web users, and databases.. This screen also allows the set up of a mail bounce message or a catch-all email address for invalid user names. These items are used to handle mail received by this domain for mail accounts not existing within the domain. If a user wishes to change the status of the 'www' prefix requirement for the domain; that would be changeable on this page. You may also pass on scripting capabilities to domain web users and setup the use of webmail for the domain.

To adjust the domain preference settings, follow these steps:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you want to work with. The *Domain Administration page* appears.

3. Click on the **PREFERENCES** button to access the *Domain Preferences page*. Note that there may be some preset limits set based on the limits set on the client owner of the given domain. A domain limit can not exceed the limits of the resources available to the client who owns the domain.

4. To set the **Disk space limit**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit, in MegaBytes, in the field provided. This number represents all content within the domains root directory and sub-directories as well as disk space used by the given domain's databases.

5. To set the **Maximum Mail Boxes**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit in the field provided.

6. To set the **Mailbox Quota**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit, in KiloBytes, in the field provided.

7. To set the **Maximum Mail Redirects**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit in the field provided.

8. To set the **Maximum Mail Groups**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit in the field provided.

9. To set the **Maximum Mail Autoresponders**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit in the field provided.

   NOTE: If the value for any of these mail features is set to zero, then the client is not allowed to create that particular account type.

10. To set the **Maximum Web Users**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit in the field provided.

11. To set the **Maximum Databases**, click on the radio button to the right for **Unlimited** to set the maximum as unlimited, or click on **Enter Number**, then enter the desired Maximum limit in the field provided.

12. To utilize a mail bounce message, select the radio button for **Bounce with Phrase** and enter the appropriate text.

13. To utilize a catch-all email address, select the radio button for **Catch to Address** and enter the appropriate e-mail address.

    NOTE: You cannot select both a mail bounce message and a catch-all email address.

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

15. Check or uncheck the **Allow scripting for web users** checkbox to allow or disallow the use of scripting for web users created within the given domain. Note that this simply allows the domain owner to select from the scripting options given to the domain.

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

17. Click the **UPDATE** button to submit any and all changes and return to the *Domain List page.*

18. Click the **UP LEVEL** button to ignore all changes and return to the *Domain List page*.

NOTE: If data is improperly entered (i.e. the wrong format of an email address, et cetera), an error message appears with an error notice.

Domain Report

The Plesk Server Administrator (PSA) keeps a summary of pertinent data for every domain on the PSA server. You can view this information at any time. At the top of the

page, the domain being reported on is listed in boldface. The domain report includes the following information as is applicable to the given domain:

- Domain owner (client)
- Domain status
- Creation date
- Hosting type
- Virtual host type
- IP-Address
- FTP Login
- FTP Password
- Disk space limit
- Real disk space
- Traffic limit
- Real traffic
- FrontPage support
- SSI support
- PHP support
- CGI support
- mod_perl support
- Apache ASP support
- SSL support
- Web statistics
- Web users
- Apache ErrorDocuments
- Anonymous FTP
- Mailboxes
- Redirects

- Mail Groups
- Autoresponders
- Domain user
- Databases

In order to utilize this feature follow these steps:

1. Access the Domain Management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you need to work with. The *Domain Administration page* appears.
3. Click the **REPORT** button to see the domain's data and statistics.
4. From here, as an administrator, you can do several things:
    - You can send the report as an email to the client. Your client may need this detailed information about his/her domain. Email the report to the client by clicking **SEND AS E-MAIL**. Or, enter a different email address in the "X" box to send the report to another administrator or individual.
    - You can access graphical site statistics for the domain by selecting the **WEBALIZER** option. This opens a separate window where you will see the site statistics for the given domain. It should be noted that Webalizer, by default, is set to update statistics for the domain once every 24 hours. If you attempt to access Webalizer before it has operated its first update you will receive a notice that Webalizer is either not running or has not yet been started.

      NOTE: In order to be able to utilize **WEBALIZER** the **Web statistics** checkbox must be checked at the *Physical Hosting Configuration page* for this domain.
    - To print a copy of the domain report screen, select **File/Print** in your browser and a paper copy of the report will print.
    - To return to the domain record, click **UP LEVEL**. The report will close and you will return to the domain administration page.

Managing Mail

The Plesk Server Administrator (PSA) uses the qmail system. Because qmail does not allow the mail server to be accessed remotely, the email system is protected against spamming. You can create and manage email boxes for individuals within a domain, or your client can manage the email accounts via domain self-administration. As an

administrator, you can use the domain administration page for several email administration functions:

- Create, edit or delete email boxes and set individual mailbox quotas
- Redirect or forward messages from one email address to another email address
- Create, edit or delete email groups (several individual accounts grouped together under one email address for convenient multi-copy messaging).
- Create, edit, or delete email autoresponders (automatic reply to email sent to the given mail name)

Mail Names Page

When you create email accounts for domain users, you are creating email boxes which will be accessible via POP3 or IMAP protocols. Mailbox creation is as easy as keying in a name and password. Follow these steps to manage mail names:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you need to work with. The *Domain Administration page* appears.
3. Click the **MAIL** button. The *Mail Names Management page* appears. From this page, users can:
    - View the number of mail names (if any) for the given domain listed in **bold**.
    - Create a new mail name.
    - View a list of mail names currently existing under the specified domain. To the left of each domain name on the list are four icons, each representing different mail account types. They are:
        - Mailbox (represented by the "mailbox" icon)
        - Redirect (represented by the "outgoing envelope" icon)
        - Mail Group (represented by the "people" icon)
        - Mail Autoresponder (represented by the “revolving envelope” icon)
    - Click on a specific mail name to access the *Mail Name Properties page* for that given name.
    - Search the mail names list for a certain pattern. It may help you in case you have a great number of mail names in the system and you need to

work with a particular one. To search the list, type the pattern string in the text input field and click **SEARCH**.

- Sort the list by various parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

- Delete mail names. To remove one or more mail names, check the checkboxes in the **Del** column of the mail names list corresponding to the mail names you wish to remove and click **REMOVE SELECTED**. The *Mail Names Removal page* appears. There you will need to either confirm the removal (check the checkbox and click **SUBMIT**) or **CANCEL** it.

4. To create a new mail name, click in the field provided and enter the desired name. Click **ADD** to submit this name. This will immediately take you to the *Mail Name Properties page*, where you can adjust the Mail Name properties.

5. The new Mail Name will appear on the Mail Names list.

NOTE: The four icons to the left of each mail name are faded (or grayed out) when they are not active. They appear in color when they are active. To change the status of these settings, the user must click on a given mail name, and adjust the settings on the *Mail Name Properties Page* to enable any of the features.

Mail Name Properties Page

This page gives the user the ability to activate any combination of POP3 Mail, Mail Redirects, Mail Groups, and Mail Autoresponders for a given mail name. To edit the mail name:

1. Access the Domain Management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you need to work with. The *Domain Administration page* appears.

3. Click the **MAIL** button. The *Mail Names page* appears.

4. The number of mail names for the given domain is listed at the top of the screen.

5. In the mail users list, click on the name you wish to edit.

6. This will take you to the *Mail Name Properties page.*

7. The **Mail Name** text box is listed at the top of the page. By clicking in this text box, changing the mail name and clicking **UPDATE**. You can change the mail name from this screen.

8. From this page, you can also enable and set up:

- Mailbox Accounts and quotas
- Mail Redirects
- Mail Groups
- Mail Autoresponders

9. When you are done editing mail name properties, click **UP LEVEL** to return to the *Mail Names page*.

Managing Mailbox Accounts

Using this function, you can set up a mailbox account and password for a given mail name. This account will be accessible using either POP3 or IMAP protocols.

NOTE: To limit the number of mailboxes a client can have for a given account, you must access the *Preferences page* from the *Domain Administration page*.

In order to enable and set a password for a given mailbox, from the *Mail Name Properties* page, follow these steps:

1. To enable a mailbox, click in the checkbox provided next to **Mailbox**.
2. When you enable a mailbox for a particular mail account for the first time, you must enter a password.
    - The **Old Password** will say "NONE" if you have yet to enter a password. Once entered, the password cannot be viewed from this screen.
    - To enter a password, click in the **New Password** field and enter the selected password.
    - To properly update the password, you must re-enter the password in the **Confirm Password** field.
    - To set up the mailbox quota, select the **Default for domain** radio button to set the limit to the maximum available in the given domain, or select **Enter size** and enter the quota you wish to set, in KiloBytes, for the given mailbox. Note that this limit may not exceed the default set for the domain.
    - Once you have enabled the mailbox, entered the passwords, and set the mailbox quota, click **UPDATE** to submit.
    - In the event that you need to change a password, simply re-enter the new password in the **New Password** field. Then re-enter the password in the **Confirm** field, and click **UPDATE**.

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

Managing Mail Redirects

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

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

NOTE: To limit the number of redirects a client can use, you must access the *Preferences page* from the *Domain Administration page*.

In order to enable and set a redirect for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. To enable redirects for the account, click in the checkbox provided next to **Redirects**.
2. In the text box to the right, enter the appropriate address that you wish mail for this mail name to be forwarded to.
3. To change the redirect address for a given mail name, click on the existing entry in the **Redirects** box, and edit it to the new address.
4. Click **UPDATE** to execute the changes.

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

Managing Mail Groups

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

NOTE: To limit the number of mail groups a client can use, you must access the

Preferences page from the *Domain Administration page*.

In order to enable and set up a mail group for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. To enable mail groups for a mail name account, click in the checkbox provided next to **Mail Groups**.
2. To create a new mail group, after checking the box, click **ADD**.
3. The **Add Mail Groups** box appears.

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

4. To add an external mail address to a Mail Group, fill in the correct address in the **enter external recipient mail** text box, and click **ADD**.
5. To add an existing account from the same domain, click on the desired address in the **Select registered users** list, and click **ADD**.
6. The selected addresses will appear in the box to the right of the mail groups checkbox on the *Mail Name Properties page*.
7. To delete one or more group members, highlight the selected group member in the box to the left of the mail group check box. Click the **REMOVE** button.
8. A warning will appear. Click **OK** to confirm that you want to delete the address from the mail group.
9. After completing your changes, click **UPDATE** to submit all changes.

NOTE: Once enabled, the mail groups icon on the *Mail Names page* appears in color.

Managing Mail Autoresponders

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

In order to enable and set up a mail autoresponder for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. To enable autoresponders for a mail name account, click in the checkbox provided next to **Mail autoresponders.** When the check appears, autoresponders are enabled for the mail name. If you click again, it will uncheck the box, and autoresponders will be disabled.

2. For the Autoresponder feature you have the option to include file attachments. To include a file to be selectable within the set up of autoresponders for the given mail name, use the **Browse** button to search for and select the desired file(s). (File sizes should be limited to no more than 1MB.)

3. Click the **SEND FILE** button. The attachments will then appear in the **Repository.**

4. These files will be available for any autoresponders that are set up for the given mail name. To delete one or more files highlight the desired file(s) and click the **REMOVE** button. A warning will appear prior to deleting the selected file(s).

5. To add a new mail autoresponder, click the **ADD** button.

6. A pop-up screen prompts you to enter a name for the autoresponder. Enter the desired identification name, and click **OK** to submit.

7. The *Edit Mail Autoresponder page* appears.

    - The selected autoresponder name is listed for the given mail name account. You can click in the text box where the autoresponder name is listed, and edit the name. Click **UPDATE** to submit.

    - The ON/OFF status for the autoresponder is shown. **[ON]** indicates that the autoresponder is on. **[X]** indicates that the autoresponder is off. You can adjust this setting by clicking the **ON/OFF** button. This status icon also appears on the autoresponders list on the *Mail Names Properties page.*

    - Beneath the Request text input box, you can determine whether an autoresponder responds to specific text found within either the subject line or body of the incoming email, or if it responds to ALL incoming requests.

    - To set up the autoresponder to always respond, regardless of the contained text, click the bottom radio button for **always respond**.

    - Using the **Request text** input box and radio buttons, you can set up the autoresponder to send an auto response when an incoming request contains defined text in its subject line or body.

    - Click the **in the subject** radio button to respond to specific text in the subject of the request, or click the **in the body** radio button to respond to specific text in the body of the request.

    - You can select a specific subject to appear in your autoresponder using the **Answer with subject** optoin. To simply respond with the same subject as was

received from the incoming request select the radio button for the default setting. To specify a specific subject line select the radio button beside the text box and enter the desired text.

- You can enter text to be included in the autoresponder in the **Answer text** field.

- Using the **ADD** and **REMOVE** buttons, you can attach files to be included in the autoresponder. These files must be uploaded into the **Repository** on the *Mail Names Properties page*. Select the uploaded file from the **Attach files** list, and use the **ADD** button to attach the file to the autoresponder. Click **REMOVE** to remove a file.

- You can specify the frequency at which the autoresponder responds to the same unique address, after receiving multiple emails from it. By clicking in the appropriate radio button next to **Reply To Unique Email Address**, you can set the autoresponder to **always** respond, to respond **once**, or to respond once per a specified number of **days**. The default setting is to respond once in one day to unique mail addresses. It is highly recommended that you leave this setting, or set to respond once in a given number of days. Selecting always respond can potentially overload your mail server. If the days value is defined as "0", then the autoresponder will respond each time a request is received.

- You can define the number of unique addresses that the autoresponder will remember. Enter the desired number in the **Store up to:** field.

- This memory enables the system to implement the answer-frequency and respond-once functionality. In the event of extremely high mail volume, to protect server performance, you can limit the address memory of the system database.

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

- Click the **UPDATE** button to submit all changes.

Customize DNS Settings

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

NOTE: Improper set up of DNS results in improper functioning of your web, mail and ftp services.

DNS Settings Page

There are five types of accessible DNS records:

A = Address - This record is used to translate host names to IP addresses.
CNAME = Canonical Name - Used to create additional host names, or aliases, for hosts in a domain.
NS = Name Server - Defines an association between a given domain name and the name servers that store information for that domain. One domain can be associated with any number of name servers.
MX = Mail Exchange - Defines the location of where mail should be delivered for the domain.
PTR = Pointer - Defines the IP address and host name of individual hosts in the domain. Translates IP addresses into host names.

When you first enter this screen, you see the DNS status for the domain, as well as the default DNS settings created for the given domain. PSA will pull the default DNS settings from those set up under the SERVER DNS option.

Changing DNS Settings

In order to change DNS settings, follow these steps:

1. From the Client Home page, click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.

2. Click the **DNS** button to access the *DNS Settings page*.

3. The **DNS Zone Status** icon indicates whether a DNS is turned on or off.

    - If you wish to turn DNS on or off for the domain, select **ON/OFF**.

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

    - If you are running remote DNS, and therefore want to turn DNS off for the domain, you should first create the appropriate **NS** entries for the domain and remove any inappropriate **NS** entries possibly created by the default DNS template created under the SERVER function. At that point, turn DNS off. You see that the name server(s) for the domain remains listed as a link.

    - You can perform a test on these name servers by selecting any of them. Selecting any name server will perform an NSLookup to check for the DNS records for your specific domain on that specific name server. NSLookup is used to verify the A record for the domain, the CNAME record for www, and the MX record to ensure that these basic records are

resolved properly on the remote name server. The results are interpreted and presented through the user interface.

4. In order to add a DNS entry, select the type of record you wish to create and select **ADD**. Each record type has its own different set up. When created DNS entries within a specific DNS zone the name of the zone must be present for all entries. PSA sets the screen up with certain unchangeable fields in order to prevent possible errors within the zone.

    - For an A record you will need to enter the domain name for which you wish to create an A record. If you are simply defining an A record for your main domain, then you leave the available field empty. If you are defining an A record for a name server then you will need to input the appropriate entry for the given name server (ie. ns1). Then, you need to enter the appropriate IP address to which to associate the domain name. Then select **UPDATE** to submit your entry.

    - For an 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 in the appropriate name server name in the field provided. You will need to enter in the complete name (i.e. ns1.mynameserver.com). Then, select **UPDATE** to submit your entry ***For a MX record, you will need to enter the domain for which you are creating the MX record. For the main domain, you would simply leave the available field blank. You will then need to enter your mail exchanger, this is the name of the mail server. If you are running a remote mail server named "**mail.myhostname.com**" then you would simply enter "**mail.myhostname.com**" into the field provided. You will then need to set the priority for the mail exchanger. Select the priority, 10 being the highest and 40 being the lowest, from the drop down list. Keep in mind you also would need to add the appropriate A record, and/or CNAME if applicable for the remote mail server. Select **UPDATE** to submit your entry. NOTE: Use of a remote mail server also requires backend modifications to the 'virtualdomains' and 'rcpthosts' files located in the ../qmail/control/ directory. Locations of the ../qmail/control/ directory may vary, but information on this can be found within the /etc/psa/psa.conf file.For a CNAME record, you will need to first enter the alias domain name for which you wish to create the CNAME record. You then need to enter the domain name within which you want the alias to reside. Any domain name can be entered. It does not need to reside on the same server. Select **UPDATE** to submit your entry.

    - For a PTR record you will first enter the IP address for which you wish to define the pointer. Then enter the appropriate domain name for this IP to be translated to. Select **UPDATE** to submit your entry.

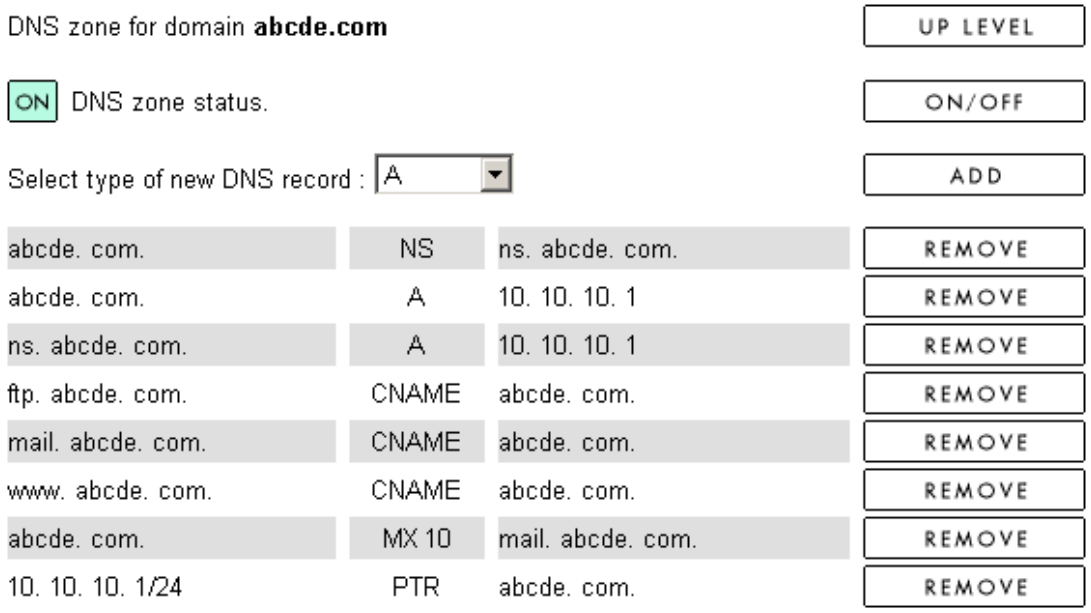
5. You may remove any DNS records by selecting **REMOVE** beside the record you wish to delete. Before anything is processed you will be asked to confirm the deletion.

DNS Example Setups

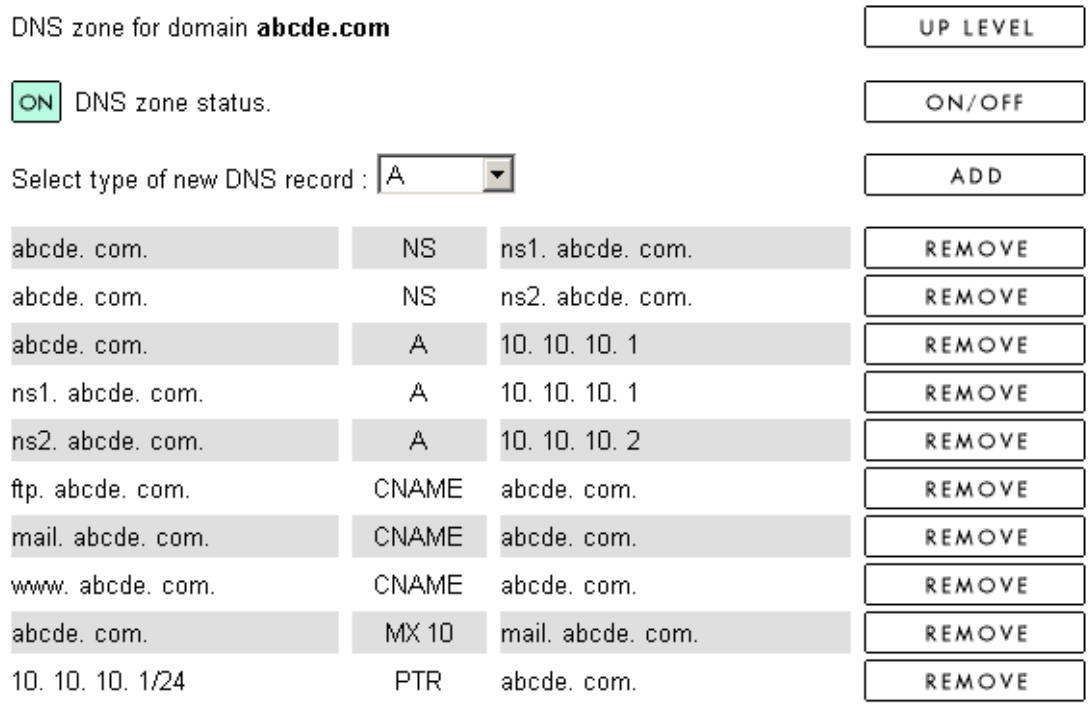
Example 1: A hosting company (we'll use *abcde.com*, which is for example purposes only, and is not intended to represent any existing companies or domains) wishes to setup their PSA enabled server as the primary DNS server for all the domains they create and will run secondary DNS services on an external server (the recommended configuration). The PSA enabled server has an IP address of *10.10.10.1* and the external name server has an IP address of *10.10.10.2*. These addresses will be used for *ns1.abcde.com* and *ns2.abcde.com* respectively. IP address *10.10.10.1* is also the main server IP address that was set up during PSA installation.

NOTE: All name servers need to be properly registered. They need to specifically be registered as name servers with Internic. Also, all domains must be registered with the appropriate name server information.

*The first step in the process is to create the domain *abcde.com* on the server. By default, when a domain is initially created, even before hosting has been configured, PSA sets up a DNS record for the domain. This DNS record is created based on the DNS template that is created by the Admin under the SERVER - DNS option. For the purpose of this example we will use the default setup prior to any modifications made by the Admin under the SERVER –DNS option. With this default setup a properly registered domain will resolve. However the setup does require some modification. The initial assumptions are that the domain is a name-based account and that DNS, Mail and FTP services are to be handled locally. So the resulting default DNS settings for a domain named *abcde.com* are as follows:

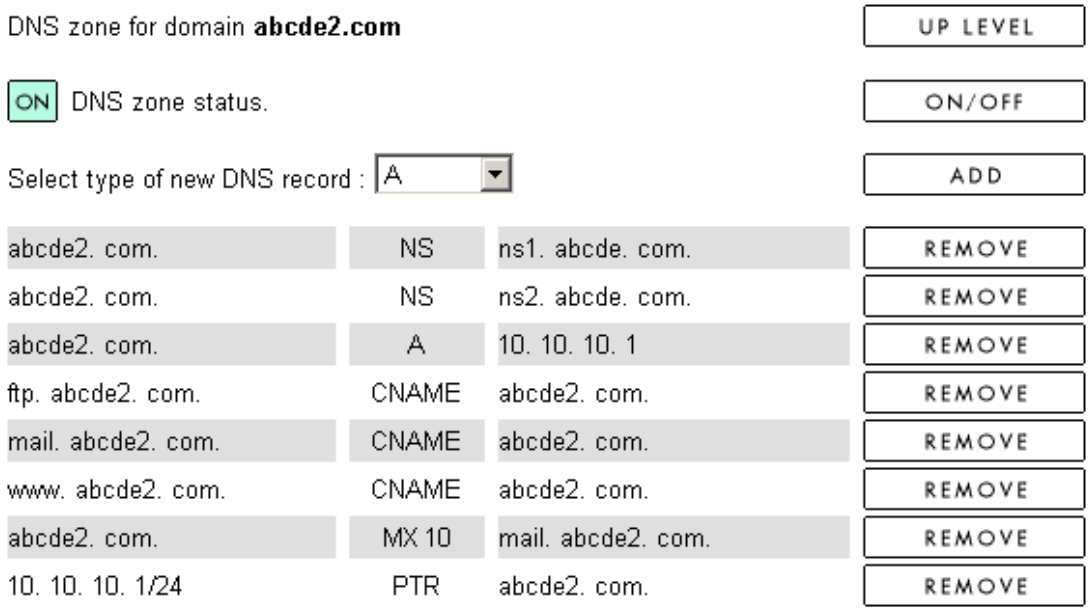


*The next step is to create A records for the name server names you will be using. Every name server name must have a specific IP Address associated with it. Manipulate the DNS records for *abcde.com* to reflect the following. Exact instructions for adding and removing DNS records are described earlier in the section or can be found by selecting HELP within PSA.



No other entries are needed.

From that point on you would only need to change the NS records for each individual domain, such as abcde2.com*, to be *ns1.abcde.com* and *ns2.abcde.com* and then remove the A record that is created for the default name server (*ns.abcde2..com*). The result for a different domain, *abcde2.com*, would be as follows:



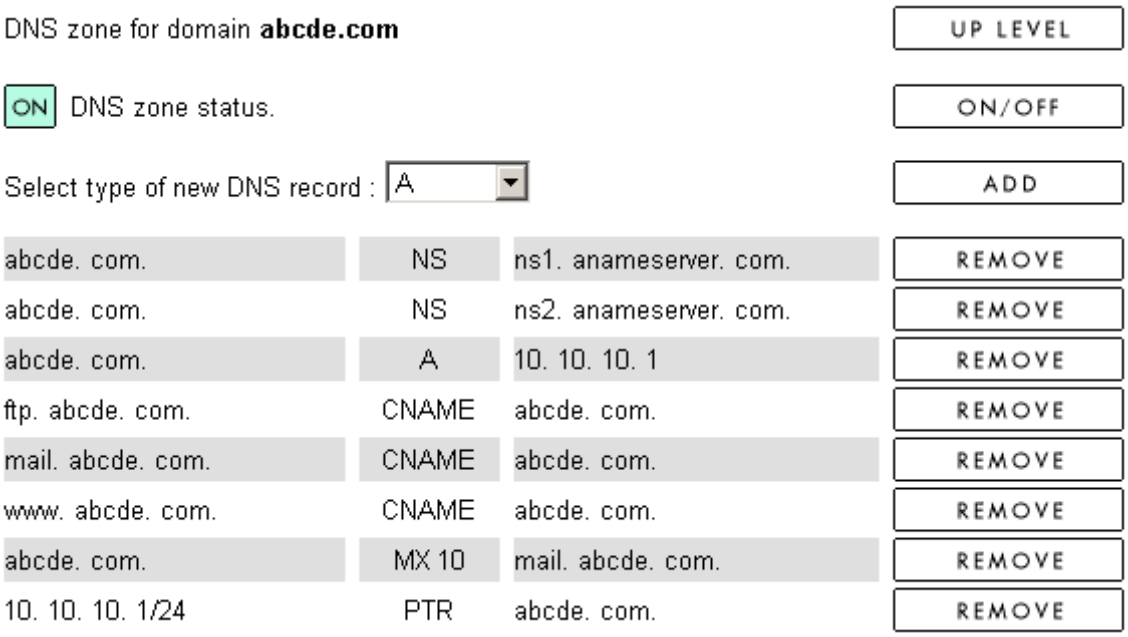
This would be repeated for all the domains created on the server.

NOTE: PSA creates the Primary Zone Files for every domain on the server. It will not create any Slave Zone Files for the secondary DNS. If you plan to setup both primary and secondary name servers locally on your PSA machine it important to understand that you will technically have no Slave Zone Files. For some registrars this can cause rejection of your domain registration request. It is always recommended that secondary DNS services be run on a separate physical server from the primary.

Example 2: A hosting company, *abcde.com*, wishes to run both their primary and secondary DNS services remotely from the PSA enabled server. They have two name servers: *ns1.anameserver.com* and *ns2.anameserver.com*. Their PSA enabled server has the IP-Address of *10.10.10.1*.

NOTE: By default, when a domain is created in PSA, it is assumed that DNS is being resolved locally. In the case described above, *abcde.com* needs to add in the appropriate NS records within each newly created domain and then turn DNS off for that domain.

*The first step is to modify the default PSA DNS settings for the new domain, *abcde.com*, to include the appropriate NS records. The result would be as follows:



*Then select the **ON/OFF** button. PSA will remove the DNS records, however you will still see the records that you had entered as the NS records for the domains. The result would be as follows:

You can then perform a test on these name servers by selecting either of them. Selecting either name server will perform an NSLookup to check for the DNS records for your specific domain on that name server. If there are any errors PSA will report them to you.

Changing Hosting Account Settings

You may have hosting privileges established in your domain so that you can provide various Internet services (e.g. software applications, a forwarding address, and FTP transfers). PSA allows three different types of hosting services, as listed below. To access the hosting settings, follow these steps:

1. Access the Domain Management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you want to work with. The *Domain Administration page* appears.

3. Click the **HOSTING** button. The hosting type page appears. When you provide hosting for a client's domain, PSA offers three types of hosting services:

    - **Physical Hosting** - This is the most common type of hosting service, creating a virtual host (disk space on the local server) for the client. The client controls and publishes his own website without having to purchase a server and dedicated communication lines.

    - **Standard Forwarding** - With this type of forwarding, all requests to the domain are forwarded by your server to another Internet address (no virtual server is created). When an end user searches the Internet for the client's domain, he is routed to another URL, and the address in his browser window changes to the new URL. This may be confusing to the end user.

    - **Frame Forwarding** - All requests to this domain are forwarded to another Internet address (no virtual server is created). But with this type of forwarding, the end user sees the client's domain name in his browser, not the forwarding address. PSA uses frames to "trick" the browser into displaying the correct domain name. The problem with this type of forwarding is that some search engines do not index these frame pages and some browsers do not support frames.

    Click the radio button for the hosting service you wish to define.

4. Click **NEXT** to configure the hosting service. Depending upon the type of service chosen, a customized hosting configuration page appears.

NOTE: If you edit the domain's hosting services and choose a different type of hosting, PSA warns you that all current settings will be lost. You can either proceed or keep the present settings.

You can also delete all the domain’s hosting data – forwarding links (for forwarding type of hosting), web users, databases, protected directories, etc. (for physical type of hosting) – by clicking the **DELETE** button. You will be asked to confirm deletion of the hosting information.

Physical Hosting Configuration

There are several settings to configure for physical hosting. It is helpful to use the TAB key to move between fields when configuring your account.

1. You access this page from the *Hosting Type page* when you select Physical Hosting. Use this page to set up or modify a physical hosting account.

2. Depending on the limits set within the given Client’s Preferences, you can create two different types of virtual hosts: name-based or IP-based. The Plesk Server

Administrator (PSA) defaults to the most commonly used type, name-based. If you want to change the host type, click the IP-based choice. Then, select a valid IP address from the drop down list. The list of available IP's will reflect the settings within the given Client's Preferences.

NOTE: You can create additional IP addresses using PSA's IP Aliasing feature found within the **SERVER** section.

3. You must set an FTP login name and password. FTP allows end users to upload and download files from the Internet site to remote PCs. If you want to provide FTP services, click in the FTP login box. Then, enter or edit a login name to be used for accessing FTP file transfer services on the domain.
4. TAB to the **FTP Password** text box and enter or edit the FTP password.
5. TAB to the **Confirm FTP Password**text box and enter the FTP password for confirmation.
6. TAB to the **Traffic limit** text box and enter or edit the number of megabytes available for monthly transfers. If the traffic limitation is exceeded, the domain's status will change to [!].
7. The **Delete Apache Log Files** text box allows you to decide whether or not you would like the Apache log files to be deleted automatically, if at all. The default setting will say NEVER, indicating that no automated deletion will occur. If you prefer to enable the deletion function, click on the drop-down arrow; then, you can choose between the WEEKLY and MONTHLY deletion frequencies.
8. TAB to the **FrontPage Support** check box to install FrontPage server extensions into the domain. FrontPage is Microsoft's Web publishing tool. It is one of the most commonly used tools for creating a client's website. FrontPage includes several extensions that provide special functionality. If you want this domain to support these extensions, be sure that a check mark appears in the FrontPage box.
9. TAB to the **Authorization ENABLED** choice. You can authorize or disable remote editing of the website using FrontPage. If you are supporting FrontPage, you should disable authorization for additional security. This setting is changeable by the Admin, Client, and Domain User logins to the control panel. For security purposes the main server administrator should notify their Clients and Domain Users that FrontPage authorization should be disabled whenever not in use. To activate FrontPage authorization, make sure this choice is selected. If you want to turn off FrontPage authorization, select the **Authorization DISABLED** choice.
10. If FrontPage support is selected, then the **FP Admin Login,FP Admin Password**, and **Confirm Password** fields must be entered. This login and password will be used to login to the domain when FrontPage is being used. Click in each box and enter the desired Login and Password.

NOTE: For security reasons, the FrontPage admin password will be hidden after initial creation.

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

12. TAB to the **PHP support** check box. PHP is a server-based HTML embedded scripting language used to create dynamic Web pages. If your client wants to support PHP scripting in HTML documents, make sure a check mark appears in the PHP box.

13. TAB to the **CGI support** check box. CGI is a set of rules that describes how a web server communicates with another piece of software on the same machine, and how the other piece of software (based on the CGI program) communicates back to the web server. If your client wants to support CGI, make sure a check mark appears in the CGI box.

14. TAB to the **mod_perl support** check box. Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use it for a vast number of automation tasks. Many CGI programs are written in Perl. If your client wants to support Perl, make sure a check mark appears in the mod_perl box.

15. TAB to the Apache ASP support checkbox. Apache::ASP allows for the use of Active Server Pages utilizing with Perl scripting only. It enables the development of dynamic web applications with session management and embedded perl code.

16. TAB to the **SSL support** check box. SSL certificates provide additional security for Web sessions. SSL certificates are often used for e-commerce applications and other private or confidential applications. Enabling SSL creates an **httpsdocs** directory in the FTP account, and provides https protocol; as a result, users access the domain with the command **https://newdomain.com**. If you want to grant permission to your client to implement an SSL certificate, make sure a check mark appears in the SSL box.

17. TAB to the **Web statistic** check box. Activation of web statistics will result in the installation of a graphical statistics package for the domain. This package is accessible via the PSA interface within the given domain's **Report** page or via the internet using the URL http://<domainname>/webstat.

18. TAB to the **Apache ErrorDocs** checkbox. Selecting this option will place the domain's error documents into a location that is accessible via FTP allowing users to customize their own Apache error documents.

19. When you are satisfied that you have fully defined the hosting services for this domain, click **UPDATE** to return to the *Domain Administration page*.

NOTE: If you want a different hosting type other than physical hosting, then click **BACK** to return to the *hosting type page*.

NOTE: If you do not want to save these physical hosting parameters, click **UP LEVEL** to delete any entries made on the page, and return to the *Domain Administration page.*

Standard Forwarding Configuration

Configuring a standard forwarding service is easy, it requires only one setting:

1. You access this page when you create **HOSTING** services on a domain using standard forwarding. Use this page to set up or modify the hosting account.
2. Click in the **Destination URL** text box and enter or edit a URL address. Users will be redirected to this address when they access your client's domain on the web. The URL change will be visible in the browser.
3. Click **UPDATE** to return to the *Domain Administration page*.

NOTE: If you want a different hosting type other than standard forwarding, click **BACK** to return to the *hosting type page*.

NOTE: If you do not want to save these hosting parameters, click **UP LEVEL** to delete entries made on this page and return to the *Domain Administration page*.

Frame Forwarding Configuration

For frame forwarding, you only need to configure one setting.

1. You access this page when you create **HOSTING** services on a domain with frame forwarding. Use this page to set up or modify the hosting account.
2. Click in the **Destination URL** text box and enter or edit a URL address. Users will be redirected to this address when they access your client's domain on the web. The URL change will not be visible in the browser.
3. Click **UPDATE** to return to the *Domain Administration page*.

NOTE: If you want a different hosting type other than frame forwarding, click **BACK** to return to the *hosting type page*.

NOTE: If you do not want to save these hosting parameters, click **UP LEVEL** to delete entries made on the page and return to the *Domain Administration page*.

Web User Management

A web user is a user account within Apache. It is used to define locations for personalized web pages with individual FTP access. The result of creating a web user is a subdirectory within your domain (e.g. domain.com/~webuser).

A list of all of the web users within a given domain will appear on the main *Web Users page*. At this page you can:

- Select any web user name to edit the web user password and/or to add or remove different scripting options (provided the **Allow scripting for web users** option has been activated at the *Domain Preferences page*).
- Search the web users' list for a certain pattern. It may help you in case you have a great number of web users in the system and you need to work with a particular one. To search the list, type the pattern string in the text input field and click **SEARCH**.
- Sort the list by various parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

To create a new web user:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you want to work with. The *Domain Administration page* appears.
3. Click the **WEB USERS** button. The *Web Users page* appears.
4. On the top of the screen, the number of web users displays for the selected domain.
5. To add a web user, enter the name of the new web user in the text box provided next to **Web user name** and click **ADD**.
6. You are taken to the *Web User Configuration Page* , where you must enter and confirm the password for your new web user and select from the available scripting options for the given domain (availability of scripting options is set in the Domain Preferences). To do this, enter a password in the **New Password** text box, and then re-enter it in the **Confirm Password** text box. Then select from the available scripting options if applicable. Once you have completed all entries click on **UPDATE** to enter the information. Selecting **UP LEVEL** will return you to the *Web Users page* without assigning a password or scripting capabilities to the given web user. Although the directory will be create, it will not be accessible via FTP using the web user name.

7. As you create web users, the user names appear on the Web Users page in the web user list.

8. To change web user passwords or edit scripting options, click on the user name in the web user list. This takes you to the *Web User Configuration Page*. Follow the same procedure as taken in Step 6.

9. To delete existing web users select the users that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the web users.

10. When you are done, click **UP LEVEL** to return to the *Domain Administration page*.

To remove one or more web users, check the checkboxes in the **Del** column of the web users' list corresponding to the web users you wish to remove and click **REMOVE SELECTED**. The *Domain Removal page* appears. There you will need to either confirm the removal (check the checkbox and click **SUBMIT**) or **CANCEL** it.

Important Notes on web users:

- For security purposes, the password must be between 5 and 14 characters and cannot contain the user name.
- Each web user creates a system account within Apache; therefore, you cannot have two web users with identical names on the same server.
- New web users can access the directory using FTP software by entering the domain name under which the web user account was created and using the appropriate web user name and password.

Protected Directories

This feature is active if virtual hosting has been configured for the domain. It creates and provides password-protected access to the directories where the secure documents reside in the virtual domain. It is possible to create directories under either the standard virtual host accessible via http protocol, or if applicable for the given domain, under the SSL virtual host accessible via https protocol (to enable SSL, check the **SSL support** checkbox at the *Hosting Configuration page* for the given domain). Icons are used next to each directory name in the directory list to define which virtual host type (SSL or non-SSL) the directory resides within. An open lock depicts non-SSL; a closed lock depicts SSL.

NOTE: We strongly recommend that you create and change directories through the Plesk Server Administrator software and not within the FTP program. PSA may not recognize manual changes.

Creating a Protected Directory

Follow these steps to create secure directories for the domain:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you want to work with. The *Domain Administration page* appears.

3. Click the **DIRECTORIES** button. The *Protected Directory List page* appears. The top of the page states how many protected directories there are for a given domain.

4. To create a new protected directory select ADD.

5. This takes you to the *Protected Directory Control page*. Enter the name of the protected directory you wish to create in the **Protected Directory** field provided. .

6. For **Directory Location:** you can choose either a non-SSL or SSL secure directory. To choose a non-SSL directory, click in the radio button next to **Non-SSL**. To choose SSL security for the directory, click in the radio button next to **SSL**.

7. If the directory has SSL enabled, it will appear in the Protected Directory list with a blue **Lock** icon beside it. If the directory is non-SSL, a gold **Unlocked** icon will appear next to the directory name in the directory list.

8. Click in the **Header Text** text box. When a user tries to access the protected directory, the text in this box displays as the Realm they are entering. In this text box, enter the header text.

9. To add a new user, under **Protected Directory Users** click in the **New User:** text box**,** and write the name of the directory user.

10. Click the **ADD** button.

11. You are taken to the directory user password screen. Here you must enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box.

12. Click the **UPDATE** button to submit. You will return to the *Protected Directory Control page*. The new user will appear in the Protected Directory Users list. Clicking **UP LEVEL** will return to the *Protected Directory Control page* without creating a password for the given user. Although the user is created no access to the directory will be granted until a password is created for the user.

13. To remove existing directory users select the users that you wish to remove using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the directory users.

14. To access a directory user in order to edit the user password, click on the user name in the list, and you will again be taken to the directory user password screen. Enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box.

15. Select **UPDATE** to submit your changes and return to the *Protected Directory Control page.*

16. Once you have completed everything within your new protected directory Click **UPDATE** to complete all changes to the system and to return to the *Protected Directory List page*.

Changing a Protected Directory

You can edit a protected directory definition to:

- Add a user
- Change a password
- Delete a user
- Change header text
- Change the SSL status

Follow these steps to edit protected directories:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you want to work with. The *Domain Administration page* appears.
3. Click the **DIRECTORIES** button. The *Protected Directory List page* appears.
4. Click on any directory from the list that you wish to change.
5. You will be taken to the *Protected Directory Control page.*
6. From here, you can edit the directory by following the same steps outlined above, in the **Creating a Protected Directory** section.
7. Click **UPDATE** to complete all changes to the system and to return to the *Protected Directory List page*.

Searching the Protected Directories List

PSA allows you to search the Protected Directory List for a certain pattern. It may help you in case you have a great number of directories in the system and you need to work with a particular one. To search in the list:

1. Select the input field and type in the pattern string.
2. Click the **SEARCH** button.
3. If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Protected Directory List.
4. If no matches were found it will be so stated.
5. The button **SHOW ALL** will revert to displaying the whole list of domains.

There is also another way to ease the process of working with a large list of directories. An option of sorting the list by several various parameters is made available to you. You can sort the list by several parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Removing a Protected Directory

To remove one or more directories, follow these steps:

1. Check the checkboxes in the **Del** column of the Protected Directories List corresponding to the directories you wish to remove.
2. Click on **REMOVE SELECTED**. The *Protected Directory Removal page* appears.
3. For every directory you chose to remove the name of the directory and the names of this directory users will be displayed.
4. If you are certain that the displayed information is correct and wish to proceed with deleting, check the "Yes, I have read, understood, and agree to remove protect from these domains" checkbox. Then click **SUBMIT**. If you decide to not delete these directories or wish to modify the list of directories chosen for deletion, click the **CANCEL** button.

Both buttons will return you to the *Protected Directory Management page*, one committing the changes, the other one leaving everything unchanged.

NOTE: Removing a protected directory in PSA does not delete the directory off the server. It simply takes the protected status off the directory. Meaning that the directory and its contents will now be reachable via the Internet without the need for login and password.

SSL Certificate Management

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

Important Notes on Certificates:

- In order to use SSL certificates for a given domain, the domain MUST be set-up for IP-Based hosting.
- When an IP-based hosting account is created with SSL support, a default SSL certificate is uploaded automatically. However, this certificate will not be recognized by a browser as one that is signed by a certificate signing authority.
- The default SSL certificate can be replaced by either a self-signed certificate or one signed by a recognized certificate-signing authority. The self-signed certificate is valid and secure, but many clients prefer to have a certificate signed by a known Certificate Signing Authority.
- You can acquire SSL certificates from various sources. You can purchase a certificate directly through your control panel interface through the Buy Certs option; using our services web-site My.Plesk.com (MPC). Also, you can generate a certificate with the SSLeay utility and submit it to any valid certificate authority. This can be done using the CSR option within PSA.
- If using a SSL certificate issued by a certificate authority other than Thawte or Verisign, a rootchain certificate is required to appropriately identify and authenticate the certificate authority that has issued your SSL certificate.
- If the given domain has the **www** prefix enabled, you must set-up your CSR or self-signed certificate with the **www** prefix included. If you do not, you will receive a warning message when trying to access the domain with the **www** prefix.
- Remember to enter your certificate information in PEM format. PEM format means that the RSA Private Key text must be followed by the Certificate text.
- All certificates are located in the ../vhosts/<domain name>/cert/httpsd.pem file. Where this directory reads <domain name> , you must enter the domain name for which the certificate was created.

Generate a Self-signed Certificate or Certificate Signing Request

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you want to work with. The *Domain Administration page* appears.

3. If you have established an IP based hosting account with SSL support, the **CERTIFICATE** button will be enabled.

4. Click the **CERTIFICATE** button. The *SSL certificate setup page* appears.

5. The **Certificate Information:** section lists information needed for a certificate signing request, or a self-signed certificate. You must fill out these fields before generating your CSR or self-signed certificate.

6. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop down box next to **Bits:.**

7. To enter the information into the provided text input fields (**State or Province**, **Locality**, **Organization Name** and **Organization Unit Name** (optional)) click in the text boxes and enter the appropriate name.

8. To enter the Domain Name for the certificate, click in the text box next to **Domain Name:** and enter the appropriate domain.

9. The domain name is a required field. This will be the only domain name that can be used to access the Control Panel without receiving a certificate warning in the browser. The expected format is www.domainname.com or domainname.com.

10. Click on either the **SELF-SIGNED** or **REQUEST** button.

11. Clicking **SELF-SIGNED** results in your certificate being automatically generated and installed.

12. Selecting **REQUEST** results in the sending of a certificate-signing request (CSR) to the email address you provided in the certificate fields discussed above. When a CSR (certificate signing request) is generated there are two different text sections, the RSA Private Key and the Certificate Request. **DO NOT LOSE YOUR RSA PRIVATE KEY. YOU WILL NEED THIS DURING THE CERTIFICATE INSTALLATION PROCESS. LOSING IT IS LIKELY TO RESULT IN THE NEED TO PURCHASE ANOTHER CERTIFICATE**

13. When you are satisfied that the SSL certificate has been generated or the SSL certificate request has been correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

Purchase an SSL Certificate

To purchase a certificate through My.Plesk.com (MPC), first complete the steps given in items 1 – 12 of the previous instruction (generating a self-signed certificate or a certificate-signing request) and then proceed to:

1. Click on the **BUY CERTS** button to gain access to the certificate management interface on My.Plesk.com. The *MPC Gate page* appears.

2. This page allows you to create an account (the **CREATE ACCOUNT** button) and access (the **LOG IN** button) MPC from where you are taken through step-by-step instructions on how to purchase and manage your certificate.

3. In case you already have an existing account on MPC but forgot the password for it, there is a button provided especially for such occasions: **FORGET PASSWORD?** Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your user profile.

4. When you are satisfied that the SSL certificate has been generated or the SSL certificate request has been correctly implemented, click **UP LEVEL** to return to the *Domain Administration page.*

NOTE: if you do not wish to purchase certificates at this time but do wish to view the certificates currently owned by you, you may proceed directly to the *MPC Gate page* by clicking the **VIEW CERTS** button. At that you will not be prompted to fill in the details at the *SSL Certificate setup page.*

Upload Existing Certificate w/o Private Key

For instances where a CSR was generated inside PSA the system is designed to save the RSA Private Key for this specific CSR inside of the system database. This feature will allow a user to take the formally signed certificate from the Certificate Authority and upload it to the server without the private key. PSA will find the private key for the given certificate and install it properly on the server in PEM format. To do this operation follow the process below.

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you want to work with. The *Domain Administration page* appears.

3. Click the **CERTIFICATE** button. The *SSL Certificate page* appears.

4. If you wish to upload a Certificate File authorized by the Certificate Signing Authority, click the **BROWSE…** button under the **Upload previously bought Certificate File (without private key)** section to select the file (the file must be in .txt format)

5. Then, click **SEND FILE** to copy the certificate to the server.

Upload a New Certificate w/ Private Key

For certificates purchased using a CSR not generated through the PSA interface it is imperative that you include both the RSA Private Key text block and the Certificate text block in one file before selecting to upload this to the PSA server. To do this operation follow the process below.

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you want to work with. The *Domain Administration page* appears.

3. Click the **CERTIFICATE** button. The *SSL Certificate page* appears.

4. If you wish to upload a certificate file from a local computer, under the **Uploading Certificate File** section, click the **BROWSE…** button to select the file (the file must be in .txt format).

5. Then, click **SEND FILE** to copy the certificate to the server. Or, if you want to type in the text of the certificate without downloading a specific file, click in the text box and enter and paste the certificate information.

6. Click **SEND TEXT** to implement the text on the server.

   NOTE: Ensure that the private key text block is included along with the SSL certificate text block when using the **SEND FILE** or **SEND TEXT** options.

   EXAMPLE FORMAT:

```
-----BEGIN RSA PRIVATE KEY-----

[[ECRYPTED BLOCK OF TEXT]]

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

[[ECRYPTED BLOCK OF TEXT]]

-----END CERTIFICATE-----
```

8. When you download the certificate to the server, PSA checks for errors. If an error is detected, PSA restores the old version of the SSL certificate, and PSA warns you to update the certificate. At this point, you can try again to enter text or to download the certificate file.

9. When you are satisfied that the SSL certificate is correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

Uploading the Rootchain Certificate

If you are using a certificate that has been signed by an authority other than Thawte or Verisign then it is likely that this will require the use of a rootchain, or CA, certificate. To install a rootchain certificate for the domain:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you want to work with. The *Domain Administration page* appears.
3. Click the **CERTIFICATE** button. The *SSL Certificate setup page* appears.
4. The icon next to **Use rootchain certificate for this domain** appears on this page.
5. If the icon is **[ON]** then the rootchain certificate will be enabled for this domain. If the icon is **[X]** this function will be disabled.
6. To change the status of the rootchain certificate, click the **ON/OFF** button.
7. To upload your rootchain certificate, first make sure that it has been saved on your local machine or network. Use the **Browse** button to search for and select the appropriate rootchain certificate file.
8. Then click the **SEND FILE** button. This will upload your rootchain certificate to the server to assure proper authentication of the certificate authority.
9. When you are satisfied that the rootchain certificate is correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

Anonymous FTP

Within PSA the Administrator, or Client given domain creation capabilities, can setup Anonymous FTP capabilities for a given IP-based virtual host. Anonymous FTP is used to allow an open, yet controlled, environment for visitors to the domain to download and/or upload files to and from the domain account. Users will be able to log into ftp.<domain name> with the standard anonymous user name and any password. PSA allows the setup and limitation of incoming file space, connected users, and bandwidth usage throttling. Administrators should take care when allowing the use of anonymous FTP and be sure to use all the limitation capabilities within the interface wisely. If setup with excessive limits, it could lead to problems with server resources as well as excessive bandwidth usage.

To set up Anonymous FTP:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you want to work with. The *Domain Administration page* appears.
3. Click the **ANONYMOUS FTP** button. The *Anonymous FTP Feature Management page* appears.
4. By default anonymous FTP capabilities will be inactive. To activate anonymous FTP select the **ON/OFF** button. The status indicator next to **Anonymous FTP account status** will identify the status as either ON or X (off).
5. Select the checkbox beside **Allow uploading to incoming directory** to allow visitors access the anonymous ftp site to upload files into the /incoming directory.
6. Select the checkbox beside **Limit disk space in the incoming directory** to set the disk space quota (i.e. hard limit) on the /incoming directory. Then select the **Up to** field and enter the disk space, in KiloBytes, you wish to allow for the /incoming directory. If no specific limit is set, or zero is used in the **Up to** field, the setting is unlimited.
7. Select the checkbox beside **Limit maximum simultaneous connections number** to set limits on the number of users who can be simultaneously connected to the anonymous FTP site. Then select the **Up to** field and enter the number of connections allowed. If no specific limit is set, or zero is used in the **Up to** field, the setting is unlimited.
8. Select the checkbox beside **Limit download bandwidth for this virtual FTP domain** to set throttling up for the anonymous FTP site. Then select the **Up to** field and enter the maximum average bandwidth, in KiloBytes per second, allowed. If no specific limit is set, or zero is used in the **Up to** field, the setting is unlimited.
9. Once you have completed all changes, select **UPDATE** to submit all changes and return to the *Domain Administration page*.
10. Selecting **UP LEVEL** will ignore all changes made and return to the *Domain Administration page*.

Database Management

Within PSA there is the ability to create multiple mysql databases as well as multiple users within each database. Also, directly accessible via PSA, is a link to PhpMyAdmin, a PHP interface that abstracts mysql into a web-based administration tool, allowing you to sort, edit, and create tables within a given database. Database limits are set through

domain preferences and database disk usage is calculated within the domain's total allotted disk space.

Searching the Database List

PSA allows you to search the Database List for a certain pattern. It may help you in case you have a great number of databases in the system and you need to work with a particular one. To search in the Database List:

1. Select the input field and type in the pattern string.
2. Click the **SEARCH** button.
3. If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Database List.
4. If no matches were found it will be so stated.
5. The button **SHOW ALL** will revert to displaying the whole list of databases.

There is also another way to ease the process of working with a large list of databases. An option of sorting the list by several various parameters is made available to you. You can sort the Database List by **Type** and **Database Name**. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Creating a New Database

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you want to work with. The *Domain Administration page* appears.
3. Click the **DATABASES** button. The *Databases Feature Management page* appears.
4. To add a new database select the **Database name** field, enter the desired name, and select **ADD**. The *Database Editing page* appears.
5. To add database users to the newly created database enter the user name into **New user** text box and select **ADD**. The *Database User Management page* appears.
6. Enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the new user. Selecting **UP LEVEL** will ignore all entries and return to the *Database Editing page* making no changes.

7. Once you have completed the creation of the new database and its users select **UP LEVEL** to return to the *Database Feature Management page*.

8. To add further databases, follow the steps outlined in 1-7 above. To return to the *Domain Administration page* select **UP LEVEL**.

Editing an Existing Database

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.

2. Click the domain name that you want to work with. The *Domain Administration page* appears.

3. Click the **DATABASES** button. The *Databases Feature Management page* appears.

4. Click on the database that you wish to edit. The *Database Editing page* appears.

5. To add database users to the selected database enter the user name into **New user** text box and select **ADD**. The *Database User Management page* appears.

6. Enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the new user. Selecting **UP LEVEL** will ignore all entries and return to the *Database Editing page* making no changes.

7. To edit the password of an existing database user, select the user from the database user list. The *Database User Management page* appears.

8. To delete existing database users select the users that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the selected users.

9. To access and/or edit database content you can do so using the **PHPMYADMIN** option. PhpMyAdmin provides a web-based graphical interface for mysql. This can be used to make content edits to your existing databases.

10. Once you have completed all edits of the database and its users select **UP LEVEL** to return to the *Database Feature Management page*.

11. To delete existing databases select the databases that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the selected databases.

12. To edit further databases, follow the steps outlined in 1-11 above. To return to the *Domain Administration page* select **UP LEVEL**.

Domain User

The domain user setup provides entry to the PSA control panel within a single domain. Domain users have the ability to administer mail accounts, web users, databases, protected directories, and the domain ssl certificate. Limits to the domain user are set by the Client and/or Administrator using the Domain Preferences.

Access to the control panel for the database user is done using https://<domain name>:8443. The control login will be the domain name, and the password will be whatever is set through the control panel.

To set up the Domain User:

1. Access the domain management function by clicking on the **DOMAINS** button at the top of the PSA interface. The *Domain List page* appears.
2. Click the domain name that you want to work with. The *Domain Administration page* appears.
3. Click the **DOMAIN USER** button. The *Domain User Properties* page appears.
4. To allow access to the control panel for the database user select the checkbox for **Allow domain user access**.
5. Enter the password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the domain user and return to the *Domain Administration page.*
6. Selecting **UP LEVEL** will ignore any changes and return to the *Domain Administration page*.

4. Client-Level Administration

- 4.1 Introduction to Client Usage
- 4.2 The Client Home Page
    - Domain List
    - Searching the Domain List
    - Editing your Client Record
    - View Account Status Report
    - Viewing and Editing Preferences for the account
    - Create a New Domain
    - Registering and Managing the Domain via MPC.
    - Additional Services (Extras)
- 4.3 Domain Administration Page
    - Turning a Domain On or Off
    - Access the Domain Preferences
    - Accessing the Domain Report
    - Managing Mail
        - Mail Names page
        - Manage Mail Name Properties
            - Manage Mailbox Accounts
            - Manage Mail Redirects
            - Manage Mail Groups
            - Manage Mail Autoresponders
    - Customize DNS Settings
        - DNS Settings Page
        - Changing DNS Settings
        - DNS Example Setups

- Changing Hosting Settings
    - Physical Hosting Configuration
    - Forwarding Configuration
- Web Users Management
- Protected Directories
    - Creating a Protected Directory
    - Changing a Protected Directory
    - Searching the Protected Directories List
    - Removing a Protected Directory
- Manage the Domain SSL Certificate Management
    - Generate a Self-signed Certificate or Certificate Signing Request
    - Purchase an SSL Certificate
    - Upload Existing Certificate w/o Private Key
    - Upload a New Certificate w/ Private Key
    - Uploading the Rootchain Certificate
- Anonymous FTP
- Databases
    - Searching the Database List
    - Creating a New Database
    - Editing an Existing Database
- Domain User

4.1 Introduction to Client Usage

As a client (or an end user) on a Plesk server, you can remotely administer your account. With PSA, you no longer need to depend on your Internet provider's system administrator to manage tasks such as adding email accounts, changing domain parameters or obtaining an SSL certificate; you can do it all via PSA's graphical user interface. PSA is user-friendly. You do not have to know operating system commands or complex programming

languages to take full advantage of the product; rather you only need to know how to navigate using a mouse and standard Internet browser. By accessing the PSA through your web browser (Netscape 4.x+ or Microsoft Internet Explorer 4.x+), you can:

- View and change your client record
- Change your login password
- Reconfigure your domain
- Change your hosting settings
- Create CSR's or self-signed certificates and/or install SSL certificates (IP-based hosting only)
- Create email boxes, redirects, groups and autoresponders
- Create web users
- Create protected directories
- View status statistics relating to your disk space and traffic

PSA warns you of any consequences before allowing you to execute a major change.

4.2 The Client Home Page

When you log in, the *Client Home page* appears. From here, you can:

- View the Domain List
- Search the Domain List
- Edit your client record
- View a status report
- Viewing and Editing Preferences for the account
- Create new domains
- Register and manage domains via MPC
- Utilize Additional Services (Extras)
- Access and manage your domains
- Log out of PSA

Domain List

The domain list on this page displays all domains belonging to you. To the left of each domain name are three icons that indicate domain status. These icons appear as such:

[OK][ON][ON]

The first status icon indicates the status of the domain:

[OK] if the domain is operated within the disk space and traffic limitations.
[!] if the domain has exceeded disk space or traffic limitations. The PSA system evaluates disk space and traffic every 24 hours.

The second icon indicates whether the domain has been turned **ON** or **OFF** by the Administrator:

[ON] means that the domain is activated.
[X] means that this domain is presently turned off and presently deactivated or inaccessible. If the domain is turned **OFF**, no service will be rendered to the given domain.

The third icon indicates whether the domain has been turned **ON** or **OFF** by the client:

[ON] means that the domain is activated.
[X] means that this domain is presently turned off and presently deactivated or inaccessible. If the domain is turned **OFF**, no service will be rendered to the given domain.

When a new domain is created, a corresponding new entry is added to the Domain List. The Domain List also allows you to remove domains from the system. To remove one or more domains, follow these steps:

1. Check the checkboxes in the **Del** column of the Domain List corresponding to the domains you wish to remove.
2. Click on **REMOVE SELECTED**. The *Domain Removal page* appears.
3. For every domain you chose to remove the Domain Name will be displayed.
4. If you are certain that the displayed information is correct and wish to proceed with deleting, check the “Yes, I have read, understood, and agree to remove these domains” checkbox. Then click **SUBMIT**. If you decide to not delete these domains or wish to modify the list of domains chosen for deletion, click the **CANCEL** button.

5. Both buttons will return you to the *Client Home page*, one committing the changes, the other one leaving everything unchanged.

Searching the Domain List

PSA allows you to search the Domain List for a certain pattern. It may help you in case you have a great number of domains in the system and you need to work with a particular one. To search in the Domain List:

1. Select the input field and type in the pattern string.
2. Click the **SEARCH** button.
3. If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Domain List.
4. If no matches were found it will be so stated.
5. The button **SHOW ALL** will revert to displaying the whole list of domains.

There is also another way to ease the process of working with a large list of domains. An option of sorting the list by several various parameters is made available to you. You can sort the Domain List by **Problem State**, **Status (Admin)**, **Status (Client)**, **Creation Date** and **Domain Name**. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Editing your Client Record

If your contact information ever changes, you should update your client record.

1. Access the client function by clicking the **EDIT** button on your *Client home page*.
2. Your client record appears.
3. Click in any text box to enter or edit data, or use the TAB key to move from one text box to the next. The **Control Panel password** and **E-mail** are the required fields.
4. When you are satisfied that the information is complete and correct, click **UPDATE**.
5. PSA informs you if you have not entered any of the required information. If the some of it has not been entered, return to the client record and enter it. Click **UPDATE** to save the edited information.

NOTE: You cannot change your Control Panel login name, only your password. To change your login name, you must contact the system administrator at your Internet provider organization.

NOTE: You can leave editing any of the PSA client functions or properties at any time

without saving your work. Click **UP LEVEL** to return to your home page and cancel any edits made.

View Account Status Report

The client report lets you view the status of your account. To access the report:

1. Access your *Client home page*.
2. Click the **REPORT** button. Your client account report appears.
3. To print the report, use your browser's **File/Print** command.
4. To email this status report, enter an email address in the text box and click **SEND AS E-MAIL**.
5. Click **UP LEVEL** to return to the *Client Home page*.

Viewing and Editing Preferences for the account

When a client is added to the PSA system, in order to become a legitimate user this client needs to have the necessary permissions, privileges, quotas and limits set by the administrator. Click the **PREFERENCES** button on the *Client Home page* to access the page with two buttons: **PERMISSIONS** and **LOGO SETUP**.

- The **PERMISSIONS** button takes you to the *Client Permissions page*. This page allows you to view limits and quotas set for your account by the Administrator.
- The **LOGO SETUP** button takes you to the *Client Logo Setup page*. This page allows you to set up the logo preferences for your account.

The list of features subjected to limiting by the Administrator:

- Maximum number of domains the client can have
- Total disk space
- Total amount of traffic
- Maximum number of mailboxes
- Maximum mailbox quota
- Maximum number of redirects
- Maximum amount of mail groups
- Maximum number of autoresponders
- Maximum number of web users the client can create
- Maximum number of databases

To set up or modify the logo preferences, follow these steps:

1. Click the **PREFERENCES** button at the *Client Home page*, and then, when the *Client Preferences page* appears, click **LOGO SETUP**. The *Client Logo Setup page* appears.

2. To submit a logo you must have the desired graphics file on your local machine. Choose the file from your local machine and click on **SEND LOGO**. (*.GIF and *.JPG files only, 558x81 recommended).

3. To submit a link, type the desired URL in the field provided and click on **SEND LINK**.

4. The **DEFAULT LOGO** button will revert to the logo back to the default Server Administrator logo on default language.

5. Click **UP LEVEL** to return to the *Client Preferences page*.

Create a New Domain

From the *Client Home page* you can create new domains, provided the Administrator has enabled you to do that. To create a new domain:

1. Click the **NEW DOMAIN** button at the *Client Home page*.

2. The *Client Domain Creation page* appears with text boxes containing all the necessary client information.

3. To create the new client domain, click in the **New domain name** text box and enter the name.

4. Make sure a check mark appears in the WWW check box if users must include the WWW prefix to access this domain. If WWW is not required (typically because this domain is for local use only), click to clear the WWW check box so that it is unchecked.

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

5. Click **UPDATE** to add the domain to the client's account. Repeat these steps to add additional domains.

   NOTE: You can exit the domain creation function without saving your changes. Click **UP LEVEL** to discard all changes you have made to this record and to revert to the most recent version of the client record.

Registering and Managing the Domain via MPC.

When a new domain is created it must be officially registered. There are a number of Internet services where you can register your domain but there is one that is offered by Plesk Inc.

To register a new domain, follow these steps:

1. Click the **REGISTER** button at the *Client Home page* to access the *MPC Gate page*.
2. From *MPC Gate page* you can access the services provided to you by My.Plesk.com. To do that, enter the **MPC Login** and **MPC Password** into the provided corresponding text input fields and click **LOG IN**.
3. You can check the **Remember account** checkbox to have you login and password remembered by the system. This way the next time you wish to access MPC, you will be taken directly to My.Plesk.com and will not be prompted to enter your login and password.
4. In case you forgot the password, there is a button provided especially for such occasions: **FORGET PASSWORD?** Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your Server Administrator profile.
5. You can return to the *Client Home page* by clicking **UP LEVEL**.

To manage already existing domains, follow these steps:

1. Click the **MANAGE** button at the *Client Home page* to access the *MPC Gate page*.
2. From *MPC Gate page* you can access the services provided to you by My.Plesk.com. To do that, enter the **MPC Login** and **MPC Password** into the provided corresponding text input fields and click **LOG IN**.
3. You can check the **Remember account** checkbox to have you login and password remembered by the system. This way the next time you wish to access MPC, you will be taken directly to My.Plesk.com and will not be prompted to enter your login and password.
4. In case you forgot the password, there is a button provided especially for such occasions: **FORGET PASSWORD?** Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your Server Administrator profile.
5. You can return to the *Client Home page* by clicking **UP LEVEL**.

Additional Services (Extras)

From the *Client Home page* you can access external services (other than registering domains and managing domains registration) provided through My.Plesk.com. To do that, click the **EXTRAS** button.

4.3 Domain Administration Page

A domain is a virtual address on the Internet for any organization or entity. To an Internet user, a domain appears as space on one server, regardless of its implementation. Domains are identified by their familiar Internet URL (uniform resource locator) addresses. Syntactically, a domain name is a string of names or words separated by periods. For example, www.plesk.com is the name of the domain where Plesk's information resides on its servers.

A domain belongs to a client. For example, John Smith may be a programmer whose domain is aceprogrammer.com. In the same respect, the ABCDE, Inc. company may own a domain by the name of abcde.com. The Plesk system administrator at your Internet service provider's organization must create your domain. However, you can remotely administer your domain once the account is established.

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

From the *Domain Administration page,* you can manage several aspects of your domain, including:

- Turn the Domain **ON/OFF**
- Access the Domain Preferences
- Access the Domain Report
- Manage Mail for the Domain
- Customize DNS settings
- Register a Domain
- Set up Hosting
- Create Web Users
- Create Protected Directories
- Manage the Domain SSL Certificate
- Set up Anonymous FTP
- Manage Databases
- Set up the Domain Level Control Panel Login

Turning a Domain On or Off

There are times when you may need to deactivate a domain. You can turn a domain on or off when you are logged on as a client.

The domain status consists of three icons:

[OK][ON][ON]

The first status icon indicates the status of the domain:

[OK] if the domain is operated within the disk space and traffic limitations.
[!] if the domain has exceeded disk space or traffic limitations. The PSA system evaluates disk space and traffic every 24 hours.

The second icon indicates whether the domain has been turned **ON** or **OFF** by the Administrator:

[ON] means that the domain is activated.
[X] means that this domain is presently turned off and presently deactivated or inaccessible. If the domain is turned **OFF**, no service will be rendered to the given domain.

The third icon indicates whether the domain has been turned **ON** or **OFF** by the client:

[ON] means that the domain is activated.
[X] means that this domain is presently turned off and presently deactivated or inaccessible. If the domain is turned **OFF**, no service will be rendered to the given domain.

To turn a domain **On** or **Off**, follow these steps:

1. From the *Client Home page*, click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.
2. Click the **ON/OFF** button to change the domain's status.
3. PSA asks you to confirm that you want to change the status of the domain. Click **OK** to change the status, or **Cancel** to keep the current client status.
4. If you are deactivating a domain, you should inform the domain owner as to why the status has changed.

Access the Domain Preferences

The *Domain Preferences page* displays the preferences that the Plesk administrator has set up for this domain. It also allows you to edit certain parameters.

The parameters available for viewing and editing from at this page are:

- **Disk Space Limit** – the amount of disk space allocated for this domain.
- **Maximum Mailboxes** - the maximum number of mail accounts allowed for creation at this domain.
- **Mailbox quota** – the limit set for the size of the mail accounts (mailboxes).
- **Maximum Mail Redirects** - the maximum number of mail allowed for setting up at this domain.
- **Maximum Mail Groups** - the maximum number of mail groups allowed for creation at this domain.
- **Maximum Autoresponders –** the maximum number of mail autoresponders allowed for setting up at this domain.
- **Maximum Web Users** – the maximum number of web users allowed for creation at this domain.
- **Maximum Databases** – the maximum number of databases allowed for creation at this domain.
- For **Mail sent to non-existent users**, the client is able to select either a mail bounce message to return to the sender, or a catch-all email address to which the messages are sent.
- The **WWW prefix** checkbox determines whether the given domain will require the www prefix in order to be accessed.
- **Allow Scripting for Web Users** – enables the Web Users to download and execute scripts.
- **WebMail** – allows utilizing access to mailboxes via web-interface. If the box is checked, the mailbox can be accessed by means of a web-client , which is made available from the URL: webmail.<domain.name>

To adjust the settings, follow these steps:

1. From the *Client Home page*, click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.
2. Click the **PREFERENCES** button to access the *Domain Preferences page*.
3. To set the value for the desired parameter, click on the **Enter Number** radio button to the right for the parameter. Click in the text input field and enter the value. If the value entered does not satisfy limitations set by the administrator, a warning will be issued upon trying to **UPDATE** the settings.
4. To utilize a mail bounce message, select the radio button for **Bounce with phrase** and enter the text that the mail bounce message is to contain.

5. To utilize a catch-all email address, select the radio button for **Catch to address** and enter the appropriate email address.

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

7. Check or uncheck the **Allow scripting for web users** and **WebMail** checkboxes to enable or disable the corresponding options.

8. The **UPDATE** button is used to submit any and all changes.

9. The **UP LEVEL** button returns you to the *Domain Administration page*.

NOTE: Selecting **UP LEVEL** without selecting **UPDATE** will cancel all changes.

NOTE: If data is improperly entered (i.e. the wrong format of an email address, et cetera), an error message appears with a notice of the error.

Accessing the Domain Report

PSA keeps a summary of pertinent data relating to all of your domains. You can view this information at any time. At the top of the *Report page*, the domain being reported on is listed in boldface. The domain report includes the following information:

- Domain owner (client)
- Domain status
- Creation date
- Hosting type
- Virtual host type
- IP Address
- FTP Login
- FTP Password
- Disk space limit
- Real disk space
- Traffic

- Real Traffic
- FrontPage support
- SSI support
- PHP support
- CGI support
- mod_perl support
- Apache ASP support
- SSL support
- Web statistics
- Web users
- Apache error docs
- Anonymous FTP
- Mailboxes
- Redirects
- Mail Groups
- Autoresponders
- Domain user
- Databases

To access the domain report, follow these steps:

1. From the *Client Home page*, click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.
2. Click the **REPORT** button to see the domain's data and statistics.
3. From this screen, you can do several things:
    - You can send the report as email. You may need to send this report to your administrator. Email the report by clicking **SEND AS E-MAIL**. Or, enter a different email address to send the report to another recipient.
    - You can access graphical site statistics for the domain by selecting the **WEBALIZER** option. This opens a separate window where you will see the site statistics for the given domain. It should be noted that Webalizer, by default, is set to update statistics for the domain once every 24 hours. If you attempt to access Webalizer before it has operated its first update you

will receive a notice that Webalizer is either not running or has not yet been started.

- To print a copy of the report, select **File/Print** in your browser and a paper copy of the report will print.
- To return to the domain record, click **UP LEVEL** to close the report and to return to the *Domain Administration page*.

Managing Mail

PSA allows the client to perform several email administration functions. PSA uses the qmail system to help you set up email accounts and services. Your email system is protected against spamming, because qmail does not allow the mail server to be remotely accessed.

You can create and manage email boxes for individuals or customers within your domain. Email management functionality includes:

- Create, edit or delete email boxes and edit individual mailbox quotas.
- Redirect or forward messages from one email box to another email address
- Create, edit or delete email groups (several individual accounts grouped together under one email address for convenient multi-copy messaging).
- Create, edit, or delete email autoresponders (automatic reply to email sent to the given mail name)

Mail Names page

When you create email accounts for domain users, you are creating email boxes, which will be accessible via POP3 or IMAP protocols. Mailbox creation is as easy as keying in a name and password. Follow these steps to manage mail names:

1. From the *Client Home page*, click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.
2. Click the **MAIL** button. The *Mail Names Management page* appears. From this page, users can:
    - Create a new mail name.
    - View a list of mail names currently existing under the specified domain. To the left of each domain name on the list there are four icons representing different mail account types. They are:
        - Mailbox (represented by the "mailbox" icon)
        - Redirects (represented by the "outgoing envelope" icon)

        - Mail groups (represented by the "people" icon)
        - Autoresponders (represented by the “revolving envelope” icon)
    - Click on a specific mail name to access to the *Mail Name Properties Page* for that given name.
    - Search the mail names list for a certain pattern. It may help you in case you have a great number of mail names in the system and you need to work with a particular one. To search the list, type the pattern string in the text input field and click **SUBMIT**.
    - Sort the list by various parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.
    - Delete mail names. To remove one or more mail names, check the checkboxes in the **Del** column of the mail names list corresponding to the mail names you wish to remove and click **REMOVE SELECTED**. The *Mail Names Removal page* appears. There you will need to either confirm the removal (check the checkbox and click **SUBMIT**) or **CANCEL** it.

3. To create a new mail name, click in the **Mail Name** text box provided and enter the desired name. Click **ADD** to submit this name. You then access the *Mail Name Properties page*, where you can adjust the Mail Name properties.
4. The new mail name appears on the mail names list.

NOTE: The four icons to the left of each mail name are faded (grayed out) when they are inactive. The icons appear in color when active. To change the activation settings, the user must click on a given mail name. The *Mail Name Properties page* displays. From here, the user can enable any of the features.

Manage Mail Name Properties

The *Mail Name Properties page* allows the client to activate any combination of mailboxes, mail redirects, and mail groups for a given mail name.

1. From the *Client Home page*, click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.
2. Click the **MAIL** button. The *Mail Names page* appears.
3. In the **Mail names list**, click on the name you want to edit. You then access the *Mail Name Properties page*.
4. The mail name is listed at the top of the page. To change the mail name, click in the name field, change the name, and click **UPDATE**.

NOTE: From the *Mail Name Properties page*, you can also enable and set up:

- Mailbox Accounts and Quotas

- Mail Redirects
- Mail Groups
- Mail Autoresponders

5. When you are finished editing mail name properties for the domain, click **UP LEVEL** to return to the *Mail Names page*.

Manage Mailbox Accounts
You can set up a mailbox and password for your mail name. This mailbox will be accessible using either POP3 or IMAP protocol.

NOTE: An administrator can limit the number of mailboxes a client can have for a given domain.

To create a mailbox for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. Click in the check box provided next to **Mailbox**.
2. When enabling a mailbox for the first time for a mail name account, you must enter a password.
    - The **Old Password** will say "NONE" if you have yet to enter a password. Once it is entered, the password cannot be viewed from this screen.
    - To enter a password, click in the **New Password** text box and enter the selected password.
    - To properly update the password, you must re-enter the password in the **Confirm Password** text box.
    - To set up the mailbox quota, select the **Default for domain** radio button to set the limit to the maximum available in the given domain, or select **Enter size** and enter the quota you wish to set, in KiloBytes, for the given mailbox. Note that this limit may not exceed the default set for the domain.
    - Once you have enabled the mailbox, entered the passwords and set up mailbox quota, click **UPDATE** to submit the information.
    - To change a password, simply re-enter the new password in the **New Password** text box, re-enter this password in the **Confirm** text box, and click **UPDATE**.

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

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

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

NOTE: The administrator has the ability to limit the number of mail redirects that the client can create for a given domain.

In order to create or enable a mail redirect for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. Click in the check box provided next to **Redirects**.
2. In the text field to the right, enter the appropriate address to which to forward mail sent to this mail name.
3. To change the redirect address for a given mail name, click on the existing entry in the **Redirects** box and change it to the new address.
4. Click the **UPDATE** button to enter these changes.

NOTE: Once enabled, the redirects icon on the *Mail Names page* appears in color.

Manage Mail Groups
A mail group is a list of several email accounts that are grouped together under one email address for convenient multi-copy messaging. For example, if you want to send the same message to 5 people in the programming department, you can create a "Programming" email group that includes the individual email addresses for all 5 staff members. So, when someone sends a message to the Programming email group, he/she only types and sends one message. Copies of the message are emailed to all 5 individuals. By using mail groups, the sender does not need to know each individual's email address, just the group name. In this way, mail groups save time.

NOTE: The administrator has the ability to limit the number of mail groups that the client can create for a given domain.

To create a mail group for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. Click in the checkbox provided next to **Mail Groups**.

2. To create a new mail group, ensure the box is checked, then click the **ADD** button.

3. The **Add Mail Groups** box appears.

   NOTE: Group members can consist of either external mail addresses (those not belonging to this domain) or accounts existing within the domain.

4. To add an external mail address to a Mail Group, fill in the correct address in the **enter external recipient mail** text box, and click **ADD**.

5. To add an existing account from the same domain, click on the desired address in the **Select registered users** list, and click **ADD**.

6. The selected addresses will appear in the box to the right of the mail groups checkbox on the *Mail Name Properties page*.

7. To delete one or more group members, highlight the selected group member in the box to the left of the mail group check box. Click the **REMOVE** button.

8. A warning will appear. Click **OK** to confirm that you want to delete the address from the mail group.

9. After completing your changes, click **UPDATE** to submit all changes.

NOTE: Once enabled, the mail groups icon on the *Mail Names page* appears in color.

Manage Mail Autoresponders

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

In order to enable and set up an autoresponder for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. To first enable autoresponders for a mail name account, click in the checkbox provided next to **Mail autoresponders.** When the check appears, autoresponders are enabled for the mail name. If you click again, it will uncheck the box, and autoresponders will be disabled.
2. For the Autoresponder feature you have the option to include file attachments. To include a file to be selectable within the set up of autoresponders for the given mail name, use the **Browse** button to search for and select the desired file(s). (File sizes should be limited to no more than 1MB.)

3. Click the **SEND FILE** button. The attachments will then appear in the **Repository.**
4. These files will be available for any autoresponders that are set up for the given mail name. To delete one or more files highlight the desired file(s) and click the **REMOVE** button. A warning will appear prior to deleting the selected file(s).
5. To add a new mail autoresponder, click the **ADD** button.
6. A pop-up screen prompts you to enter a name for the autoresponder. Enter the desired identification name, and click **OK** to submit.
7. The *Edit Mail Autoresponder page* appears.
    - The selected autoresponder name is listed for the given mail name account. You can click in the text box where the autoresponder name is listed, and edit the name. Click **UPDATE** to submit.
    - The ON/OFF status for the autoresponder is shown. **[ON]** indicates that the autoresponder is on. **[X]** indicates that the autoresponder is off. You can adjust this setting by clicking the **ON/OFF** button. This status icon also appears on the autoresponders list on the *Mail Names Properties page*.
    - Beneath the Request text input box, you can determine whether an autoresponder responds to specific text found within either the subject line or body of the incoming email, or if it responds to ALL incoming requests
    - To set up the autoresponder to always respond, regardless of the contained text, click the bottom radio button for **always respond**.
    - Using the **Request text** input box and radio buttons, you can set up the autoresponder to send an auto response when an incoming request contains defined text in its subject line or body.
    - Click the **in the subject** radio button to respond to specific text in the subject of the request, or click the **in the body** radio button to respond to specific text in the body of the request.
    - You can select a specific subject to appear in your autoresponder using the **Answer with subject** optoin. To simply respond with the same subject as was received from the incoming request select the radio button for the default setting. To specify a specific subject line select the radio button beside the text box and enter the desired text.
    - You can enter text to be included in the autoresponder in the **Answer text** field.
    - Using the **ADD** and **REMOVE** buttons, you can attach files to be included in the autoresponder. These files must be uploaded into the **Repository** on the *Mail Names Properties page*. Select the uploaded file from the **Attach files** list, and use the **ADD** button to attach the file to the autoresponder. Click **REMOVE** to remove a file.
    - You can specify the frequency at which the autoresponder responds to the same unique address, after receiving multiple emails from it. By clicking in the appropriate radio button next to **Reply To Unique Email Address**, you can set the autoresponder to **always** respond, to respond **once**, or to respond once per a specified number of **days**. The default setting is to respond once in one day to unique mail addresses. It is highly

recommended that you leave this setting, or set to respond once in a given number of days. Selecting always respond can potentially overload your mail server. If the days value is defined as "0", then the autoresponder will respond each time a request is received.

- You can define the number of unique addresses that the autoresponder will remember. Enter the desired number in the **Store up to:** field.
- This memory enables the system to implement the answer-frequency and respond-once functionality. In the event of extremely high mail volume, to protect server performance, you can limit the address memory of the system database.
- To specify an email address to which incoming requests are forwarded, enter the new email in the **Forward request to e-mail** field. Email requests meeting the properties established on this page will be forwarded to this alternate email address.
- Click the **UPDATE** button to submit all changes.

Customize DNS Settings

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

NOTE: Improper set up of DNS results in improper functioning of your web, mail and ftp services.

DNS Settings Page
There are five types of accessible DNS records:

A = Address - This record is used to translate host names to IP addresses.
CNAME = Canonical Name - Used to create additional host names, or aliases, for hosts in a domain.
NS = Name Server - Defines an association between a given domain name and the name servers that store information for that domain. One domain can be associated with any number of name servers.
MX = Mail Exchange - Defines the location of where mail should be delivered for the domain.
PTR = Pointer - Defines the IP address and host name of individual hosts in the domain. Translates IP addresses into host names.

When you first enter this screen, you see the DNS status for the domain, as well as the default DNS settings created for the given domain. PSA will pull the default DNS settings from those set up under the SERVER DNS option.

Changing DNS Settings
In order to change DNS settings, follow these steps:

1. From the Client Home page, click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.
2. Click the **DNS** button to access the *DNS Settings page*.
3. The **DNS Zone Status** icon indicates whether a DNS is turned on or off.
    - If you wish to turn DNS on or off for the domain, select **ON/OFF**.
    - Turning the DNS zone off will refresh the page, so that only a list of nameservers remains.
    - If you are running remote DNS, and therefore want to turn DNS off for the domain, you should first create the appropriate **NS** entries for the domain and remove any inappropriate **NS** entries possibly created by the default DNS template created under the SERVER function. At that point, turn DNS off. You see that the name server(s) for the domain remains listed as a link.
    - You can perform a test on these name servers by selecting any of them. Selecting any name server will perform an NSLookup to check for the DNS records for your specific domain on that specific name server. NSLookup is used to verify the A record for the domain, the CNAME record for www, and the MX record to ensure that these basic records are resolved properly on the remote name server. The results are interpreted and presented through the user interface.
4. In order to add a DNS entry, select the type of record you wish to create and select **ADD**. Each record type has its own different set up.
    - 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 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 (i.e. ns1). Then, you need to enter the appropriate IP address to which to associate the domain name. Then select **UPDATE** to submit your entry.
    - For an 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 in the appropriate name server in the field provided. You will need to enter in the complete name (i.e. ns1.mynameserver.com). Then, select **UPDATE** to submit your entry.
    - For a MX record, you will need to enter the domain for which you are creating the MX record. For the main domain, you would simply leave the available field blank. You will then need to enter your mail exchanger, this is the name of the mail server. If you are running a remote mail server

named "**mail.myhostname.com**" then you would simply enter "**mail.myhostname.com**" into the field provided. You will then need to set the priority for the mail exchanger. Select the priority, 10 being the highest and 40 being the lowest, from the drop down list. Keep in mind you also would need to add the appropriate A record, and/or CNAME if applicable for the remote mail server. Select **UPDATE** to submit your entry.

- For a CNAME record, you will need to first enter the alias domain name for which you wish to create the CNAME record. You then need to enter the domain name within which you want the alias to reside. Any domain name can be entered. It does not need to reside on the same server. Select **UPDATE** to submit your entry.

- For a PTR record you will first enter the IP address for which you wish to define the pointer. Then enter the appropriate domain name for this IP to be translated to. Select **UPDATE** to submit your entry.

5. You may remove any DNS records by selecting **REMOVE** beside the record you wish to delete. Before anything is processed you will be asked to confirm the deletion.

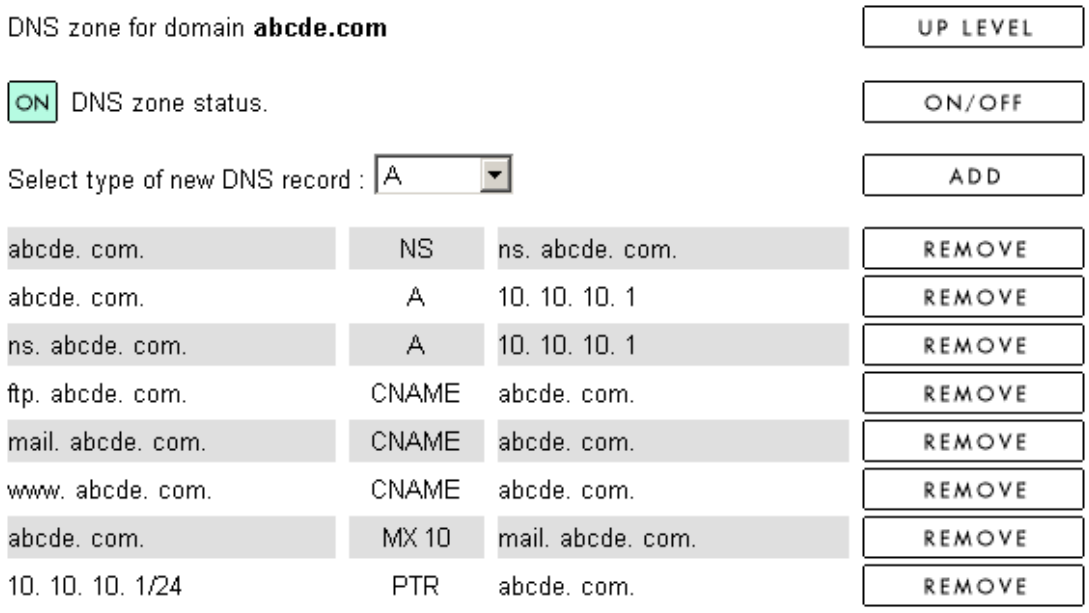
DNS Example Setups

Example 1: A hosting company (we'll use *abcde.com*, which is for example purposes only, and is not intended to represent any existing companies or domains) wishes to setup their PSA enabled server as the primary DNS server for all the domains they create and will run secondary DNS services on an external server (the recommended configuration). The PSA enabled server has an IP address of *10.10.10.1* and the external name server has an IP address of *10.10.10.2*. These addresses will be used for *ns1.abcde.com* and *ns2.abcde.com* respectively. IP address *10.10.10.1* is also the main server IP address that was set up during PSA installation.

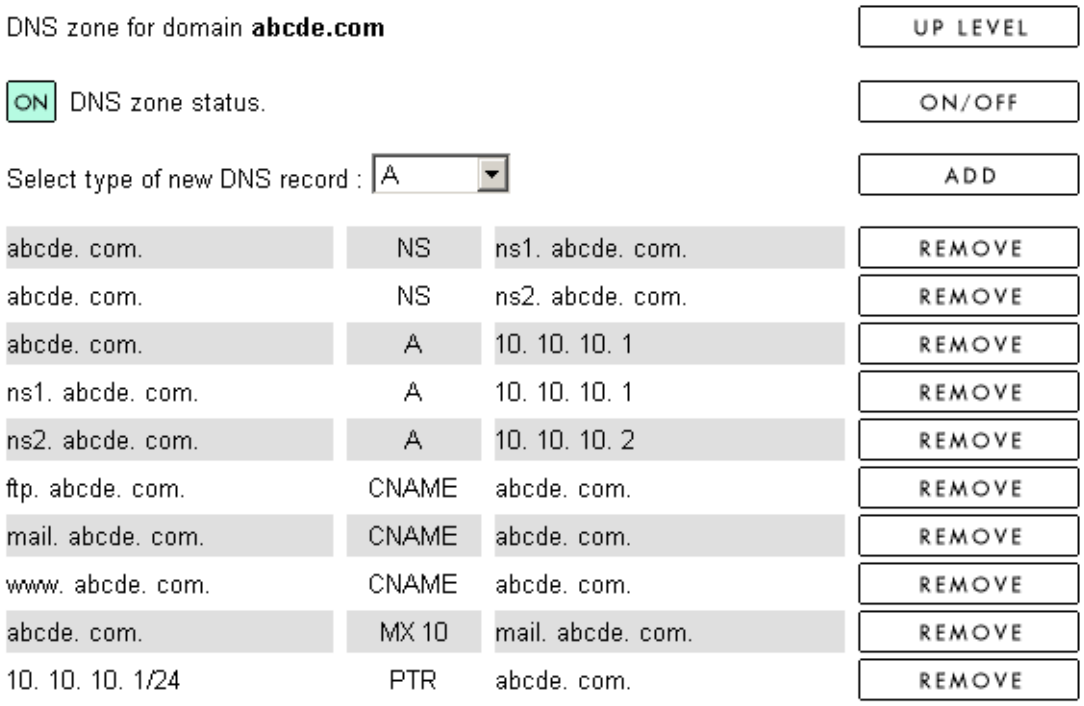
NOTE: All name servers need to be properly registered. They need to specifically be registered as name servers with Internic. Also, all domains must be registered with the appropriate name server information.

*The first step in the process is to create the domain *abcde.com* on the server. By default, when a domain is initially created, even before hosting has been configured, PSA sets up a DNS record for the domain. This DNS record is created based on the DNS template that is created by the Admin under the SERVER - DNS option. For the purpose of this example we will use the default setup prior to any modifications made by the Admin under the SERVER –DNS option. With this default setup a properly registered domain will resolve. However, the setup does require some modification. The initial assumptions are that the domain is a name-based account and that DNS, Mail and FTP services are to

be handled locally. So the resulting default DNS settings for a domain named *abcde.com* are as follows:

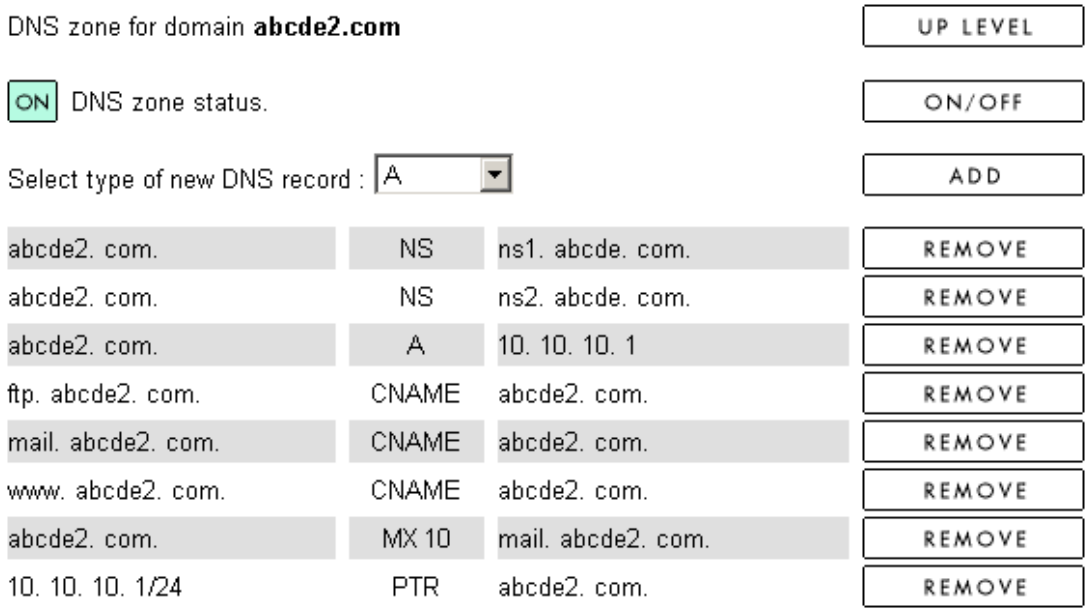


*The next step is to create A records for the name server names you will be using. Every name server name must have a specific IP Address associated with it. Manipulate the DNS records for *abcde.com* to reflect the following. Exact instructions for adding and removing DNS records are described earlier in the section or can be found by selecting HELP within PSA.



No other entries are needed.

*From that point on you would only need to change the NS records for each individual domain, such as *abcde2.com*, to be *ns1.abcde.com* and *ns2.abcde.com* and then remove the A record that is created for the default name server (*ns.abcde2.com*). The result for a different domain, *abcde2.com*, would be as follows:



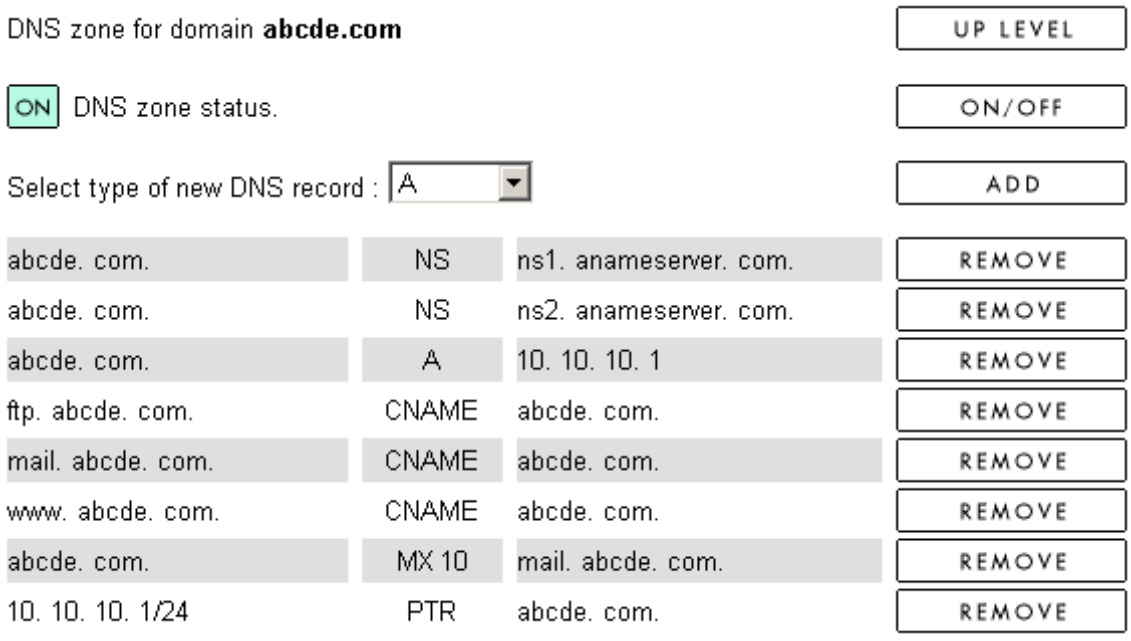
This would be repeated for all the domains created on the server.

NOTE: PSA creates the Primary Zone Files for every domain on the server. It will not create any Slave Zone Files for the secondary DNS. If you plan to setup both primary and secondary name servers locally on your PSA machine it important to understand that you will technically have no Slave Zone Files. For some registrars this can cause rejection of your domain registration request. It is always recommended that secondary DNS services be run on a separate physical server from the primary.

Example 2: A hosting company, *abcde.com*, wishes to run both their primary and secondary DNS services remotely from the PSA enabled server. They have two name servers: *ns1.anameserver.com* and *ns2.anameserver.com*. Their PSA enabled server has the IP-Address of *10.10.10.1*.

NOTE: By default, when a domain is created in PSA, it is assumed that DNS is being resolved locally. In the case described above, *abcde.com* needs to add in the appropriate NS records within each newly created domain and then turn DNS off for that domain.

*The first step is to modify the default PSA DNS settings for the new domain, *abcde.com*, to include the appropriate NS records. The result would be as follows:



*Then select the **ON/OFF** button. PSA will remove the DNS records, however you will still see the records that you had entered as the NS records for the domains. The result would be as follows:

You can then perform a test on these name servers by selecting either of them. Selecting either name server will perform an NSLookup to check for the DNS records for your specific domain on that name server. If there are any errors PSA will report them to you.

Register a Domain

When a new domain is created it must be officially registered. There are a number of Internet services where you can register your domain but there is one that is offered by Plesk Inc.

To register a new domain, follow these steps:

1. Click the **REGISTER** button at the *Domain Administration page* to access the *MPC Gate page*.

2. From *MPC Gate page* you can access the services provided to you by My.Plesk.com. To do that, enter the **MPC Login** and **MPC Password** into the provided corresponding text input fields and click **LOG IN**.

3. You can check the **Remember account** checkbox to have you login and password remembered by the system. This way the next time you wish to access MPC, you will be taken directly to My.Plesk.com and will not be prompted to enter your login and password.

4. In case you forgot the password, there is a button provided especially for such occasions: **FORGET PASSWORD?** Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your Server Administrator profile.

5. You can return to the *Domain Management page* by clicking **UP LEVEL**.

Changing Hosting Settings

You may have hosting privileges established in your domain so that you can provide various Internet services (e.g. software applications, a forwarding address, and FTP transfers). PSA allows three different types of hosting services:

- **Physical Hosting** - This is the most common type of hosting service, creating a virtual host (disk space on the local server) for the client. The client controls and publishes his own website without having to purchase a server and dedicated communication lines.

- **Standard Forwarding** - With this type of forwarding, all requests to the domain are forwarded by your server to another Internet address (no virtual server is created). When an end user searches the Internet for the client's domain, he is routed to another URL, and the address in his browser window changes to the new URL. This may be confusing to the end user.

- **Frame Forwarding** - All requests to this domain are forwarded to another Internet address (no virtual server is created). But with this type of forwarding, the end user sees the client's domain name in his browser, not the forwarding address. PSA uses frames to "trick" the browser into displaying the correct domain name. The problem with frame forwarding is that some search engines do not index frame pages and some browsers do not support frames.

The system administrator has already performed all the technical system administration for hosting services relating to your domain; however, the type of hosting service set up for your domain determines the extent to which you can manage your hosting parameters. If you have physical hosting, you can use FTP software to access your hosting directions. Additionally, you can change the FTP password, set log rotation schedules, and enable/disable FP support, only if FP has been activated for your domain by the Plesk administrator. If frame or standard forward hosting is set for this domain, than you can change (or toggle between these two types) forwarding for the given domain. You may also be granted a right to choose among all three types.

Follow these steps to administer your hosting services:

1. From the *Client Home page*, click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.

2. Click the **HOSTING** button. A page with a choice of types of hosting appears.

3. Select the type of hosting and click **NEXT**. Depending upon the type of service chosen, a customized hosting configuration page appears.

Physical Hosting Configuration

There are several physical hosting services for your domain. Some of them may or may not be made available by the administrator for you to configure:

- FTP services, or file transfer capabilities - FTP allows end users to upload and download files from the Internet site to remote PCs. If you have an FTP account, you can change its access password. You may want to change the password occasionally for security purposes.

- FrontPage support - You can authorize remote editing of the website, for this domain, using Microsoft's FrontPage web publishing tool.

- SSI - SSI stands for "server-side include," a type of HTML comment that directs the web server to dynamically generate data for the Web page whenever information is requested. SSIs can also be used to execute programs and insert the results; therefore they represent a powerful tool for web developers.
- PHP - PHP is an HTML scripting language for creating dynamic web pages.
- CGI - CGI is a set of rules that describes how a web server communicates with another piece of software on the same machine, and how the other piece of software (based on the CGI program) communicates back to the web server.
- mod_perl – Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use is for a vast number of automation tasks. Most CGI programs are written in Perl.
- Apache ASP – Active Service Page support enables the use of dynamic web applications. Apache::ASP allows for the use of Active Server Pages utilizing with Perl scripting only.
- SSL - Secure Socket Layer (SSL) certificates provide additional security for web sessions, for e-commerce applications and for other private or confidential applications. By enabling this option, users access your website with the command **https://**.
- Web statistics
- Apache ErrorDocs – allows custom error-message files to be used for displaying whenever an error occurs (i.e. **404 – URL Not Found**).

Follow these instructions to manage your virtual host (physical hosting account) services:

1. You access this page from the *Hosting Type page* when you select Physical Hosting. Use this page to set up or modify a physical hosting account.
2. Depending on the limits set within the given Client's Preferences, you can create two different types of virtual hosts: name-based or IP-based. The Plesk Server Administrator (PSA) defaults to the most commonly used type, name-based. If you want to change the host type, click the IP-based choice. Then, select a valid IP address from the drop down list. The list of available IP's will reflect the settings within the given Client's Preferences.
3. You may set or modify the FTP login name and password. FTP allows end users to upload and download files from the Internet site to remote PCs. If you want to provide FTP services, click in the FTP login box. Then, enter or edit a login name to be used for accessing FTP file transfer services on the domain.
4. TAB to the **FTP Password** text box and enter or edit the FTP password.
5. TAB to the **Confirm FTP Password** text box and enter the FTP password for confirmation.

6. TAB to the **Traffic limit** text box and enter or edit the number of megabytes available for monthly transfers. If the traffic limitation is exceeded, the domain's status will change to [!].

7. The **Delete Apache Log Files** text box allows you to decide whether or not you would like the Apache log files to be deleted automatically, if at all. The default setting will say NEVER, indicating that no automated deletion will occur. If you prefer to enable the deletion function, click on the drop-down arrow; then, you can choose between the WEEKLY and MONTHLY deletion frequencies.

8. TAB to the **FrontPage Support** check box to install FrontPage server extensions into the domain. FrontPage is Microsoft's Web publishing tool. It is one of the most commonly used tools for creating a client's website. FrontPage includes several extensions that provide special functionality. If you want this domain to support these extensions, be sure that a check mark appears in the FrontPage box.

9. TAB to the **Authorization ENABLED** choice. You can authorize or disable remote editing of the website using FrontPage. If you are supporting FrontPage, you should disable authorization for additional security. This setting is changeable by the Admin, Client, and Domain User logins to the control panel. For security purposes the main server administrator should notify their Clients and Domain Users that FrontPage authorization should be disabled whenever not in use. To activate FrontPage authorization, make sure this choice is selected. If you want to turn off FrontPage authorization, select the **Authorization DISABLED** choice.

10. If FrontPage support is selected, then the **FP Admin Login,FP Admin Password**, and **Confirm Password** fields must be entered. This login and password will be used to login to the domain when FrontPage is being used. Click in each box and enter the desired Login and Password.

11. TAB to the **SSI support** check box. SSI stands for "server-side include," a type of HTML comment that directs the web server to dynamically generate data for the Web page whenever information is requested. SSI can also be used to execute programs and insert the results; therefore they represent a powerful tool for web developers. If you want the SSI support enabled, make sure a check mark appears in the SSI box.

12. TAB to the **PHP support** check box. PHP is a server-based HTML embedded scripting language used to create dynamic Web pages. If you want to support PHP scripting in HTML documents, make sure a check mark appears in the PHP box.

13. TAB to the **CGI support** check box. CGI is a set of rules that describes how a web server communicates with another piece of software on the same machine, and how the other piece of software (based on the CGI program) communicates back to the web server. If you want to support CGI, make sure a check mark appears in the CGI box.

14. TAB to the **mod_perl support** check box. Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use it for a vast number of automation tasks. Many CGI programs are written in Perl. If you want to support Perl, make sure a check mark appears in the mod_perl box.

15. TAB to the Apache ASP support checkbox. Apache::ASP allows for the use of Active Server Pages utilizing with Perl scripting only. It enables the development of dynamic web applications with session management and embedded perl code.

16. TAB to the **SSL support** check box. SSL certificates provide additional security for Web sessions. SSL certificates are often used for e-commerce applications and other private or confidential applications. Enabling SSL creates an **httpsdocs** directory in the FTP account, and provides https protocol; as a result, users access the domain with the command **https://newdomain.com**. If you want to be able to implement an SSL certificate, make sure a check mark appears in the SSL box.

17. TAB to the **Web statistic** check box. Activation of web statistics will result in the installation of a graphical statistics package for the domain. This package is accessible via the PSA interface within the given domain's **Report** page or via the internet using the URL http://<domainname>/webstat.

18. TAB to the **Apache ErrorDocs** checkbox. Selecting this option will place the domain's error documents into a location that is accessible via FTP allowing you to customize your own Apache error documents.

19. When you are satisfied that you have fully defined the hosting services for this domain, click **UPDATE** to return to the *Domain Administration page*.

NOTE: If you do not want to save the physical hosting parameters you have entered, or if you need a different hosting type, click **UP LEVEL** to return to the *Domain Administration page*.

Forwarding Configuration

If you have either of the two forwarding options defined for your hosting services, standard or frame, then you can change between the two types of forwarding. Also, you can edit the URL to which domain transactions are re-directed or forwarded.

1. To change the type of forwarding you have, from the *Hosting page*, click on the type you want to change.

   NOTE: Confirm that you really need to change the type of forwarding before actually changing it. Only a Plesk administrator can change a forward hosting account to physical hosting. A client cannot make this change.

2. Click **NEXT** to access the URL page.

3. To change the forwarding address, click in the **URL** text box and enter or edit an Internet address to which you wish to re-direct all domain traffic.

4. Click **UPDATE** to submit changes.

Web Users Management

A web user is a user account within Apache. It is used to define locations for personalized web pages with individual FTP access. The result of creating a web user is a subdirectory within your domain (e.g. domain.com/~webuser).

A list of all of the web users within a given domain will appear on the main *Web Users page*. At this page you can:

- Select any web user name to edit the web user password and/or to add or remove different scripting options.
- Search the web users' list for a certain pattern. It may help you in case you have a great number of web users in the system and you need to work with a particular one. To search the list, type the pattern string in the text input field and click **SEARCH**.
- Sort the list by various parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

To create a new web user:

1. From the *Client Home page*, click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.
2. Click the **WEB USERS** button. The *Web Users page* appears.
3. To add a web user, enter the **Web User name** in the text box provided next to **Web user name:** and click **ADD**.
4. You are taken to the *Web User Password Entry Page*, where you must enter and confirm the password for your new web user and select from the available scripting options for the given domain (availability of scripting options is set in the Domain Preferences). To do this, enter a password in the **New password** text box, and then re-enter it in the **Confirm password** text box. Then select from the available scripting options if applicable. Once you have completed all entries, click on **UPDATE** to enter the information. Selecting **UP LEVEL** will return you to the *Web Users page* without assigning a password or scripting capabilities to the given web user. Although the directory will be created, it will not be accessible via FTP using the web user name.
5. As you create web users, the user names appear on the *Web User Management page* in the web user list.

6. To change web user passwords or edit scripting options, click on the user name in the web user list. This takes you to the *New Password page*.

7. When you are done, click **UP LEVEL** to return to the *Domain Administration page*.

To remove one or more web users, check the checkboxes in the **Del** column of the web users' list corresponding to the web users you wish to remove and click **REMOVE SELECTED**. The *Domain Removal page* appears. There you will need to either confirm the removal (check the checkbox and click **SUBMIT**) or **CANCEL** it.

Important Notes on web users:

- For security purposes, the password must be between 5 and 14 characters and cannot contain the user name.
- Each web user creates a system account within Apache; therefore, you cannot have two web users with identical names on the same server.
- New web users can access the directory using FTP software by entering the domain name under which the web user account was created and using the appropriate web user name and password.
- Your administrator CAN limit the number of web users you can create. You will receive a warning if you try to exceed this number, and will not be able to do so.

Protected Directories

This feature is active if virtual hosting (physical hosting account) has been configured for your domain. It creates secure directories in your virtual domain, in which to place documents. Secure directories are recommended to ensure security of confidential and private information. It is possible to create directories under either the standard virtual host accessible via http protocol, or if applicable for the given domain, under the SSL virtual host accessible via https protocol. Icons are used next to each directory name in the directory list to define which virtual host type (SSL or non-SSL) the directory resides within. An open lock depicts non-SSL; a closed lock depicts SSL.

Creating a Protected Directory

Follow these steps to create secure directories for the domain:

1. From the *Client Home page,* click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.

2. Click the **DIRECTORIES** button. The *Protected Directory Management page* appears.

3. To create a new directory, click the **ADD** button.

4. This takes you to the *Protected Directory Control page*. Enter the name of the protected directory you wish to create in the **Protected Directory** field provided.

5. For **Directory Location:** you can choose either a non-SSL or SSL secure directory. To choose a non-SSL directory, click in the radio button next to **Non-SSL**. To choose SSL security for the directory, click in the radio button next to **SSL**.

6. If the directory has SSL enabled, it will appear in the Protected Directory list with a gray **Lock** icon beside it. If the directory is non-SSL, a gold **Unlocked** icon will appear next to the directory name in the directory list.

7. Click in the **Header Text** text box. When a user tries to access the protected directory, the text in this box displays as the Realm they are entering. In this text box, enter the header text.

8. To add a new user, under **Protected Directory Users** click in the **New User:** text box**,** and write the name of the directory user.

9. Click the **ADD** button.

10. You are taken to the directory user password screen. Here you must enter your new password in the **New Password** text box, and then enter it again in the **Confirm password** text box.

11. Click the **UPDATE** button to submit. You will return to the Protected Directory Control page. The new user will appear in the Protected Directory Users list. Clicking **UP LEVEL** will return to the *Protected Directory Control page* without creating a password for the given user. Although the user is created no access to the directory will be granted until a password is created for the user.

12. To remove existing directory users select the users that you wish to remove using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the directory users.

13. To access a directory user in order to edit the user password, click on the user name in the list, and you will again be taken to the directory user password screen. Here you can edit the password.

14. Select **UPDATE** to submit your changes and return to the *Protected Directory Control page.*

15. Click **UP LEVEL** to return to the *Protected Directory Management page* without saving any changes.

Changing a Protected Directory

You can edit a protected directory definition to:

- Add a user

- Change a password
- Delete a user
- Rename the directory
- Change header text
- Change the SSL status

Follow these steps to edit protected directories:

1. From the *Client Home page*, click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.
2. Click the **DIRECTORIES** button. The *Protected Directory Management page* appears.
3. Click on any directory from the list that you wish to change.
4. You will be taken to the *Protected Directory Control page.*
5. From here, you can edit the directory by following the same steps outlined above, in the **Creating a Protected Directory** section.
6. Click **UPDATE** to complete all changes to the system and to return to the *Protected Directory List page*.

Searching the Protected Directories List

PSA allows you to search the Protected Directory List for a certain pattern. It may help you in case you have a great number of directories in the system and you need to work with a particular one. To search in the list:

- Select the input field and type in the pattern string.
- Click the **SEARCH** button.
- If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Protected Directory List.
- If no matches were found it will be so stated.
- The button **SHOW ALL** will revert to displaying the whole list of domains.

There is also another way to ease the process of working with a large list of directories. An option of sorting the list by several various parameters is made available to you. You can sort the list by several parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Removing a Protected Directory

To remove one or more directories, follow these steps:

1. Check the checkboxes in the **Del** column of the Protected Directories List corresponding to the directories you wish to remove.

2. Click on **REMOVE SELECTED**. The *Protected Directory Removal page* appears.

3. For every directory you chose to remove the name of the directory and the names of this directory users will be displayed.

4. If you are certain that the displayed information is correct and wish to proceed with deleting, check the "Yes, I have read, understood, and agree to remove protect from these domains" checkbox. Then click **SUBMIT**. If you decide to not delete these directories or wish to modify the list of directories chosen for deletion, click the **CANCEL** button.

Both buttons will return you to the *Protected Directory Management page*, one committing the changes, the other one leaving everything unchanged.

NOTE: Deleting a protected directory in PSA does not delete the directory off the server. It simply takes the protected status off the directory. Meaning that the directory and its contents will now be reachable via the Internet without the need for login and password.

Manage the Domain SSL Certificate

PSA enables you to upload a Secure Socket Layer (SSL) Certificate, generate a Certificate Signing Request (CSR), generate a Self-signed Certificate, and/or purchase a SSL certificate through a registered certificate authority. Each certificate represents a set of rules used when exchanging encrypted information between two computers. Certificates establish secure communications; this is especially important when handling e-commerce transactions and other private transmittals. Only authorized users can access and read an encrypted data stream.

Notes on Certificates:

- In order to use SSL certificates for a given domain, the domain MUST be set-up for IP-Based hosting.
- When an IP-based hosting account is created with SSL support, a default SSL certificate is uploaded automatically. However, this certificate will not be recognized by a browser as one that is signed by a certificate signing authority.
- The default SSL certificate can be replaced by either a self-signed certificate or one signed by a recognized certificate-signing authority. The self-signed certificate is valid and secure, but many clients prefer to have a certificate signed by a known Certificate Signing Authority.
- You can acquire SSL certificates from various sources. You can purchase a certificate directly through your control panel interface through the Buy Certs option; using our services web-site My.Plesk.com (MPC). Also, you can generate

a certificate with the SSLeay utility and submit it to any valid certificate authority. This can be done using the CSR option within PSA.

- If using a SSL certificate issued by a certificate authority other than Thawte or Verisign, a rootchain certificate is required to appropriately identify and authenticate the certificate authority that has issued your SSL certificate.
- If the given domain has the **www** prefix enabled, you must set-up your CSR or self-signed certificate with the **www** prefix included. If you do not, you will receive a warning message when trying to access the domain with the **www** prefix.
- Remember to enter your certificate information in PEM format. PEM format means that the RSA Private Key text must be followed by the Certificate text.
- All certificates are located in the ../vhosts/<domain name>/cert/httpsd.pem file. Where this directory reads <domain name> , you must enter the domain name for which the certificate was created.

To generate a self-signed certificate or a certificate-signing request, follow these steps:

1. From the *Client Home page*, click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.

2. If you have established an IP based hosting account with SSL enabled, the **CERTIFICATE** button will be enabled.

3. Click the **CERTIFICATE** button. The *SSL certificate setup page* appears.

4. The **Certificate Information:** section lists information needed for a certificate Request, or a Self-Signed certificate.

5. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop down box next to **Bits:.**

6. To enter the information into the provided text input fields (**State or Province**, **Locality**, **Organization Name** and **Organization Unit Name** (optional)) click in the text boxes and enter the appropriate name.

7. To enter the Domain Name for the certificate, click in the text box next to **Domain Name:** and enter the appropriate domain.

8. The domain name is a required field. This will be the only domain name that can be used to access the Control Panel without receiving a certificate warning in the browser. The expected format is www.domainname.com or domainname.com.

9. Click on either the **SELF-SIGNED** or **REQUEST** button.

10. Clicking **SELF-SIGNED** results in your certificate being automatically generated and installed.

11. Selecting **REQUEST** results in the sending of a certificate-signing request (CSR) to the email address you provided in the fields discussed above. When a CSR (certificate signing request) is generated there are two different text sections, the

RSA Private Key and the Certificate Request. **DO NOT LOSE YOUR RSA PRIVATE KEY. YOU WILL NEED THIS DURING THE CERTIFICATE INSTALLATION PROCESS. LOSING IT IS LIKELY TO RESULT IN THE NEED TO PURCHASE ANOTHER CERTIFICATE.**

12. When you are satisfied that the SSL certificate has been generated or the SSL certificate request has been correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

To purchase a certificate through My.Plesk.com (MPC), first complete the steps given in items 1 – 11 of the previous instruction (generating a self-signed certificate or a certificate-signing request) and then proceed to:

12. **BUY CERTS** button to gain access to the certificate management interface on My.Plesk.com. The *MPC Gate page* appears.

13. This page allows you to create an account (the **CREATE ACCOUNT** button) and access (the **LOG IN** button) MPC from where you are taken through step-by-step instructions on how to purchase and manage your certificate.

14. In case you already have an existing account on MPC but forgot the password for it, there is a button provided especially for such occasions: **FORGET PASSWORD?**. Click it and enter your MPC account login name when requested into the provided text input field. Your password will be sent via e-mail to the address specified in your user profile.

15. When you are satisfied that the SSL certificate has been generated or the SSL certificate request has been correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

NOTE: if you do not wish to purchase certificates at this time but do wish to view the certificates currently owned by you, you may proceed directly to the *MPC Gate page* by clicking the **VIEW CERTS** button. At that you will not be prompted to fill in the details at the *SSL Certificate setup page*.

To upload a file containing the certificate authorized by the Certificate Signing Authority:

1. Click the **CERTIFICATE** button at the *Domain Administration page*. The *SSL Certificate page* appears.

2. If you wish to upload a Certificate File authorized by the Certificate Signing Authority, click the **BROWSE…** button under the **Upload previously bought Certificate File (without private key)** section to select the file (the file must be in .txt format)

3. Then, click **SEND FILE** to copy the certificate to the server.

To upload a new certificate:

1. Click the **CERTIFICATE** button from the *Domain Administration page*. The *SSL Certificate page* appears.

2. If you wish to upload a certificate file from a local computer, under the **Uploading Certificate File** section, click the **BROWSE…** button to select the file (the file must be in .txt format).

3. Then, click **SEND FILE** to copy the certificate to the server. Or, if you want to type in the text of the certificate without downloading a specific file, click in the text box and enter and paste the certificate information.

4. Click **SEND TEXT** to implement the text on the server.

   NOTE: Ensure that the private key text block is included along with the SSL certificate text block when using the **SEND FILE** or **SEND TEXT** options.

   EXAMPLE FORMAT:

```
-----BEGIN RSA PRIVATE KEY-----

[[ECRYPTED BLOCK OF TEXT]]

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

[[ECRYPTED BLOCK OF TEXT]]

-----END CERTIFICATE-----
```

5. When you download the certificate to the server, PSA checks for errors. If an error is detected, PSA restores the old version of the SSL certificate, and PSA warns you to update the certificate. At this point, you can try again to enter text or to download the certificate file.

6. When you are satisfied that the SSL certificate is correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

If you are using a certificate that has been signed by an authority other than Thawte or Verisign then it is likely that this will require the use of a rootchain, or CA, certificate. To install a rootchain certificate for the domain:

1. Click the **CERTIFICATE** button at the *Domain Administration page*. The *SSL Certificate setup page* appears.

2. The icon next to **Use rootchain certificate for this domain** appears on this page.

3. If the icon is **[ON]** then the rootchain certificate will be enabled for this domain. If the icon is **[X]** this function will be disabled.

4. To change the status of the rootchain certificate, click the **ON/OFF** button.

5. To upload your rootchain certificate, first make sure that it has been saved on your local machine or network. Use the **Browse** button to search for and select the appropriate rootchain certificate file.

6. Then click the **SEND FILE** button. This will upload your rootchain certificate to the server to assure proper authentication of the certificate authority.

7. When you are satisfied that the rootchain certificate is correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

Anonymous FTP

Within PSA the Client, given domain creation capabilities, can setup Anonymous FTP capabilities for a given IP-based virtual host. Anonymous FTP is used to allow an open, yet controlled, environment for visitors to the domain to download and/or upload files to and from the domain account. Users will be able to log into ftp.<domain name> with the standard anonymous user name and any password. PSA allows the setup and limitation of incoming file space, connected users, and bandwidth usage throttling. Administrators should take care when allowing the use of anonymous FTP and be sure to use all the limitation capabilities within the interface wisely. If setup with excessive limits, it could lead to problems with server resources as well as excessive bandwidth usage.

To set up Anonymous FTP:

1. Click the **ANONYMOUS FTP** button at the *Domain Administration page*. The *Anonymous FTP Feature Management page* appears.

2. By default anonymous FTP capabilities will be inactive. To activate anonymous FTP select the **ON/OFF** button. The status indicator next to **Anonymous FTP account status** will identify the status as either ON or X (off).

3. Select the checkbox beside **Allow uploading to incoming directory** to allow visitors access the anonymous ftp site to upload files into the /incoming directory.

4. Select the checkbox beside **Limit disk space in the incoming directory** to set the disk space quota (ie hard limit) on the /incoming directory. Then select the **Up to** field and enter the disk space, in KiloBytes, you wish to allow for the /incoming directory. If no specific limit is set, or zero is used in the **Up to** field, the setting is unlimited.

5. Select the checkbox beside **Limit maximum simultaneous connections number** to set limits on the number of users who can be simultaneously connected to the anonymous FTP site. Then select the **Up to** field and enter the number of connections allowed. If no specific limit is set, or zero is used in the **Up to** field, the setting is unlimited.

6. Select the checkbox beside **Limit download bandwidth for this virtual FTP domain** to set throttling up for the anonymous FTP site. Then select the **Up to** field and enter the maximum average bandwidth, in KiloBytes per second, allowed. If no specific limit is set, or zero is used in the **Up to** field, the setting is unlimited.

7. Once you have completed all changes, select **UPDATE** to submit all changes and return to the *Domain Administration page*.

8. Selecting **UP LEVEL** will ignore all changes made and return to the *Domain Administration page*.

Databases

Within PSA there is the ability to create multiple mysql databases as well as multiple users within each database. Also, directly accessible via PSA, is a link to PhpMyAdmin, a PHP interface that abstracts mysql into a web-based administration tool, allowing you to sort, edit, and create tables within a given database. Database limits are set through domain preferences and database disk usage is calculated within the domain's total allotted disk space.

Searching the Database List

PSA allows you to search the Database List for a certain pattern. It may help you in case you have a great number of databases in the system and you need to work with a particular one. To search in the Database List:

1. Select the input field and type in the pattern string.

2. Click the **SEARCH** button.

3. If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Database List.

4. If no matches were found it will be so stated.

5. The button **SHOW ALL** will revert to displaying the whole list of databases.

There is also another way to ease the process of working with a large list of databases. An option of sorting the list by several various parameters is made available to you. You can sort the Database List by **Type** and **Database Name**. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Creating a New Database

1. Click the **DATABASES** button at the *Domain Administration page*. The *Databases Feature Management page* appears.

2. To add a new database select the **Database name** field, enter the desired name, and select **ADD**. The *Database Editing page* appears.

3. To add database users to the newly created database enter the user name into **New user** text box and select **ADD**. The *Database User Management page* appears.

4. Enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the new user. Selecting **UP LEVEL** will ignore all entries and return to the *Database Editing page* making no changes.

5. Once you have completed the creation of the new database and its users select **UP LEVEL** to return to the *Database Feature Management page*.

6. To add further databases, follow the steps outlined in 1-5 above. To return to the *Domain Administration page* select **UP LEVEL**.

Editing an Existing Database

1. Click the **DATABASES** button at the *Domain Administration page*. The *Databases Feature Management page* appears.

2. Click on the database that you wish to edit. The *Database Editing page* appears.

3. To add database users to the selected database enter the user name into **New user** text box and select **ADD**. The *Database User Management page* appears.

4. Enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the new user. Selecting **UP LEVEL** will ignore all entries and return to the *Database Editing page* making no changes.

5. To edit the password of an existing database user, select the user from the database user list. The *Database User Management page* appears.

6. To delete existing database users select the users that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the selected users.

7. To access and/or edit database content you can do so using the **PHPMYADMIN** option. PhpMyAdmin provides a web-based graphical interface for mysql. This can be used to make content edits to your existing databases.

8. Once you have completed all edits of the database and its users select **UP LEVEL** to return to the *Database Feature Management page*.

9. To delete existing databases select the users that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the selected users.

10. To edit further databases, follow the steps outlined in 1-9 above. To return to the *Domain Administration page* select **UP LEVEL**.

Domain User

The domain user setup provides entry to the PSA control panel within a single domain. Domain users have the ability to administer mail accounts, web users, databases, protected directories, and the domain ssl certificate. Limits to the domain user are set by the Client and/or Administrator using the Domain Preferences.

Access to the control panel for the database user is done using https://<domain name>:8443. The control login will be the domain name, and the password will be whatever is set through the control panel.

To set up the Domain User:

1. Click the **DOMAIN USER** button at the *Domain Administration page*. The *Domain User Properties* page appears.

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

3. Enter the password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the domain user and return to the *Domain Administration page*.

4. Selecting **UP LEVEL** will ignore any changes and return to the *Domain Administration page*.

5. Domain-Level Administration

- 5.1 Introduction to Domain Usage
- 5.2 Domain Administration Page
    - View the Domain Preferences
    - Accessing the Domain Report
    - Managing Mail
        - Mail Names page
        - Manage Mail Name Properties
            - Manage Mailbox Accounts
            - Manage Mail Redirects
            - Manage Mail Groups
            - Manage Mail Autoresponders
    - View DNS Settings
        - DNS Settings Page
    - View Hosting Settings
        - Physical Hosting Configuration
        - Forwarding Configuration
    - Web Users Management
    - Protected Directories
        - Creating a Protected Directory
        - Changing a Protected Directory
        - Searching the Protected Directories List
        - Removing a Protected Directory
    - Manage the Domain SSL Certificate
    - Anonymous FTP
    - Databases

        - Searching the Database List
        - Creating a New Database
        - Editing an Existing Database
    - Domain User
        - Logging in
        - Changing the password

5.1 Introduction to Domain Usage

Domain User is also a Plesk server client. The only difference is that the Domain User is limited to a single domain and is not capable of managing matters that influence system's functioning (i.e.: limits and quotas for the domain). The Domain User is however able to manage mail accounts at the owned domain, create Certificate Signing Requests (CSR) or generate self-signed certificates. Other than that the Domain User is granted all the nice things that make life easier, such as interface, that the Client does. Accessing the PSA through the web browser (Netscape 4.x+ or Microsoft Internet Explorer 4.x+), you can:

- View settings and preferences for the domain
- Change your Control Panel password
- Manage mail accounts
- Create CSR's or self-signed certificates and/or install SSL certificates (IP-based hosting only)
- Create Web Users
- Create Protected Directories

PSA warns you of any consequences before allowing you to execute a major change.

5.2 Domain Administration Page

A domain is a virtual address on the Internet for any organization or entity. To an Internet user, a domain appears as space on one server, regardless of its implementation. Domains are identified by their familiar Internet URL (uniform resource locator) addresses. Syntactically, a domain name is a string of names or words separated by periods. For example, www.plesk.com is the name of the domain where Plesk's information resides on its servers.

A domain belongs to a user. For example, John Smith may be a programmer whose domain is aceprogrammer.com. In the same respect, the ABCDE, Inc. company may own a domain by the name of abcde.com. The Plesk system administrator at your Internet service provider's organization must create your domain. However, you can remotely administer your domain once the account is established.

From the *Domain Administration page*, you can manage several aspects of your domain, including:

- View the Domain Preferences
- Access the Domain Report
- Manage Mail for the Domain
- View DNS settings
- View Hosting settings
- Create Web Users
- Create Protected Directories
- Manage the Domain SSL Certificate
- View Anonymous FTP settings
- Manage Databases
- Change the Domain Level Control Panel password

View the Domain Preferences

The *Domain Preferences page* displays the preferences that the Plesk administrator or/and Client have set up for this domain. It also allows you to edit few parameters.

The parameters available for viewing from at this page are:

- **Disk Space Limit** – the amount of disk space allocated for this domain.

- **Maximum Mailboxes** - the maximum number of mail accounts allowed for creation at this domain.
- **Mailbox quota** – the limit set for the size of the mail accounts (mailboxes).
- **Maximum Mail Redirects** - the maximum number of mail allowed for setting up at this domain.
- **Maximum Mail Groups** - the maximum number of mail groups allowed for creation at this domain.
- **Maximum Autoresponders –** the maximum number of mail autoresponders allowed for setting up at this domain.
- **Maximum Web Users** – the maximum number of web users allowed for creation at this domain.
- **Maximum Databases** – the maximum number of databases allowed for creation at this domain.
- **Allow Scripting for Web Users** – enables the Web Users to download and execute scripts.
- **WebMail** – allows utilizing access to mailboxes via web-interface. If the option is provided, the mailbox can be accessed by means of a web-client , which is made available from the URL: webmail.<domain.name>

The following parameters you are able to set up:

- For **Mail sent to non-existent users**, you are able to select either a mail bounce message to return to the sender, or a catch-all email address to which the messages are sent.
- The **WWW prefix** checkbox determines whether the given domain will require the www prefix in order to be accessed.

To adjust the settings, follow these steps:

1. From the *Client Home page*, click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.
2. Click the **PREFERENCES** button to access the *Domain Preferences page*.
3. To utilize a mail bounce message, select the radio button for **Bounce with phrase** and enter the text that the mail bounce message is to contain.
4. To utilize a catch-all email address, select the radio button for **Catch to address** and enter the appropriate email address.
5. Check or uncheck the **WWW prefix** checkbox to determine whether the given domain will allow the www prefix to be used to access the domain. If the box is checked, Internet users will be able to access a domain (i.e. domain.bogus) by

utilizing either the domain name itself or the domain with the 'www' prefix. If the box is unchecked it will not be accessible with the 'www' prefix (i.e. www.domain.bogus).

6. The **UPDATE** button is used to submit any and all changes.
7. The **UP LEVEL** button returns you to the *Domain Administration page*.

NOTE: Selecting **UP LEVEL** without selecting **UPDATE** will cancel all changes.

Accessing the Domain Report

PSA keeps a summary of pertinent data relating to all of your domains. You can view this information at any time. At the top of the *Report page*, the domain being reported on is listed in boldface. The domain report includes the following information:

- Domain owner (client)
- Domain status
- Creation date
- Hosting type
- Virtual host type
- IP Address
- FTP Login
- FTP Password
- Disk space limit
- Real disk space
- Traffic
- Real Traffic
- FrontPage support
- SSI support
- PHP support
- CGI support
- mod_perl support
- Apache ASP support

- SSL support
- Web statistics
- Web users
- Apache error docs
- Anonymous FTP
- Mailboxes
- Redirects
- Mail Groups
- Autoresponders
- Domain user
- Databases

To access the domain report, follow these steps:

1. Click the **REPORT** button at the *Domain Administration page* to see the domain's data and statistics.
2. From this screen, you can do several things:
    - You can send the report as email. You may need to send this report to your administrator. Email the report by clicking **SEND AS E-MAIL**. Or, enter a different email address to send the report to another recipient.
    - You can access graphical site statistics for the domain by selecting the **WEBALIZER** option. This opens a separate window where you will see the site statistics for the given domain. It should be noted that Webalizer, by default, is set to update statistics for the domain once every 24 hours. If you attempt to access Webalizer before it has operated its first update you will receive a notice that Webalizer is either not running or has not yet been started.
    - To print a copy of the report, select **File/Print** in your browser and a paper copy of the report will print.
    - To return to the domain record, click **UP LEVEL** to close the report and to return to the *Domain Administration page*.

Managing Mail

PSA allows you to perform several email administration functions. PSA uses the qmail system to help you set up email accounts and services. Your email system is protected against spamming, because qmail does not allow the mail server to be remotely accessed.

You can create and manage email boxes for individuals or customers within your domain. Email management functionality includes:

- Create, edit or delete email boxes and edit individual mailbox quotas.
- Redirect or forward messages from one email address to another email address
- Create, edit or delete email groups (several individual accounts grouped together under one email address for convenient multi-copy messaging).
- Create, edit, or delete email autoresponders (automatic reply to email sent to the given mail name)

Mail Names page

When you create email accounts for domain users, you are creating email boxes, which will be accessible via POP3 or IMAP protocols. Mailbox creation is as easy as keying in a name and password. Follow these steps to manage mail names:

1. Click the **MAIL** button at the *Domain Administration page*. The *Mail Names Management page* appears. From this page, users can:
    - Create a new mail name.
    - View a list of mail names currently existing under the specified domain. To the left of each domain name on the list there are four icons representing different mail account types. They are:
        - Mailbox (represented by the "mailbox" icon)
        - Redirects (represented by the "outgoing envelope" icon)
        - Mail groups (represented by the "people" icon)Mail
        - Autoresponders (represented by the “revolving envelope” icon)
    - Click on a specific mail name to access to the *Mail Name Properties Page* for that given name.
    - Search the mail names list for a certain pattern. It may help you in case you have a great number of mail names in the system and you need to work with a particular one. To search the list, type the pattern string in the text input field and click **SEARCH**.
    - Sort the list by various parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

- Delete mail names. To remove one or more mail names, check the checkboxes in the **Del** column of the mail names list corresponding to the mail names you wish to remove and click **REMOVE SELECTED**. The *Mail Names Removal page* appears. There you will need to either confirm the removal (check the checkbox and click **SUBMIT**) or **CANCEL** it.

2. To create a new mail name, click in the **Mail Name** text box provided and enter the desired name. Click **ADD** to submit this name. You then access the *Mail Name Properties page*, where you can adjust the Mail Name properties.

3. The new mail name appears on the mail names list.

NOTE: The four icons to the left of each mail name are faded (grayed out) when they are inactive. The icons appear in color when active. To change the activation settings, the user must click on a given mail name. The *Mail Name Properties page* displays. From here, the user can enable any of the features.

Manage Mail Name Properties

The *Mail Name Properties page* allows the client to activate any combination of mailboxes, mail redirects, and mail groups for a given mail name.

1. Click the **MAIL** button at the *Domain Administration page*. The *Mail Names page* appears.

2. In the **Mail names list**, click on the name you want to edit. You then access the *Mail Name Properties page*.

3. The mail name is listed at the top of the page. To change the mail name, click in the name field, change the name, and click **UPDATE**.

NOTE: From the *Mail Name Properties page*, you can also enable and set up:

- Mailbox Accounts and Quotas
- Mail Redirects
- Mail Groups
- Mail Autoresponders

4. When you are finished editing mail name properties for the domain, click **UP LEVEL** to return to the *Mail Names page*.

Manage Mailbox Accounts

You can set up a mailbox and password for your mail name. This mailbox will be accessible using either POP3 or IMAP protocol.

NOTE: An administrator or/and Client can limit the number of mailboxes a Domain User can have for a given domain.

To create a mailbox for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. Click in the check box provided next to **Mailbox**.
2. When enabling a mailbox for the first time for a mail name account, you must enter a password.
3. The **Old Password** will say "NONE" if you have yet to enter a password. Once it is entered, the password cannot be viewed from this screen.
4. To enter a password, click in the **New Password** text box and enter the selected password.
5. To properly update the password, you must re-enter the password in the **Confirm Password** text box.
6. To set up the mailbox quota, select the **Default for domain** radio button to set the limit to the maximum available in the given domain, or select **Enter size** and enter the quota you wish to set, in KiloBytes, for the given mailbox. Note that this limit may not exceed the default set for the domain.
7. Once you have enabled the mailbox, entered the passwords and set up mailbox quota, click **UPDATE** to submit the information.
8. To change a password, simply re-enter the new password in the **New Password** text box, re-enter this password in the **Confirm** text box, and click **UPDATE**.

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

Manage Mail Redirects

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

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

NOTE: The administrator has the ability to limit the number of mail redirects that the client can create for a given domain.

In order to create enable a mail redirect for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. Click in the check box provided next to **Redirects**.

2. In the text field to the right, enter the appropriate address to which to forward mail sent to this mail name.

3. To change the redirect address for a given mail name, click on the existing entry in the **Redirects** box and change it to the new address.

4. Click the **UPDATE** button to enter these changes.

NOTE: Once enabled, the redirects icon on the *Mail Names page* appears in color.

Manage Mail Groups

A mail group is a list of several email accounts that are grouped together under one email address for convenient multi-copy messaging. For example, if you want to send the same message to 5 people in the programming department, you can create a "Programming" email group that includes the individual email addresses for all 5 staff members. So, when someone sends a message to the Programming email group, he/she only types and sends one message. Copies of the message are emailed to all 5 individuals. By using mail groups, the sender does not need to know each individual's email address, just the group name. In this way, mail groups save time.

NOTE: The administrator has the ability to limit the number of mail groups that the client can create for a given domain.

To create a mail group for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. Click in the checkbox provided next to **Mail Groups**.

2. To create a new mail group, ensure the box is checked, then click the **ADD** button.

3. The **Add Mail Groups** box appears.

   NOTE: Group members can consist of either external mail addresses (those not belonging to this domain) or accounts existing within the domain.

4. To add an external mail address to a Mail Group, fill in the correct address in the **enter external recipient mail** text box, and click **ADD**.

5. To add an existing account from the same domain, click on the desired address in the **Select registered users** list, and click **ADD**.

6. The selected addresses will appear in the box to the right of the mail groups checkbox on the *Mail Name Properties page*.

7. To delete one or more group members, highlight the selected group member in the box to the left of the mail group check box. Click the **REMOVE** button.

8. A warning will appear. Click **OK** to confirm that you want to delete the address from the mail group.

9. After completing your changes, click **UPDATE** to submit all changes.

NOTE: Once enabled, the mail groups icon on the *Mail Names page* appears in color.

Manage Mail Autoresponders

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

In order to enable and set up a mail group for a given mail name, from the *Mail Name Properties page*, follow these steps:

1. To first enable autoresponders for a mail name account, click in the checkbox provided next to **Mail autoresponders.** When the check appears, autoresponders are enabled for the mail name. If you click again, it will uncheck the box, and autoresponders will be disabled.
2. For the Autoresponder feature you have the option to include file attachments. To include a file to be selectable within the set up of autoresponders for the given mail name, use the **Browse** button to search for and select the desired file(s). (File sizes should be limited to no more than 1MB.)
3. Click the **SEND FILE** button. The attachments will then appear in the **Repository.**
4. These files will be available for any autoresponders that are set up for the given mail name. To delete one or more files highlight the desired file(s) and click the **REMOVE** button. A warning will appear prior to deleting the selected file(s).
5. To add a new mail autoresponder, click the **ADD** button.
6. A pop-up screen prompts you to enter a name for the autoresponder. Enter the desired identification name, and click **OK** to submit.
7. The *Edit Mail Autoresponder page* appears.
    - The selected autoresponder name is listed for the given mail name account. You can click in the text box where the autoresponder name is listed, and edit the name. Click **UPDATE** to submit.
    - The ON/OFF status for the autoresponder is shown. **[ON]** indicates that the autoresponder is on. **[X]** indicates that the autoresponder is off. You can adjust this setting by clicking the **ON/OFF** button. This status icon also appears on the autoresponders list on the *Mail Names Properties page*.
    - Beneath the Request text input box, you can determine whether an autoresponder responds to specific text found within either the subject line or body of the incoming email, or if it responds to ALL incoming requests
    - To set up the autoresponder to always respond, regardless of the contained text, click the bottom radio button for **always respond**.

- Using the **Request text** input box and radio buttons, you can set up the autoresponder to send an auto response when an incoming request contains defined text in its subject line or body.
- Click the **in the subject** radio button to respond to specific text in the subject of the request, or click the **in the body** radio button to respond to specific text in the body of the request.
- You can select a specific subject to appear in your autoresponder using the **Answer with subject** optoin. To simply respond with the same subject as was received from the incoming request select the radio button for the default setting. To specify a specific subject line select the radio button beside the text box and enter the desired text.
- You can enter text to be included in the autoresponder in the **Answer text** field.
- Using the **ADD** and **REMOVE** buttons, you can attach files to be included in the autoresponder. These files must be uploaded into the **Repository** on the *Mail Names Properties page*. Select the uploaded file from the **Attach files** list, and use the **ADD** button to attach the file to the autoresponder. Click **REMOVE** to remove a file.
- You can specify the frequency at which the autoresponder responds to the same unique address, after receiving multiple emails from it. By clicking in the appropriate radio button next to **Reply To Unique Email Address**, you can set the autoresponder to **always** respond, to respond **once**, or to respond once per a specified number of **days**. The default setting is to respond once in one day to unique mail addresses. It is highly recommended that you leave this setting, or set to respond once in a given number of days. Selecting always respond can potentially overload your mail server. If the days value is defined as "0", then the autoresponder will respond each time a request is received.
- You can define the number of unique addresses that the autoresponder will remember. Enter the desired number in the **Store up to:** field.
- This memory enables the system to implement the answer-frequency and respond-once functionality. In the event of extremely high mail volume, to protect server performance, you can limit the address memory of the system database.
- To specify an email address to which incoming requests are forwarded, enter the new email in the **Forward request to e-mail** field. Email requests meeting the properties established on this page will be forwarded to this alternate email address.
- Click the **UPDATE** button to submit all changes.

View DNS Settings

Through PSA, a Domain User can view the DNS settings for the owned domain set by the Administrator or the Client.

DNS Settings Page
There are five types of accessible DNS records:

A = Address - This record is used to translate host names to IP addresses.
CNAME = Canonical Name - Used to create additional host names, or aliases, for hosts in a domain.
NS = Name Server - Defines an association between a given domain name and the name servers that store information for that domain. One domain can be associated with any number of name servers.
MX = Mail Exchange - Defines the location of where mail should be delivered for the domain.
PTR = Pointer - Defines the IP address and host name of individual hosts in the domain. Translates IP addresses into host names.

You can access the DNS Settings page by clicking the **DNS** button at the *Domain Administration page*.

View Hosting Settings

You may have hosting privileges established in your domain so that you can provide various Internet services (e.g. software applications, a forwarding address, and FTP transfers). PSA allows three different types of hosting services:

- **Physical Hosting** - This is the most common type of hosting service, creating a virtual host (disk space on the local server) for the client. The client controls and publishes his own website without having to purchase a server and dedicated communication lines.

- **Standard Forwarding** - With this type of forwarding, all requests to the domain are forwarded by your server to another Internet address (no virtual server is created). When an end user searches the Internet for the client's domain, he is routed to another URL, and the address in his browser window changes to the new URL. This may be confusing to the end user.

- **Frame Forwarding** - All requests to this domain are forwarded to another Internet address (no virtual server is created). But with this type of forwarding, the end user sees the client's domain name in his browser, not the forwarding address. PSA uses frames to "trick" the browser into displaying the correct domain name. The problem with frame forwarding is that some search engines do not index frame pages and some browsers do not support frames.

The system administrator has already performed all the technical system administration for hosting services relating to your domain; however, the type of hosting service set up for your domain determines the extent to which you can manage your hosting parameters. If you have physical hosting, you can use FTP software to access your hosting directions. Additionally, you can change the FTP password. If frame or standard forward hosting is set for this domain, than you can change (or toggle between these two types) forwarding for the given domain.

Follow these steps to administer your hosting services:

1. Click the **HOSTING** button at the *Domain Administration page*.
2. If you have a forwarding hosting set up for you, a page with a choice of types of hosting appears. Choose the type and click **NEXT** to proceed.
3. If the type of hosting is physical then you will be taken directly to the Physical *Hosting Configuration page*.

Physical Hosting Configuration

There are several physical hosting services for your domain. They are configurable only by the Administrator or the Client:

- FTP services. You may want to change the password occasionally for security purposes.
- FrontPage support
- SSI
- PHP
- CGI
- mod_perl
- Apache ASP
- SSL
- Web statistics
- Apache ErrorDocs

Forwarding Configuration

If you have either of the two forwarding options defined for your hosting services, standard or frame, then you can change between the two types of forwarding. Also, you can edit the URL to which domain transactions are re-directed or forwarded.

1. To change the type of forwarding you have, from the *Hosting page*, click on the type you want to change.

   NOTE: Confirm that you really need to change the type of forwarding before actually changing it. Only a Plesk administrator can change a forward hosting account to physical hosting. A Domain User cannot make this change.

2. Click **NEXT** to access the URL page.

3. To change the forwarding address, click in the **URL** text box and enter or edit an Internet address to which you wish to re-direct all domain traffic.

4. Click **UPDATE** to submit changes.

Web Users Management

A web user is a user account within Apache. It is used to define locations for personalized web pages with individual FTP access. The result of creating a web user is a subdirectory within your domain (e.g. domain.com/~webuser).

A list of all of the web users within a given domain will appear on the main *Web Users page*. At this page you can:

- Select any web user name to edit the web user password and/or to add or remove different scripting options.
- Search the web users' list for a certain pattern. It may help you in case you have a great number of web users in the system and you need to work with a particular one. To search the list, type the pattern string in the text input field and click **SEARCH**.
- Sort the list by various parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

To create a new web user:

1. Click the **WEB USERS** button at the *Domain Administration page*. The *Web Users page* appears.

2. To add a web user, enter the **Web User name** in the text box provided next to **Web user name:** and click **ADD**.

3. You are taken to the *Web User Password Entry Page*, where you must enter and confirm the password for your new web user and select from the available scripting options for the given domain (availability of scripting options is set in the Domain Preferences). To do this, enter a password in the **New password** text box, and then re-enter it in the **Confirm password** text box. Then select from the available scripting options if applicable. Once you have completed all entries, click on **UPDATE** to enter the information. Selecting **UP LEVEL** will return you to the *Web Users page* without assigning a password or scripting capabilities to the given web user. Although the directory will be created, it will not be accessible via FTP using the web user name.

4. As you create web users, the user names appear on the *Web User Management page* in the web user list.

5. To change web user passwords or edit scripting options, click on the user name in the web user list. This takes you to the *New Password page*.

6. When you are done, click **UP LEVEL** to return to the *Domain Administration page*.

To remove one or more web users, check the checkboxes in the **Del** column of the web users' list corresponding to the web users you wish to remove and click **REMOVE SELECTED**. The *Domain Removal page* appears. There you will need to either confirm the removal (check the checkbox and click **SUBMIT**) or **CANCEL** it.

Important Notes on web users:

- For security purposes, the password must be between 5 and 14 characters and cannot contain the user name.
- Each web user creates a system account within Apache; therefore, you cannot have two web users with identical names on the same server.
- New web users can access the directory using FTP software by entering the domain name under which the web user account was created and using the appropriate web user name and password.
- Your administrator CAN limit the number of web users you can create. You will receive a warning if you try to exceed this number, and will not be able to do so.

Protected Directories

This feature is active if virtual hosting (physical hosting account) has been configured for your domain. It creates secure directories in your virtual domain, in which to place documents. Secure directories are recommended to ensure security of confidential and private information. It is possible to create directories under either the standard virtual host accessible via http protocol, or if applicable for the given domain, under the SSL virtual host accessible via https protocol. Icons are used next to each directory name in the directory list to define which virtual host type (SSL or non-SSL) the directory resides within. An open lock depicts non-SSL; a closed lock depicts SSL.

Creating a Protected Directory

Follow these steps to create secure directories for the domain:

1. Click the **DIRECTORIES** button from the *Domain Administration page*. The *Protected Directory Management page* appears.

2. To create a new directory, click the **ADD** button.

3. This takes you to the *Protected Directory Control page*. Enter the name of the protected directory you wish to create in the **Protected Directory** field provided.

4. For **Directory Location:** you can choose either a non-SSL or SSL secure directory. To choose a non-SSL directory, click in the radio button next to **Non-SSL**. To choose SSL security for the directory, click in the radio button next to **SSL**.

5. If the directory has SSL enabled, it will appear in the Protected Directory list with a gray **Lock** icon beside it. If the directory is non-SSL, a gold **Unlocked** icon will appear next to the directory name in the directory list.

6. Click in the **Header Text** text box. When a user tries to access the protected directory, the text in this box displays as the Realm they are entering. In this text box, enter the header text.

7. To add a new user, under **Protected Directory Users** click in the **New User:** text box**,** and write the name of the directory user.

8. Click the **ADD** button.

9. You are taken to the directory user password screen. Here you must enter your new password in the **New Password** text box, and then enter it again in the **Confirm password** text box.

10. Click the **UPDATE** button to submit. You will return to the Protected Directory Control page. The new user will appear in the Protected Directory Users list. Clicking **UP LEVEL** will return to the *Protected Directory Control page* without creating a password for the given user. Although the user is created no access to the directory will be granted until a password is created for the user.

11. To remove existing directory users select the users that you wish to remove using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the directory users.

12. To access a directory user in order to edit the user password, click on the user name in the list, and you will again be taken to the directory user password screen. Here you can edit the password.

13. Select **UPDATE** to submit your changes and return to the *Protected Directory Control page.*

14. Click **UP LEVEL** to return to the *Protected Directory Management page* without saving any changes.

Changing a Protected Directory

You can edit a protected directory definition to:

- Add a user
- Change a password
- Delete a user

- Rename the directory
- Change header text
- Change the SSL status

Follow these steps to edit protected directories:

1. From the *Client Home page*, click the domain name that you want to work with from the list provided. The *Domain Administration page* appears.
2. Click the **DIRECTORIES** button. The *Protected Directory Management page* appears.
3. Click on any directory from the list that you wish to change.
4. You will be taken to the *Protected Directory Control page.*
5. From here, you can edit the directory by following the same steps outlined above, in the **Creating a Protected Directory** section.
6. Click **UPDATE** to complete all changes to the system and to return to the *Protected Directory List page*.

Searching the Protected Directories List

PSA allows you to search the Protected Directory List for a certain pattern. It may help you in case you have a great number of directories in the system and you need to work with a particular one. To search in the list:

- Select the input field and type in the pattern string.
- Click the **SEARCH** button.
- If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Protected Directory List.
- If no matches were found it will be so stated.
- The button **SHOW ALL** will revert to displaying the whole list of domains.

There is also another way to ease the process of working with a large list of directories. An option of sorting the list by several various parameters is made available to you. You can sort the list by several parameters. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Removing a Protected Directory

To remove one or more directories, follow these steps:

1. Check the checkboxes in the **Del** column of the Protected Directories List corresponding to the directories you wish to remove.

2. Click on **REMOVE SELECTED**. The *Protected Directory Removal page* appears.

3. For every directory you chose to remove the name of the directory and the names of this directory users will be displayed.

4. If you are certain that the displayed information is correct and wish to proceed with deleting, check the "Yes, I have read, understood, and agree to remove protect from these domains" checkbox. Then click **SUBMIT**. If you decide to not delete these directories or wish to modify the list of directories chosen for deletion, click the **CANCEL** button.

Both buttons will return you to the *Protected Directory Management page*, one committing the changes, the other one leaving everything unchanged.

NOTE: Deleting a protected directory in PSA does not delete the directory off the server. It simply takes the protected status off the directory. Meaning that the directory and its contents will now be reachable via the Internet without the need for login and password.

Manage the Domain SSL Certificate

PSA enables you to upload a Secure Socket Layer (SSL) Certificate, generate a Certificate Signing Request (CSR), generate a Self-signed Certificate, and/or purchase a SSL certificate through a registered certificate authority. Each certificate represents a set of rules used when exchanging encrypted information between two computers. Certificates establish secure communications; this is especially important when handling e-commerce transactions and other private transmittals. Only authorized users can access and read an encrypted data stream.

Notes on Certificates:

- In order to use SSL certificates for a given domain, the domain MUST be set-up for IP-Based hosting.
- When an IP-based hosting account is created with SSL support, a default SSL certificate is uploaded automatically. However, this certificate will not be recognized by a browser as one that is signed by a certificate signing authority.
- The default SSL certificate can be replaced by either a self-signed certificate or one signed by a recognized certificate-signing authority. The self-signed certificate is valid and secure, but many clients prefer to have a certificate signed by a known Certificate Signing Authority.
- If using a SSL certificate issued by a certificate authority other than Thawte or Verisign, a rootchain certificate is required to appropriately identify and authenticate the certificate authority that has issued your SSL certificate.
- If the given domain has the **www** prefix enabled, you must set-up your CSR or self-signed certificate with the **www** prefix included. If you do not, you will receive a warning message when trying to access the domain with the **www** prefix.

- Remember to enter your certificate information in PEM format. PEM format means that the RSA Private Key text must be followed by the Certificate text.
- All certificates are located in the ../vhosts/<domain name>/cert/httpsd.pem file. Where this directory reads <domain name> , you must enter the domain name for which the certificate was created.

To generate a self-signed certificate or a certificate-signing request, follow these steps:

1. If you have established an IP based hosting account with SSL enabled, the **CERTIFICATE** button at the *Domain Administration page* will be enabled.
2. Click the **CERTIFICATE** button. The *SSL certificate setup page* appears.
3. The **Certificate Information:** section lists information needed for a certificate Request, or a Self-Signed certificate.
4. The Bits selection allows you to choose the level of encryption of your SSL certificate. Select the appropriate number from the drop down box next to **Bits:.**
5. To enter the information into the provided text input fields (**State or Province**, **Locality**, **Organization Name** and **Organization Unit Name** (optional)) click in the text boxes and enter the appropriate name.
6. To enter the Domain Name for the certificate, click in the text box next to **Domain Name:** and enter the appropriate domain.
7. The domain name is a required field. This will be the only domain name that can be used to access the Control Panel without receiving a certificate warning in the browser. The expected format is www.domainname.com or domainname.com.
8. Click on either the **SELF-SIGNED** or **REQUEST** button.
9. Clicking **SELF-SIGNED** results in your certificate being automatically generated and installed.
10. Selecting **REQUEST** results in the sending of a certificate-signing request (CSR) to the email address you provided in the fields discussed above. When a CSR (certificate signing request) is generated there are two different text sections, the RSA Private Key and the Certificate Request. **DO NOT LOSE YOUR RSA PRIVATE KEY. YOU WILL NEED THIS DURING THE CERTIFICATE INSTALLATION PROCESS. LOSING IT IS LIKELY TO RESULT IN THE NEED TO PURCHASE ANOTHER CERTIFICATE.**
11. When you are satisfied that the SSL certificate has been generated or the SSL certificate request has been correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

To upload a file containing the certificate authorized by the Certificate Signing Authority:

1. Click the **CERTIFICATE** button at the *Domain Administration page*. The *SSL Certificate page* appears.

2. If you wish to upload a Certificate File authorized by the Certificate Signing Authority, click the **BROWSE…** button under the **Upload previously bought Certificate File (without private key)** section to select the file (the file must be in .txt format)

3. Then, click **SEND FILE** to copy the certificate to the server.

To upload a new certificate:

1. Click the **CERTIFICATE** button from the *Domain Administration page*. The *SSL Certificate page* appears.

2. If you wish to upload a certificate file from a local computer, under the **Uploading Certificate File** section, click the **BROWSE…** button to select the file (the file must be in .txt format).

3. Then, click **SEND FILE** to copy the certificate to the server. Or, if you want to type in the text of the certificate without downloading a specific file, click in the text box and enter and paste the certificate information.

4. Click **SEND TEXT** to implement the text on the server.

   NOTE: Ensure that the private key text block is included along with the SSL certificate text block when using the **SEND FILE** or **SEND TEXT** options.

   EXAMPLE FORMAT:

   ```
   -----BEGIN RSA PRIVATE KEY-----

   [[ECRYPTED BLOCK OF TEXT]]

   -----END RSA PRIVATE KEY-----

   -----BEGIN CERTIFICATE-----

   [[ECRYPTED BLOCK OF TEXT]]

   -----END CERTIFICATE-----
   ```

5. When you download the certificate to the server, PSA checks for errors. If an error is detected, PSA restores the old version of the SSL certificate, and PSA warns you to update the certificate. At this point, you can try again to enter text or to download the certificate file.

6. When you are satisfied that the SSL certificate is correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

If you are using a certificate that has been signed by an authority other than Thawte or Verisign then it is likely that this will require the use of a rootchain, or CA, certificate. To install a rootchain certificate for the domain:

1. Click the **CERTIFICATE** button at the *Domain Administration page*. The *SSL Certificate setup page* appears.
2. The icon next to **Use rootchain certificate for this domain** appears on this page.
3. If the icon is **[ON]** then the rootchain certificate will be enabled for this domain. If the icon is **[X]** this function will be disabled.
4. To change the status of the rootchain certificate, click the **ON/OFF** button.
5. To upload your rootchain certificate, first make sure that it has been saved on your local machine or network. Use the **Browse** button to search for and select the appropriate rootchain certificate file.
6. Then click the **SEND FILE** button. This will upload your rootchain certificate to the server to assure proper authentication of the certificate authority.
7. When you are satisfied that the rootchain certificate is correctly implemented, click **UP LEVEL** to return to the *Domain Administration page*.

Anonymous FTP

Within PSA there can be an Anonymous FTP access set up by the Client or the Administrator, for IP-based virtual host only though. Anonymous FTP is used to allow an open, yet controlled, environment for visitors to the domain to download and/or upload files to and from the domain account. Users will be able to log into ftp.<domain name> with the standard anonymous user name and any password. PSA allows the setup and limitation of incoming file space, connected users, and bandwidth usage throttling. Administrators should take care when allowing the use of anonymous FTP and be sure to use all the limitation capabilities within the interface wisely. If setup with excessive limits, it could lead to problems with server resources as well as excessive bandwidth usage. As the Domain User you can view the status of Anonymous FTP for your domain. To do that, click the **ANONYMOUS FTP** button at the *Domain Administrator page*.

Databases

Within PSA there is the ability to create multiple mysql databases as well as multiple users within each database. Also, directly accessible via PSA, is a link to PhpMyAdmin, a PHP interface that abstracts mysql into a web-based administration tool, allowing you to sort, edit, and create tables within a given database. Database limits are set through

domain preferences and database disk usage is calculated within the domain's total allotted disk space.

Searching the Database List

PSA allows you to search the Database List for a certain pattern. It may help you in case you have a great number of databases in the system and you need to work with a particular one. To search in the Database List:

- Select the input field and type in the pattern string.
- Click the **SEARCH** button.
- If there were any items found matching the pattern string entered, they will all be displayed in the form of the reduced Database List.
- If no matches were found it will be so stated.
- The button **SHOW ALL** will revert to displaying the whole list of databases.

There is also another way to ease the process of working with a large list of databases. An option of sorting the list by several various parameters is made available to you. You can sort the Database List by **Type** and **Database Name**. To sort the list by a certain parameter in ascending or descending order, click on the name of the parameter. An arrow will appear indicating the order of sorting: down for descending order, up for ascending.

Creating a New Database

1. Click the **DATABASES** button at the *Domain Administration page*. The *Databases Feature Management page* appears.
2. To add a new database select the **Database name** field, enter the desired name, and select **ADD**. The *Database Editing page* appears.
3. To add database users to the newly created database enter the user name into **New user** text box and select **ADD**. The *Database User Management page* appears.
4. Enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the new user. Selecting **UP LEVEL** will ignore all entries and return to the *Database Editing page* making no changes.
5. Once you have completed the creation of the new database and its users select **UP LEVEL** to return to the *Database Feature Management page*.
6. To add further databases, follow the steps outlined in 1-5 above. To return to the *Domain Administration page* select **UP LEVEL**.

Editing an Existing Database

1. Click the **DATABASES** button at the *Domain Administration page*. The *Databases Feature Management page* appears.
2. Click on the database that you wish to edit. The *Database Editing page* appears.
3. To add database users to the selected database enter the user name into **New user** text box and select **ADD**. The *Database User Management page* appears.
4. Enter your new password in the **New Password** text box, and then enter it again in the **Confirm Password** text box. Select **UPDATE** to complete the creation of the new user. Selecting **UP LEVEL** will ignore all entries and return to the *Database Editing page* making no changes.
5. To edit the password of an existing database user, select the user from the database user list. The *Database User Management page* appears.
6. To delete existing database users select the users that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the selected users.
7. To access and/or edit database content you can do so using the **PHPMYADMIN** option. PhpMyAdmin provides a web-based graphical interface for mysql. This can be used to make content edits to your existing databases.
8. Once you have completed all edits of the database and its users select **UP LEVEL** to return to the *Database Feature Management page*.
9. To delete existing databases select the users that you wish to delete using the checkboxes on the right of the screen and select **REMOVE SELECTED**. You will be asked for confirmation prior to final deletion of the selected users.
10. To edit further databases, follow the steps outlined in 1-9 above. To return to the *Domain Administration page* select **UP LEVEL**.

Domain User

Logging in

Access to the control panel for the database user is done using https://<domain name>:8443. The control login will be the domain name, and the password will be whatever is set through the control panel.

Changing the password

As the Domain User you can change the password that you use to log in to PSA. To do that, click the **DOMAIN USER** button. The *Domain User Properties page* appears.

There, to change password, enter the new password into the **Password** input field and confirm it in **Confirm password** input field.

Appendices

Appendix I – Reconfigurator Utility

Reconfigurator Manual Information

During the process of installing PSA the Administrator selects the IP-address to be used for name-based virtual hosts. This address is maintained strictly fixed and the Administrator is unable to change it by means of the Control Panel. The Reconfigurator utility serves the purpose of changing these parameters after an installation has already been completed. Also Reconfigurator allows the user to change the Administrator's e-mail address as well as the host name and domain.

Reconfigurator is implemented in the form of a shell script. It is located in the directory /usr/local/psa/bin . The name of the Reconfigurator utility file is reconfigurator.sh

The following are the functions performed by Reconfigurator:
1. System check
2. Configuration parameters request
3. Set up of particular services (mysql, admin, webmail, apache, qmail, named)

1) At the first stage system checks are performed:
   - has the Reconfigurator been started with root permissions?
   - does the system have all the programs necessary for the installation?
   - are shadow passwords used (for Linux)?
   - etc.

2) Then Reconfigurator requests the Administrator to enter certain parameters needed to further configure the system:
   - host name and domain
   - Admin email
   - IP address for name-based hosting

NOTE: If the specified IP address is already used by anonymous ftp for some domain Reconfigurator will issue a warning and exit without making any changes. In order to be able to use this IP address, you will have to remove it from the domain that is using it (specified by Reconfigurator) for anonymous ftp via the Control Panel.

3) Particular services are set up at this stage:
   - Host name and domain - added to the database and entered into the configuration files for each service instead of the previous values
   - Admin email - added to the database and entered into the apache server's configuration files in place of the ServerAdmin directives values
   - IP address - added to the database and used for Name-based virtual hosts. If there was an IP-based hosting on this IP before, it also becomes Name-based. The DNS(named) service is reconfigured accordingly.

Appendix II – Glossary of Terminology

Apache
Apache is an open source Web server that is distributed free. Apache runs on Unix-based operating systems (including Linux and Solaris) and Windows 95/98/NT. Apache was originally based on the NCSA server, but is now an independent product, supported by the nonprofit Apache Software Foundation.

Browser
A browser is a software application that lets you access information on the Internet. Browsers can read HTML and send HTTP or FTP requests for services on the Internet. Browsers are usually associated with the World Wide Web portion of the Internet.

BSD/OS
BSD/OS is an open source operating system from Berkeley Software Design, Inc. BSD, based on the Unix operating system, was developed for primary use on servers and is one of the most secure operating systems available. BSD is used by many Internet service providers to create some of today's most popular Internet sites.

BSDI
BSDI stands for Berkeley Software Design, Inc., a privately held company that supplies BSD/OS and networking software.

CGI
CGI, or the common gateway interface, provides a standardized method for Web servers to send a user request to an application and to receive information back for the user. For example, when you click on a URL link, the Web server sends the requested page to you. CGI is part of the HTTP protocol. CGI works in many different languages, and across several different platforms.

Client
A client is a company or individual requesting services from an Internet presence provider. A client is a customer of a Web hosting company, or a user of Internet services. In hardware terminology, a client is a computer system or a software package that

requests services or information from another application that resides across the network. Think of the client as your PC or workstation, through which you access programs and data across a network or the Internet, usually on a server. In very simple terms, a client is a user.

COMSAT Service Record
The comsat server is an older method of handling asynchronous mail notification. Comsat has been replaced by a mail variable in the operating system shell.

DAEMON
A daemon is a continually running program in Unix that handles service requests as they are received by a computer. The daemon sends service requests to other programs as needed. For example, every Web server has an HTTP daemon that receives user requests for services and information. Another example is the sendmail daemon that handles e-mail messages.

DNS
DNS, short for Domain Name Server, is a distributed database that maps names and IP addresses for computers using the Internet. DNS is a standardized system that identifies domain name servers.

Domain
A domain is a virtual address on the Internet for any organization or entity. Technically, a domain is a group of networked computers (servers) that represent an organization and provide network services. However, several domains could reside on one server, in dedicated space provided by a Web hosting service. To the Internet user, a domain appears as space on one server, regardless of the implementation. Domains are identified by their familiar Internet URL (uniform resource locator) addresses. For example, www.plesk.com is the name of the domain where Plesk information resides on its servers. Syntactically, a domain name is a string of names or words separated by periods. For example, a domain name such as: **hello.house.neighborhood.com** includes the names of:

- the host: hello
- the subdomain: house
- the network: neighborhood
- the organization type: com

Some high-level domain names include these organization types:

- arpa: ARPAnet (a Defense Department communications system that established the Internet)
- com: Commercial, for-profit organizations and businesses
- edu: Educational institutions
- gov: Government organizations

- int: International organizations
- mil: U. S.-based military
- net: Internet access providers
- org: Non-profit organizations
- 2-alphabetic characters: Countries outside the U. S., such as uk for the United Kingdom

FREEBSD
FreeBSD is a ported version of BSD/OS Unix for Intel-based personal computers. FreeBSD is an open source operating system.

FTP
FTP, or File Transfer Protocol, is a method used to transfer files to (upload) and from (download) a remote server. You can use the FTP command to:

- Copy a file from the Internet to your PC
- Move a file from your PC up to the Internet
- Rename an existing file
- Delete a file
- Update an existing file with more recent data

Gateway
A gateway is a combination of hardware and software allowing dissimilar systems to communicate by filtering data through standardized protocols. Think of a gateway as a translator that allows your PC to talk with other computers on the network.

GNU General Public License
The GNU General Public License, from the Free Software Foundation, Inc., is a license that guarantees complete freedom to users for sharing and changing freeware software.
Host
In a network, a host is usually a computer that stores software applications and data that may be accessed or retrieved by other users. But a host can be any addressable device on the network, not just a computer. The host provides services to other computers or users. An Internet Service Provider may also be referred to as a Web hosting company.

HTML
HTML, or HyperText Markup Language, is a standardized language for presenting information, graphics, and multimedia on the World Wide Web. HTML consists of hundreds of codes, tags, and symbols that define the type of information and how it should be displayed in a browser. HTML is universally understood on a wide variety of platforms.

HTTP
HTTP, or HyperText Transfer Protocol, is a standard for sharing World Wide Web files. HTTP lets you communicate across the Internet by carrying messages from your browser to a server.

IMAP
IMAP, or Internet Message Access Protocol, is a method for receiving e-mail messages from other Internet users on your local server. IMAP lets you see message headers before choosing and viewing the entire text of mail messages. You can selectively retrieve mail messages with IMAP. Compare IMAP to the POP and SMTP mail protocols.

Include Directive
Directive within Apache which allows the inclusion of customizations to the Apache configuration file, utilizing files external to the configuration file.

INETD
Inetd, or the Internet Services Daemon, is a program that runs when your server is booted and reads a configuration file (inetd conf) to identify Internet services that it monitors. Inetd replaces the need for several different daemons running at the same time, reducing the system load.

Internet Super Server
Internet Super Server is a system available from Berkeley Software Design, Inc. which includes the BSD/ OS operating system.

IP Address
An IP address (Internet Protocol address) is an internal number that identifies a host on the Internet or a network. IP numbers are invisible to end users, replaced in your user interface by the more familiar domain names and URLs.

Linux
Linux is a free operating system originally created by Linus Torvalds of Finland. Linux is based on the Unix operating system and includes features such as true multitasking, memory management, virtual memory, demand loading, networking, and shared libraries. Linux runs in protected mode and supports both 32-bit and 64-bit multitasking. Developed under the GNU General Public License, Linux is available free to everyone.

Mail Autoresponder
Mail autoresponders are automatic replies to email sent to a particular mail name. Autoresponders can include both a text message and attached files. This mail function is often used on mail accounts for individuals who are away for a certain period of time, or are unable to check their mail for any number of reasons.

Mail Group
Mail groups are used for sending e-mail to a group of people through one address rather than to each individual address. Mail groups save you time and effort in reaching several people at once; you only have to create one e-mail message to the group, rather than several identical messages to everyone.

Mail Redirect
Mail redirects are used to forward or redirect email from one POP3 mailbox to another email address. By creating an email redirect or alias, messages are sent to a different email box without the sender needing to know the new address. Email can be redirected to an address outside the domain.

Mod_Perl
Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use it for a vast number of automation tasks. Many CGI programs are written in Perl.

Mod_Throttle
This Apache module is intended to reduce the load on your server & bandwidth generated by popular virtual hosts, directories, locations, or users according to supported polices that decide when to delay or refuse requests. Also mod_throttle can track and throttle incoming connections by IP address or by authenticated remote user.

MySQL
SQL is a Structured Query Language that was created as a standardized method of defining, manipulating, and searching data in a database. It is currently the most commonly used database language. My SQL is a fast, easy-to-use, multi-user SQL database server in a standard client/server environment. MySQL handles graphics as well as text. MySQL is frequently implemented on Unix and Linux platforms and is available under a GNU General Public License. For more information, visit http://www.mysql.com.

Network
A network is a system of interconnected computers and peripheral devices (such as printers).

Packet
Data that is transported across the Internet is divided into small, manageable units called packets. Data packets can be sent more quickly and efficiently across a network than the full stream of data in a message or file.

PHP
PHP (originally meaning Personal Home Page) is a server-based HTML embedded scripting language that runs on multiple platforms, primarily on Linux servers. PHP accesses and manipulates data in a MySQL database, and helps you create dynamic Web pages. You write HTML and embed code in the HTML that performs a specific function.

The embedded code is the PHP portion of the script, identified in the HTML by special start and stop tags. A PHP file has an extension of .php or .php3 or phtml. All PHP code is executed on a server, unlike a language such as JavaScript that is executed on the client system. For more information, visit http://www.php3.org.

POP3
POP3, or Post Office Protocol Version 3, is a method used to receive electronic mail across the Internet, accommodating different mail software packages and systems. POP3 receives and holds all your e-mail on a server. You can then download all your messages when you connect to the mail server; you cannot selectively retrieve messages. Compare POP to the IMAP mail protocol.

Popper
Popper is an implementation of the Post Office Protocol server, running under Unix. Popper manages e-mail transmissions for Macintosh and MS-DOS computers.

Protected Directory
A directory is an organized collection of files and subdirectory folders on a computer. A protected directory is one that cannot be accessed by all public users; you must have access privileges to read information in a protected directory.

Qmail
Qmail is a secure and highly reliable e-mail message handling system. It replaces the sendmail daemon on Unix and Linux systems. Qmail is fast and uses little memory. Users can create their own mail lists, and system administration is minimal. Qmail uses the Simple Mail Transfer Protocol (SMTP) for message exchange with other systems.

Reboot
Rebooting simply means restarting a computer. You should not reboot a server that has users accessing it until you have informed the users that the server must be shut down temporarily. Sometimes, an emergency necessitates rebooting a server immediately, but it is not a recommended practice.

Red Hat
Red Hat, Inc. is a commercial company that markets open source operating systems and services. Red Hat Linux OS is their most popular product.

Secure HTTP
Secure HTTP (S-HTTP or HTTPS) is an encryption method uses to protect documents on the World Wide Web. An alternative to S-HTTP is an SSL certificate (or Secure Socket Layer) that secures an entire session, not just a document or a file. S-HTTP supports several different message encryption formats, and works with any communication between clients and servers.

Security
There are several different ways to control access to a computer or network, to protect proprietary data, and to maintain privacy. Security measures can be defined at several different levels (at the server level, on a directory, for an individual file, etc.) for optimum protection.

Sendmail
Sendmail is a Unix daemon (e.g., a program that stays active in the background until it is needed) that handles the transmittal of all e-mail messages on a server.

Server
A server is a computer system (a combination of hardware and software) that runs programs, stores files, directs traffic, and controls communications on a network or the Internet. Clients (also called users or workstations) access a server for specific information and services.

Skeleton Directory
In PSA, this term refers to a set of directories and files that get copied into a newly created virtual host directory structure at the time the virtual host is created. It may be used to have a set of CGI scripts included with every account created in PSA. It is very useful if you are looking to have a more informative, customized welcoming index.html page, and it is also helpful if you have anything else that needs to be included by default within the directories of the virtual host.

Slackware
Slackware Linux is a complete 32-bit multitasking "UNIX-like" system. Slackware complies with the published Linux standards, such as the Linux File System Standard.

SMTP
SMTP, or Simple Mail Transfer Protocol, is a standard for transmitting mail messages across different computers on a TCP/IP network. SMTP can only be used when both the mail sender and receiver are ready. If the destination PC is not ready, a "post office" must temporarily store the mail. In that case, a post office protocol such as IMAP or POP is used to retrieve the mail.

Solaris
Solaris is a Unix-based operating system available from Sun Microsystems, Inc.

SSI
SSI stands for "server-side include," a type of HTML comment that directs the webserver to dynamically generate data for the Web page whenever information is requested. SSIs can also be used to execute programs and insert the results; therefore they represent a powerful tool for web developers.

SSL
SSL stands for Secure Socket Layer, and is a set of rules used for exchanging information between two computer devices using a public encryption system. SSL establishes secure communications between servers and clients. SSL provides a safe and authenticated method of handling e-commerce transactions. Only authorized users can access and read an SSL-encrypted data stream. An alternative to SSL is Secure HTTP (S-HTTP), used to encrypt World Wide Web documents (rather than securing an entire session, as does SSL).

SSL Certificate
An SSL certificate is an electronic key that encrypts transmissions between two computers on a public network, providing privacy and security to the session. Think of an SSL certificate as an electronic ID card for an individual or a computer service. An SSL certificate confirms that a message that you receive actually did come from the person identified. The certificate key is issued by a third party. SSL certificates are used for secure e-commerce communications, protecting information such as credit card numbers and personal data. You can generate an SSL certificate with a utility such as SSLeay. Then, submit it to a certificate authority such as Equifax Secure (www.equifaxsecure.com).

SSLEAY
SSLeay implements the Netscape's Secure Socket Layer, the encryption protocol for the Netscape Secure Server and the Netscape Navigator browser. It is a free software package which is recognized as one of the leading standards in Internet security. SSLeay uses asymmetric cryptography, based on a Public Key Infrastructure model of an SSL certificate and private key pair.

T1
T1 is a network communications line or cable that transmits data at a very high rate of speed.

Tarball
Tar is a Unix command (meaning "Tape Archive" and originally referring to a backup that could be retrieved from a tape drive) that creates one archive file from several different files. Tar files are not compressed, but they are collected in one large file for convenient downloading or transferring. "Tarball" is a slang term for the files that are "stuck" together in a "ball of tar" by the tar command.

TCP
TCP stands for Transmission Control Protocol, and is the primary data transport protocol on the Internet. TCP transmissions are fast, reliable, and full-duplexed.

TCP/IP
Transmission Control Protocol/Internet Protocol, commonly known as TCP/IP, is a data transmission protocol that was developed by ARPA, the Advanced Research Projects Agency. ARPA is the founding organization of the Internet.

Telnet
Telnet is a method of accessing another remote computer. You can only access the other computer if you have permission to do so. Telnet differs from other protocols that simply request information from a host computer, because it actually logs you on to the remote computer as a user.

TurboLinux
TurboLinux is a Linux-based Operating System. TurboLinux makes a suite of high-performance Linux products for the workstation and server markets.

Unix
Unix is an operating system that was originally developed by Ken Thompson and Dennis Ritchie at Bell Labs in 1969. It was the first operating system written in the C programming language, and offered true interactive time-sharing. Since then, Unix has evolved into a freeware product; many versions of Unix are offered by several companies and organizations. Unix is considered the first open standard operating system. Linux is a derivative of Unix, and is also available as freeware.

URL
A URL is a Uniform Resource Locator used to identify an organization or domain on the Internet. URLs are standardized names that are typically found on the World Wide Web portion of the Internet. URL addresses identify domains on the network. Read about Domains for more detail.

User
Simply put, a user is a client. In hardware terminology, a client is the PC that you use to access information from other computers (usually servers) on the Internet or network.

Web User
A web user is a user account within Apache that is used to define locations for personalized web pages with individual FTP access.

Workstation
A workstation is a user or client that accesses information from other computers (usually servers) on a network.