Users Manual

4451 Brookfield Corporate Drive
Chantilly, Virginia 20151
Phone: 703.815.5670
Fax: 703.815.5675

3. SYSTEM ADMINISTRATION: ADMIN-LEVEL

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 1.3.1.

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

Plesk, Inc. is located in Chantilly, Virginia just outside of Washington, D.C. Plesk also has an office in 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 Linux 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 1.3.1.

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 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 functionality for both a system administrator and an end user, which is referred to as a "client" in the Plesk system. Both

can perform tasks at remote locations via any standard Internet browser. The following capabilities exist for each type of user:

System Administrator

- Create, edit, and delete clients.
- Create, edit, and delete domains.
- Manage multiple domains.
- Set up virtual hosting accounts (IP or Name-based).
- Set parameters for disk space usage and traffic.
- Create mail accounts, redirects, groups, and autoresponders.
- View server and user level statistics and reports.
- Support FrontPage, MySQL, CGI, SSI, Perl, PHP, and SSL operations.
- Change login passwords.
- Create protected directories.
- Upload, generate, and activate SSL Certificates for domains and the control panel
- Set up allowable mail relay capabilities as well as mail blockers.
- Customize DNS zone files.
- Manage IP aliases.
- Create Web Users within a domain.
- Set log rotation schedules.
- Add new logo to the Plesk Server Administrator banner.

Client

- Manage multiple domains.
- Create mail accounts, redirects, groups, and autoresponders.
- View disk utilization for each domain.
- Support FrontPage, MySQL, CGI, SSI, Perl, PHP, and SSL operations.
- Change login passwords.
- Create protected directories.
- Upload, generate, and activate SSL certificates.
- Customize DNS zone files.
- Create Web Users within a domain.
- Set log rotation schedules.

1.2.3 Compatible Operating Systems

The Plesk Server Administrator (PSA) 1.3.1 is available for the following platforms:

- FreeBSD® 4.0, 4.1, 4.2
- Red Hat® Linux 6.2 and 7.0

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 1.3.1.

Red Hat® Linux
Red Hat® Linux version 6.2 or 7.0
Pentium 100 MHz or better w/ 32MB Ram
Netscape 4.x+ or Microsoft Internet Explorer 4.x+
FreeBSD®
FreeBSD® versions 4.0, 4.1, and 4.2
Pentium 100 MHz or better w/ 32 MB Ram
Netscape 4.x+ or Microsoft Internet Explorer 4.x+

NOTE: PSA installs everything into the /USR/LOCAL/PLESK 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:

- 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 the Plesk system. However, this certificate will not be recognized by the web browser as being valid for your control panel URL, which results in warning messages. Contact a certificate-signing authority directly to obtain a new certificate for a specific domain.
- 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 webserver; all client CGI scripts are executed only with the client's permission.
- On FreeBSD and Linux systems, PSA uses the chroot feature on the FTP server, preventing clients from changing their home directories to another directory.
- If a company wishes to use its name/logo on its clients' versions, please call Plesk Technical Support (1-703-815-5670) for information on restrictions and implications.
- Firewalls are not currently supported, but will be added in a future release.
- PSA uses the Qmail system. Because Qmail does not allow the mail server to be accessed remotely, your email system is protected against spamming.

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 both the system administrator and the client administering his or her domains using PSA. Certain sections apply only to a system administrator, one section provides client-specific instructions, 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
- 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, and information on hosting partners, reseller arrangements and contacts.

  NOTE: We strongly encourage you to consult the **FAQ** section of our website when encountering problems or questions concerning PSA. Our Technical Support staff continuously updates this 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. To access this service, call Plesk Inc. toll free at 1-703-815-5670 or purchase the service online at www.plesk.com.
    - **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. on our toll-free telephone line at 1-703-815-5670.
    - **Unlimited Email Support**
      You can purchase a 1-year unlimited email support package for $249 USD. To access this service, call Plesk Inc. on our toll free telephone line 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 actually download the software. This can be done directly from the Plesk website.

1. Go to www.plesk.com/download to download the PSA software.
2. Click the operating system of your choice (FreeBSD® or Red Hat®). Each choice is a downloadable shell program.
3. 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 with the download.
4. Click on the **DOWNLOAD** button and you will be prompted to choose a location on your computer to which to download the software.
5. After indicating the download location, click the "OK" button in the **DOWNLOAD** file box and the download will begin.
6. When the download is complete, the Plesk Server Administrator is ready to be installed on your computer.

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.

Plesk Server Administrator includes the following components:

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

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.

Services Running under PSA
The following services run under PSA:

- named – BIND 8.2.3-REL
- MySQL – 3.23.32
- Qmail – 1.03
- Apache – 1.3.14 Ben-SSL/1.41
- ProFTP – 1.2.orc2
- stunnel – 3.7

NOTE: Additional services running under Apache are mod_throttle 2.11, mod_perl 1.24_01, PHP 4.0.3pl1, and FrontPage 4.0.

Directory Structure

PSA creates the directory **/usr/local/plesk/** as its root software directory. Several subdirectories are created, including:

- /usr/local/plesk/admin/...
- /usr/local/plesk/apache/...
- /usr/local/plesk/mysql/...
- /usr/local/plesk/ftpd/...
- /usr/local/plesk/namedb/...
- /usr/local/plesk/stunnel/...
- /usr/local/plesk/frontpage/...
- /usr/local/plesk/qmail/...

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.

Sendmail

Plesk Server Administrator disables the sendmail service and replaces it with qmail. The following changes occur as a result:

- 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

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 **resolve.conf** file.
2. The line **search localdomain** must be removed from the **named.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

Download the PSA software file from www.plesk.com/downloads. Run the install script. As this script is executed, you will be asked questions. Before starting the installation you will need to know the administrator's e-mail address, the host name and the domain name, and the IP address to be used for name-based hosting.

1. Change your working directory to the directory where the Server Administrator install script resides; for example:
   #cd /home/admin/plesk
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/plesk 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/Plesk 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, then you will see the software license agreement and will be asked to either accept or decline it's terms. Press "A" to accept, or "D" to decline. If you decline, the installation process will abort, if you accept, the installation will continue.
5. Install now asks you about the Administrator's e-mail address. Do not use the system root e-mail. Root account usage is restricted by the Qmail system. Choose another address when you are prompted to:
   Enter Plesk Administrator e-mail address.
6. The install script will try to guess the hostname of the server. You will then be asked to confirm it and correct it. You are then asked to confirm the domain name of the server.
7. The installation will detect all of the IP addresses that are assigned on the server and will ask you to select the one to be used for all of the name-based virtual hosts.
8. Next the script will display a series of messages displaying 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.
9. When the installation is complete, you will be asked whether you wish to start Plesk or not. If you select "Y" 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.

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

To uninstall Plesk Server Administrator you can do so by utilizing the Uninstall feature within the Server section of PSA, or by carefully following the below steps:

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. Go to the directory where the PSA install script is located.
3. Then execute the installation script with deinstall added to the end of the line.
4. Example for uninstalling RedHat 6.x: sh plesk-1.3.0-redhat-6.x-i386-install.sh deinstall

NOTE: Exercise extreme caution when using this command, since the whole PSA directory will be deleted without confirmation! 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.

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 1.3, follow these steps:

1. Open your web browser.
2. Administrators and Clients each access the control panel from different **urls**.
    - Administrators - HTTPS://PrimaryIP:8443 (Primary IP refers to the primary IP address of your server – any IP address on your server will work)
    - Clients - HTTPS://ClientDomain.com:8443 (ClientDomain.com refers to any active domain that resolves to 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 start the Plesk Server Administrator (PSA) software, 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 **LOG IN** to proceed.

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 your PSA home 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.

2.3.4 Automatic Log Out

PSA automatically logs you out if you are idle for a certain amount of time. In PSA, this is termed "Session idle time." The default is 30 minutes; only the system administrator has the access to change this setting. Since only one person can log in as an administrator at any one time, this feature frees up resources. See "Setting the Login Time Out" for more information.

1. If your session is idle for the maximum allowable time, PSA will "freeze" your screen, deactivating the page from accepting any further input.
2. Click anywhere on the screen and you automatically return to the PSA login screen.
3. Enter your Plesk login name and password, and click **LOG IN** to access PSA.

NOTE: PSA allows only one person to login at the administrator level at a time.

3. System Administration: Admin-Level

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:

- System Management
  - Rebooting the System
  - Shutting Down the System
  - Uninstall PSA from the System
  - IP Aliasing
  - Set System Time
  - System Statistics
- System Services
  - Mail System Management
- Control Panel Management
  - Logo Setup
  - Sessions Management
  - Edit Admin Information
  - Control Panel Certificate Management
- 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.

Uninstalling PSA from the System

You may wish to uninstall PSA from your server. This function can be accomplished through the interface, and doing so will also uninstall all applications which PSA installed initially. To uninstall PSA from 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 **UNINSTALL** button.
3. PSA warns you that you are about to remove the Server Administrator software and all related programs from your server, and asks you to confirm your choice. Click **OK** to uninstall PSA or **Cancel** to leave PSA on your server.

NOTE: Uninstalling PSA from your server will also uninstall Apache and all other applications and services which Plesk installed initially as well. As a result, all clients, domains, mail, and other related information will be deleted permanently.

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."
- **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 hosts 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 **UPDATE** to submit.
3. 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 **UPDATE** to submit.
4. To add an IP address/mask to the White List, type in the appropriate IP Address and mask in the fields provided. Click the **ADD** button to submit. The address selected will appear in the IP list.
5. To remove an IP address/mask from the White List, select the IP address you wish to delete from the IP list. Click the **REMOVE** button.
6. 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.

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.

Edit the Administrator 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; it is important to note that it is the only required field on this page. 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. The admin email address is initially set during installation, and is a required field.
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.

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.
- 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 **Organization Unit Name:** click in the ext box 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 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 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 downloading 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 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.
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.

3.1.4 Setting the Administrative 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 in the **Old password** text box and enter your current password.
3. Click in the **New password** text box and enter the password that you wish to change to.
4. Click in the **Confirm password** text box and re-enter the new password, exactly as you entered it in the **New password** text box.
5. Click 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 **CLIENT** 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:

- Client List Page
  - Client List
  - Creating a Client
- Client Home Page

- Activating or Deactivating a Client
- Editing a Client Record
- Deleting a Client
- Reporting on a Client's Status
- Create a New Domain

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. By clicking on the **SORT BY** button, 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. 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.

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.

By default, the client list is sorted alphabetically by name. If you wish to view client records in a different order, click on the **SORTED BY** drop-down arrow, and select your preferred order:

- Creation Date
- Creation Date (reverse)
- Client Name
- Client Name (reverse)
- Problem
- Problem (reverse)
- Status
- Status (reverse)

Click on your preferred order in the drop down box to refresh and reorganize the client list.

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.

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.
    - **Plesk login name** - By assigning a Plesk login name to a client, you grant that user access to PSA for independent account administration. Each client's PSA login name must be unique in the system.
    - **Plesk password** - You must assign a password to each client for security purposes.
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 command 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. **IMPORTANT:** Once the domain is created, the WWW option cannot be changed.

   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.

3.2.2 Client Home Page

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

- Activate or deactivate a client
- Edit a client's information
- Access a client status report
- Delete a client
- Create a new domain for a client
- Access the domain administration page for any of the client's domains

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 Record

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. Three data fields are required: contact name, Plesk login name and Plesk 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.

Deleting a Client

Sometimes, you may need to remove a client from your system. Before you delete a client, be sure that you really want to remove the client from the system. Once a client is deleted from PSA, the information is completely erased and permanently deleted.

NOTE: If you ever need to re-instate the client, you must re-create the client record from scratch.

To delete a client, 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 you wish to change.
3. The Client Home page appears.
4. Click **DELETE** to remove the client from your system.
5. The Server Administrator asks you to confirm that you really want to erase this client's record:
6. Click **OK** to delete the client, or click Cancel to keep this client on your server.

Reporting on a Client's Status

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:

- Company name
- Client status
- Street address
- Plesk login name
- Phone number
- Creation date
- Fax number
- E-mail address

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 three 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 **UPLEVEL** to close the report and to return to the *Client Summary page*.
- Print a copy of the report. Select File/Print in your browser to print a paper copy of the report you are viewing.

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 with text boxes containing all the necessary 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 command 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.

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:

- Domains List Page
  - Creating a Domain
  - Editing a Domain
- Domain Administration Page
  - Turning a Domain On or Off
  - Domain Preferences
  - Domain Report
  - Deleting a Domain
  - 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
    - DNS Definitions
    - Changing DNS Settings
    - DNS Example Setups
  - Changing Hosting Settings
    - Physical Hosting Configuration
    - Standard Forwarding Configuration
    - Frame Forwarding Configuration
  - Web Users
  - Directories
    - Creating a Directory
    - Changing a Directory
  - Certificates

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. Use any of the Internet registration services to do this.

You can create a domain in two different ways:

- Use the **CLIENTS** function. When you create a client, you can, at the same time, add a domain name to the record.
- Use the **DOMAINS** function. When you create a domain, you can create its client at the same time.

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.

The domain list is sorted alphabetically by name. If the list is long and you wish to view domain records in a different order, click on the **Sorted by:** drop down arrow. You can display domains by the date they were created, by their current status (i.e. active domains first) or by name. Click on your preferred sorting choice to refresh and reorganize the client list.

Creating a Domain

If you are in a hurry, you can create a domain by simply entering the domain name in a new client record, that is, when you are using the **CLIENTS** function to create a new client in the PSA system. Then, at a later time, you can add more detailed information and configure the domain services using the **DOMAINS** function.

NOTE: You must officially register a domain and Internet address before you create it in the Plesk Server Administrator. Use any of the Internet registration services available to do this.

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

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

- PSA displays the *New Domain page*. It prompts you for all the information you need to create a new domain.
- 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.

    - **Contact Name** - This is the name that appears in the Clients list. Enter the client who owns this domain. The Contact Name must be unique in the system.
    - **Plesk login name** - Enter a Plesk login name for the client, to grant that client access to PSA for independent account administration. The login name must be unique in the system.
    - **Plesk password** - You must assign a password to a client for security purposes. Apart from the domain name, all the other fields in the domain record are actually data fields from the client's record. So, when you complete all these fields when creating a new domain record, you are actually creating a client record as well.
- If you are creating a domain for a client who already exists in the system, instead of entering in each field, click the drop down arrow in the **Choose Existing Client** list. Click on the client name to select it. Plesk enters the client name in the Contact Name field, and adds the information from the client record to this domain record.
- You can edit data in any text box by clicking and editing a specific word or phrase.
- When you are satisfied that the information is complete and correct, click **UPDATE**.
- 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.

- Access the client list by clicking the **CLIENTS** button at the top of the PSA interface.
- Click on the name of the client who owns the domain you wish to edit.
- The client summary page appears, listing the domains that the client owns. To update the client data, click **EDIT**.
- PSA displays the full client data page. Click in any text box to edit the information.
- 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.
- Delete a Domain.
- Manage Mail for a Domain.
- Customize DNS settings.
- Set-up Hosting.
- Create Web Users.
- Create Directories.
- Generate Certificates.

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 the maximum number of POP3 mailboxes, redirects, mail groups, autoresponders, and web users. It provides fields which allow the administrator to set client permissions for management of log rotation schedules and DNS zone settings for the domain. 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 preferences not created within the domain. Lastly, if a user wishes to change the status of the ‘www’ prefix requirement for the domain; that would be changeable on this page.

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*.
4. 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.
5. 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.
6. 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.

7. 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.

8. 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.
9. To utilize a mail bounce message, select the radio button for **Bounce with Phrase** and enter the appropriate text.
10. 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.

11. 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 (ie. 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 (ie. www.domain.bogus).

12. The final two boxes which appear under the heading **Client's rights for this domain:** allow the administrator to grant or deny certain privileges on their domains. Check or uncheck the **DNS Zone Management** checkbox to determine whether or not a client can manage the DNS zone for a given domain. Check or uncheck the **Log Rotation Management** checkbox to determine whether or not a client can manage the log rotation for a given domain.

13. Click the **UPDATE** button to submit any and all changes.

14. Click the **UP LEVEL** button to return to the *Domain List page*.

IMPORTANT: 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 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:

- Domain owner (client)
- Domain status
- Creation date
- Hosting type
- FTP Login
- FTP Password
- Size
- Real Size
- Traffic
- Real Traffic
- SSI support
- PHP support
- CGI support
- Perl support
- SSL support
- MySQL support
- Web users
- Postboxes
- Redirects
- Mail Groups
- Autoresponders

In order to utilize this function, 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.
    - To return to the domain record, click **UP LEVEL**. The report will close and you return to the domain administration page.
    - To print a copy of the report, select **File/Print** in your browser and a paper copy of the report will print.

Deleting a Domain

Sometimes, you may need to remove a domain from your system. Before you delete a domain, be sure that you really want to remove the domain; once a domain is deleted from the Plesk Server Administrator, the information is permanently erased. During deletion, PSA also deletes all HTML files, mail accounts, web users, log files and FTP accounts. If you ever need to reinstate the domain, you must re-create the domain record.

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 **DELETE** button to remove the domain from your system.
4. PSA asks you to confirm that you really want to erase this domain.
5. Click **OK** to delete the domain. Or, click the **Cancel** button to keep this domain on your server.

NOTE: In some cases, it may be better to turn a domain off rather than delete it entirely. Make sure that you are certain you want to delete a domain before proceeding with the deleting a domain function.

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
- 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 POP3 email boxes. 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 three icons, each representing different mail account types. They are:
        - POP3 Mail Account (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 the *Mail Name Properties page* for that given name.
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

    - 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 POP3 account and password for a given mail name.

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 POP3 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.
    - Once you have enabled the mailbox and entered the passwords, 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 **OKAY** 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 enter text to be included in the autoresponder in the **Answer text** field. Click **UPDATE** to submit.
- 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**. 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. By default, PSA assumes the primary DNS runs locally on the server; therefore the initial DNS zone status is **ON**. PSA creates default entries for NS, A, CNAME, MX and PTR records.

DNS Definitions

We start this section by defining the default PSA setup. Then, we discuss two specific examples of how a company might set DNS definitions on its server. You can view these examples here.

- For the **NS record** of plesk.com, PSA creates an association of the domain with a name server ns.plesk.com. It also creates an **A record** for ns.plesk.com associating that name server with the main server IP-Address. It is important to note that this entry is created simply as a default, since there is no way for PSA to know the name of the true primary name server to be used for the domains residing on the server. Names properly registered will resolve regardless of this NS entry; however, it is recommended - to minimize confusion for the clients -

that this **NS record** be changed by the administrator to reflect the appropriate primary name server. Also, the A record that is created for ns.plesk.com can be removed once you have created the proper association of the domain to its true primary name server.

NOTE: By default, PSA does not create a secondary name server association for the domain. It is the administrator's responsibility of the to set up the appropriate secondary name server for the domain. The administrator performs this task regardless whether this is to be handled external to the server or local to the server. Once the administrator knows the name of the secondary name server, he/she should add an NS record within the domain, associating the domain with the secondary name server.

- The **A record** for plesk.com reflects either the IP address of the main server for name-based hosting accounts or the IP-address given to that domain for accounts configured as IP-based hosting accounts. For domains using the DNS services locally on the server, there must be an **A record** associating the domain with an IP address registered to the server.

  NOTE: When a domain is originally created, DNS records are defined and can be customized for the domain, even prior to the configuration of hosting for the domain. As a default, the DNS records for a new domain are configured as a name-based hosting account.

- The default **CNAME records** for plesk.com place an association for www.plesk.com, ftp.plesk.com and mail.plesk.com to plesk.com. These are basically aliases that will associate each of these names to the domain name plesk.com.

- The **MX record** for plesk.com associates the location for mail services for plesk.com to mail.plesk.com. By default, **CNAME** is an alias for plesk.com. So, the resulting mail server for the domain is plesk.com; however, if the administrator sets up a remote mail server to handle mail services for this domain, then the **MX record** needs to be changed. The configured file would need to read "mail.plesk.com IN MX plesk1.com" where "plesk1.com" is the name of the remote mail server.

  NOTE: Since remote mail server functionality is not currently supported by PSA, when setting up a remote mail server, all instances of the domain must be removed from the **virtualdomains** and **rcpthosts** files located in the usr/local/plesk/qmail/control/
  directory.

- The **PTR record** simply creates an association of an IP address to the domain name created. For name-based hosting accounts, PSA uses the main server IP address in this field. For IP-based hosting accounts, PSA uses the IP address assigned to the given domain in this field.

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. Click on the **DNS** button to access the *DNS Settings page*.
4. The **DNS Zone Status** icon indicates whether a DNS is turned on or off.
    - By default, DNS is turned on for every domain.
    - If you wish to turn DNS off for the domain, select **ON/OFF**.
    - Turning the DNS zone off will refresh the page, so that only a list of nameservers remains.
    - 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.
    - You should note, when turning DNS off, that PSA keeps an association of the domain to its name server(s).
    - 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. These new NS entries associate the domain with the appropriate name server(s) and remove the default **NS** entry. At that point, turn DNS off. You see that the name server(s) for the domain remains listed as a link.
5. 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 this 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 this 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 this 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. 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.

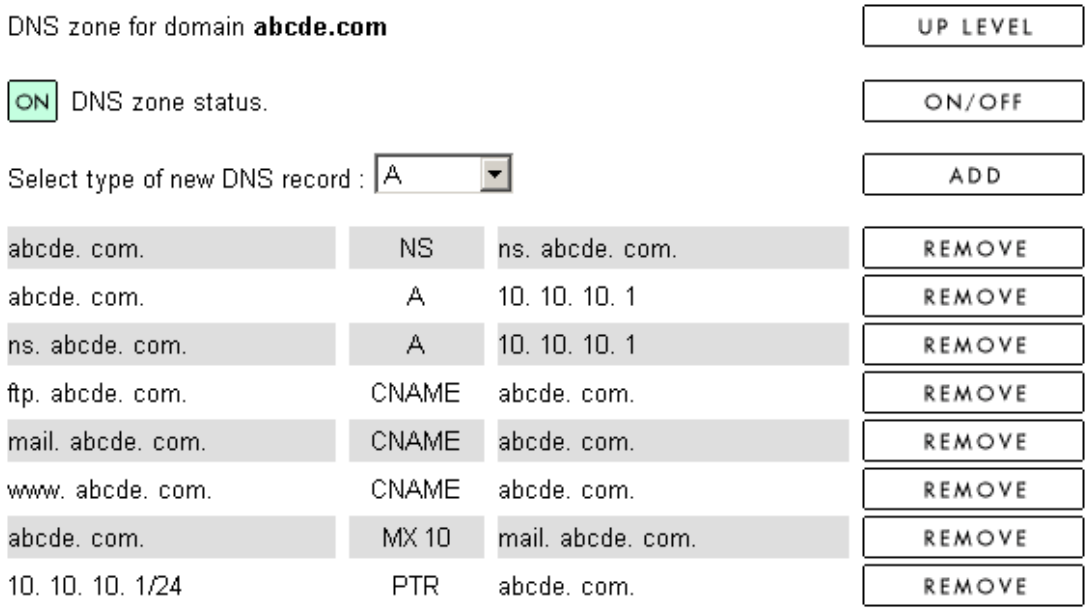
6. You may remove any DNS records by selecting **REMOVE** beside the record you wish to delete. Before anything is processed you will be asked to confirm the deletion.

DNS Example Setups

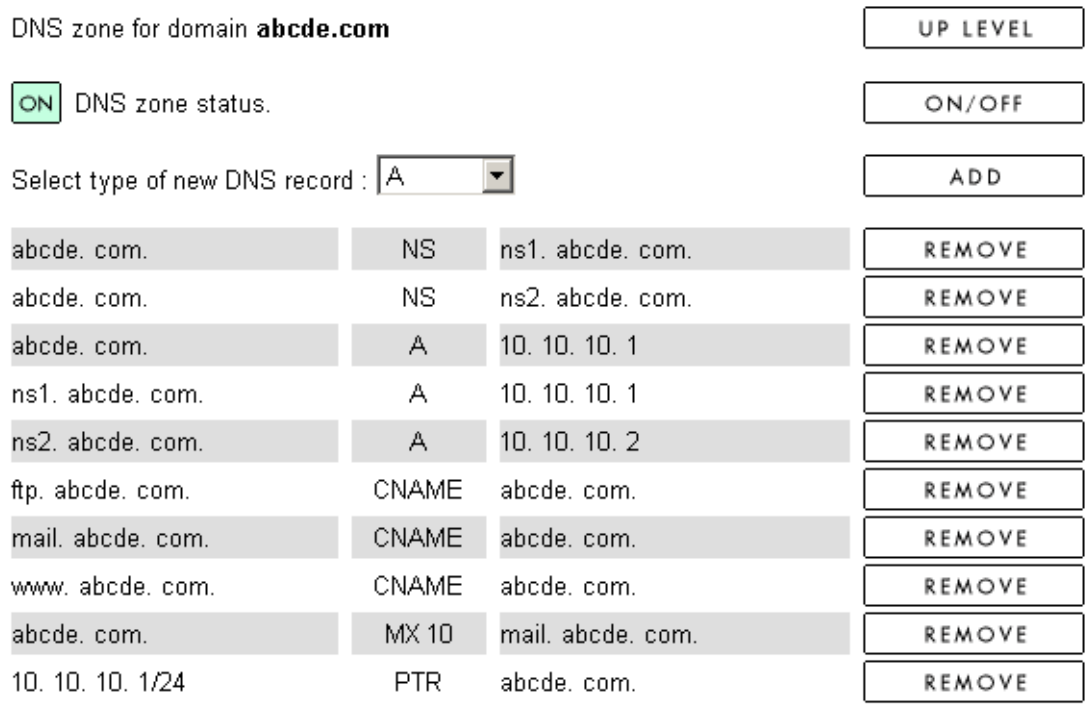
Example 1: A hosting company (we'll use *abcde.com*, which is for example purposes only, and is not intended to represent any existing companies or domains) wishes to setup their PSA enabled server as the primary DNS server for all the domains they create and will run secondary DNS services on an external 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. Although a properly registered domain will resolve at this point, 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 DNS settings for a domain named *abcde.com* are as follows:

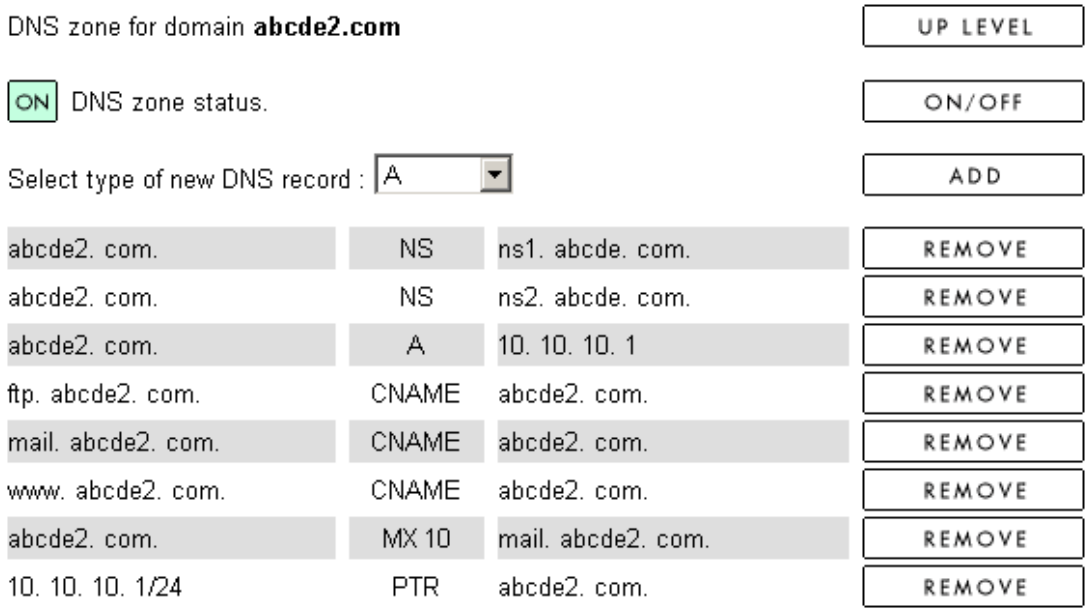


*The next step is to create A records for the name server names you will be using. Every name server name must have a specific IP Address associated with it. Manipulate the DNS records for *abcde.com* to reflect the following. Exact instructions for adding and removing DNS records are described earlier 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:



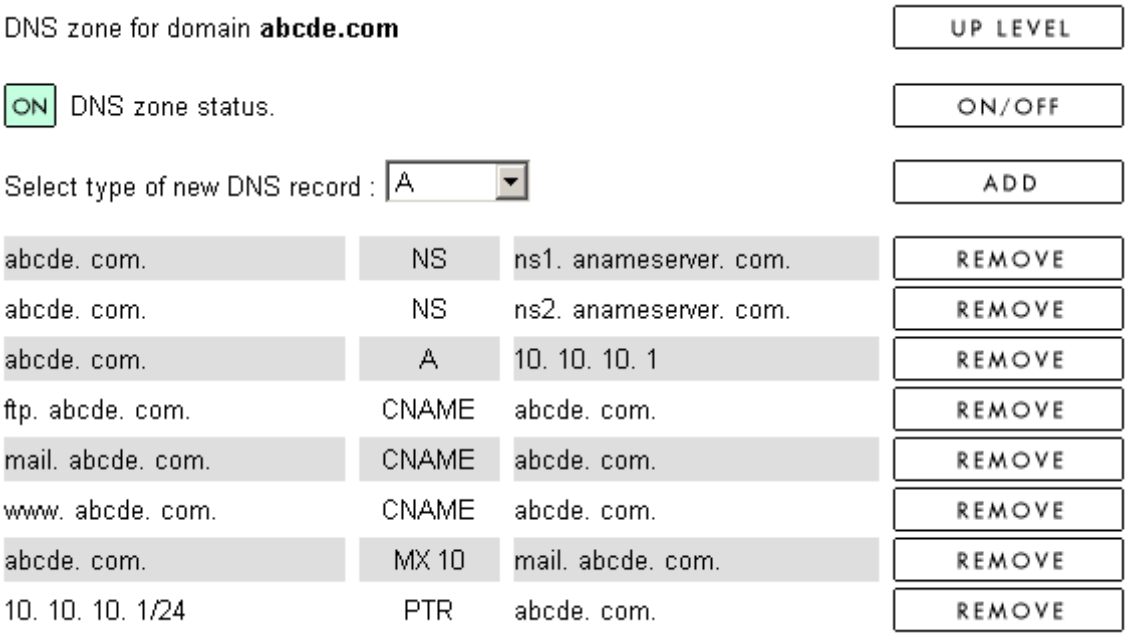
This would be repeated for all the domains created on the server.

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 option 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.

Physical Hosting Configuration

There are several settings to configure for physical hosting, the most common type of hosting service. 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. 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, enter a valid Internet address in the IP address text boxes.

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 a password for security.
5. Tab to the **disk space** text box and enter or edit the number of megabytes you are providing on the server for this domain's hosting services. If the disk space limitation is exceeded, the domain's status will change to [!].
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 enable it. 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. If you know that someone needs to remotely edit this website, you can always enable authorization and then disable authorization when the edits are complete. 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 and FP Admin 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 **Perl Support** check box. Perl is an interpreted high-level programming language. Perl is very popular among System Administrators who use it for a vast number of automation tasks. Many CGI programs are written in Perl. If your client wants to support Perl, make sure a check mark appears in the Perl box.
15. 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.
16. TAB to the **MySQL Support** check box. MySQL is a free, easy-to-use, multi-user SQL database server in a standard client/ server environment. If your client needs MySQL support, make sure a check mark appears in the **MySQL** check box. PSA creates a database named after the FTP user in the MySQL server, and enters a record for the user (including the FTP name and password) into the database.
17. 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.
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.
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*. You can select any web user name to edit the web user password. You can delete a web user by clicking the **REMOVE** button next to the corresponding web user name. Confirmation will be required before removing the user.

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 **New Web User name** in the text box provided next to "**New web user:**" and click **ADD**.
6. You are taken to the *New Password Page*, where you must enter and confirm the password for your new web user. To do this, enter a password in the **Password** text box, and then re-enter it in the **Confirm** text box, then click on **UPDATE** to enter the information.
7. As you create web users, the user names appear on this page in the web user list.
8. To change web user passwords, click on the user name in the web user list. This takes you to the *New Password page*. Follow the same procedure as taken in Step 6.
9. Click the **REMOVE** button next to any web user name you want to delete. A warning appears, click **OKAY** to delete the user name.
10. When you are done, click **UP LEVEL** to return to the *Domain Administration page*.

Important Notes on web users:

- For security purposes, the password must be between 6 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.

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.

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, click in the **Create new protected directory** text box and then enter a new directory name.
5. Click the **ADD** button.
6. This takes you to the *Protected Directory Control page*. The name of the new directory and the domain in which it has been created are listed at the top of the page.
7. 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**.
8. 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.
9. 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.
10. To add a new user, under **Protected Directory Users** click in the **New User:** text box**,** and write the name of the directory user.
11. Click the **ADD** button.
12. You are taken to the directory password screen. Here you must enter your new password in the **New Password** text box, and then enter it again in the **Confirm** text box.
13. 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.
14. To remove a directory user, click the **REMOVE** button
15. 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 password screen. Here you can edit the password.
16. Click **UP LEVEL** to return to the *Protected Directory List page*.

Changing a Protected Directory

You can edit a protected directory definition to:

- Delete the directory
- 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 Protected Directories** section.
7. Click **UP LEVEL** to return to the *Protected Directory List page*.

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.

Certificates

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:

- In order to use SSL certificates for a given domain, the domain MUST be set-up for IP-Based hosting.
- 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.

- 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.

To generate a self-signed certificate or a certificate-signing request, 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. If you have established an IP based hosting account, 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.
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 **Organization Unit Name:** click in the text box 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 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 upload a new certificate:

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.
7. 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.
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*.

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. If you have established an IP based hosting account, the **CERTIFICATE** button will be enabled.
4. Click the **CERTIFICATE** button. The *SSL certificate setup page* appears.
5. The icon next to **Use rootchain certificate for this domain** appears on this page.
6. 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.
7. To change the status of the rootchain certificate, click the **ON/OFF** button.
8. 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.
9. Then click the **SEND FILE** button. This will upload your rootchain certificate to the server to assure proper authentication of the certificate authority.

4. Client-Level Administration

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:

- Edit your client record
- View a status report
- Access and manage your domains
- Log out of PSA

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 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. Evaluation of disk space and traffic occurs every 24 hours.

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

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

By default, the domains in the list are sorted alphabetically by name. If you wish to view domain records in a different order, click on the **Sorted by** drop down arrow. You can display domains by their creation date, domain name, problem status, admin status, or client status. Click on your preferred sorting order to refresh and reorganize the list. From this page, you can access your domain. Click on the domain name you want to work with (some clients may only have one domain name), and the *Domain Administration page* appears.

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 Plesk password is a required text box.
4. When you are satisfied that the information is complete and correct, click **UPDATE**.
5. PSA informs you if you have not entered the password. If the password has not been entered, return to the client record and enter it. Click **UPDATE** to save the edited information.

NOTE: You cannot change your Plesk 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 the PSA client function at any time without saving your work. Click **UP LEVEL** to return to your home page and delete 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 **UPLEVEL** to return to the *Client Home page*.

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 register your domain and Internet address before creating it in the Plesk Server Administrator. Use any Internet registration service to do this.

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

- Turn the domain **ON/OFF**
- Report on domain activity
- Manage mail functions
- Manage DNS settings
- Change the hosting settings
- Create protected directories
- Generate and upload SSL certificates

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.

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. PSA 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** 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.

Managing Domain Preferences

The *Domain Preferences page* displays the preferences that the Plesk administrator has set up for this domain. Preferences include the maximum number of POP3 mailboxes, redirects, mail groups, autoresponders, and web users for the domain. From this page, you can set up a mail bounce message or a catch-all email address for invalid user names. These mail features are used to handle mail received by this domain, for a mail account that has not been created within the domain. Also, you can enable/disable the 'www' prefix setting for your domain by clicking in the checkbox provided. This page also indicates whether or not the Plesk administrator has enabled the client to manage the DNS zone and log rotation for the domain.

These settings appear on the page:

- **Maximum Mailboxes** - the maximum number of POP3 mail accounts that the administrator allows the client to create.
- **Maximum Mail Redirects** - the maximum number of mail redirects that the administrator allows the client to set up.
- **Maximum Mail Groups** - the maximum number of mail groups that the administrator allows the client to set up.

- **Maximum Autoresponders –** the maximum number of mail autoresponders that the administrator allows the client to set up.
- **Maximum Web Users** – the maximum number of web users that the administrator allows the client to create.
- 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. As a client, you are able to enable or disable this feature.
- The final two preferences which appear under the heading **Client's rights for this domain:** indicate whether the administrator has granted or denied certain privileges on your domain. Enabled or Disabled will appear to the right of **DNS Zone Management** and **Log Rotation Management** to indicate whether or not a client can manage either of these functions for a given domain.

To adjust the settings, follow these steps:

12. From the *Client Home page,* click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.
13. Click the **PREFERENCES** button to access the *Domain Preferences page*.
14. The administrator sets the maximum number of mailboxes, redirects, mail groups, autoresponders, and web users. The administrator also enables or disables the client to manage the DNS zone and log rotation.
15. 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.
16. To utilize a catch-all email address, select the radio button for **Catch to address** and enter the appropriate email address.
17. 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 (ie. 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 (ie. www.domain.bogus).
18. The **UPDATE** button is used to submit any and all changes.
19. The **UP LEVEL** button returns you to the *Domain List 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 Domain Reports

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
- FTP Login
- FTP Password
- Size
- Real Size
- Traffic
- Real Traffic
- SSI support
- PHP support
- CGI support
- Perl support
- SSL support
- MySQL support
- Web users
- Postboxes
- Redirects
- Mail Groups
- Autoresponders

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

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
- 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)

Manage Mail Names

When you create email accounts for domain users, you are creating POP3 email boxes. 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:
    - View the number of mail names, if any, for the given domain, listed in **bold** at the top of the page.
    - 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 three icons representing different mail account types. They are:
        - POP3 mail account (represented by the "mailbox" icon)
        - Redirects (represented by the "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.
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 Pop3 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. For the given domain, the number of mail names is listed at the top of the screen.
4. In the **Mail users list**, click on the name you want to edit. You then access the *Mail Name Properties page*.
5. 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
- Mail Redirects
- Mail Groups
- Mail Autoresponders

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 POP3 account for your mail name. When you set up a POP3 account, you must also set a password for the account.

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

To create a POP3 account 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.
    - Once you have enabled the POP3 mailbox and entered the passwords, 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 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. 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 **OKAY** 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.
8. 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.)
2. Click the **SEND FILE** button. The attachments will then appear in the **Repository.**
3. 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).
4. To add a new mail autoresponder, click the **ADD** button.
5. A pop-up screen prompts you to enter a name for the autoresponder. Enter the desired identification name, and click **OK** to submit.
6. 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 enter text to be included in the autoresponder in the **Answer text** field. Click **UPDATE** to submit.
    - 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**. 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. By default, PSA assumes the primary

DNS runs locally on the server; therefore the initial DNS zone status is **ON**. PSA creates default entries for NS, A, CNAME, MX and PTR records.

DNS Definitions

We start this section by defining the default PSA setup. Then, we discuss two specific examples of how a company might set DNS definitions on its server. You can view these examples here.

- For the **NS record** of plesk.com, PSA creates an association of the domain with a name server ns.plesk.com. It also creates an **A record** for ns.plesk.com associating that name server with the main server IP-Address. It is important to note that this entry is created simply as a default, since there is no way for PSA to know the name of the true primary name server to be used for the domains residing on the server. Names properly registered will resolve regardless of this NS entry; however, it is recommended - to minimize confusion for the clients - that this **NS record** be changed by the administrator to reflect the appropriate primary name server. Also, the A record that is created for ns.plesk.com can be removed once you have created the proper association of the domain to its true primary name server.

  NOTE: By default, PSA does not create a secondary name server association for the domain. It is the administrator's responsibility of the to set up the appropriate secondary name server for the domain. The administrator performs this task regardless whether this is to be handled external to the server or local to the server. Once the administrator knows the name of the secondary name server, he/she should add an NS record within the domain, associating the domain with the secondary name server.

- The **A record** for plesk.com reflects either the IP address of the main server for name-based hosting accounts or the IP-address given to that domain for accounts configured as IP-based hosting accounts. For domains using the DNS services locally on the server, there must be an **A record** associating the domain with an IP address registered to the server.

  NOTE: When a domain is originally created, DNS records are defined and can be customized for the domain, even prior to the configuration of hosting for the domain. As a default, the DNS records for a new domain are configured as a name-based hosting account.

- The default **CNAME records** for plesk.com place an association for www.plesk.com, ftp.plesk.com and mail.plesk.com to plesk.com. These are basically aliases that will associate each of these names to the domain name plesk.com.

- The **MX record** for plesk.com associates the location for mail services for plesk.com to mail.plesk.com. By default, **CNAME** is an alias for plesk.com. So, the resulting mail server for the domain is plesk.com; however, if the administrator sets up a remote mail server to handle mail services for this domain, then the **MX record** needs to be changed. The configured file would need to read "mail.plesk.com IN MX plesk1.com" where "plesk1.com" is the name of the remote mail server.

  NOTE: Since remote mail server functionality is not currently supported by PSA, when setting up a remote mail server, all instances of the domain must be removed from the **virtualdomains** and **rcpthosts** files located in the usr/local/plesk/qmail/control/
  directory.

- The **PTR record** simply creates an association of an IP address to the domain name created. For name-based hosting accounts, PSA uses the main server IP address in this field. For IP-based hosting accounts, PSA uses the IP address assigned to the given domain in this field.

Changing DNS Settings

In order to change DNS settings, follow these steps:

7. From the Client Home page, click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.
8. Click the **DNS** button to access the *DNS Settings page*.
9. Click on the **DNS** button to access the *DNS Settings page*.
10. The **DNS Zone Status** icon indicates whether a DNS is turned on or off.
    - By default, DNS is turned on for every domain.
    - If you wish to turn DNS off for the domain, select **ON/OFF**.
    - Turning the DNS zone off will refresh the page, so that only a list of nameservers remains.
    - 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.
    - You should note, when turning DNS off, that PSA keeps an association of the domain to its name server(s).
    - 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. These new NS entries associate the domain with the appropriate name

server(s) and remove the default **NS** entry. At that point, turn DNS off. You see that the name server(s) for the domain remains listed as a link.

11. 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 this 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 this 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 this 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. 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.
12. 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.

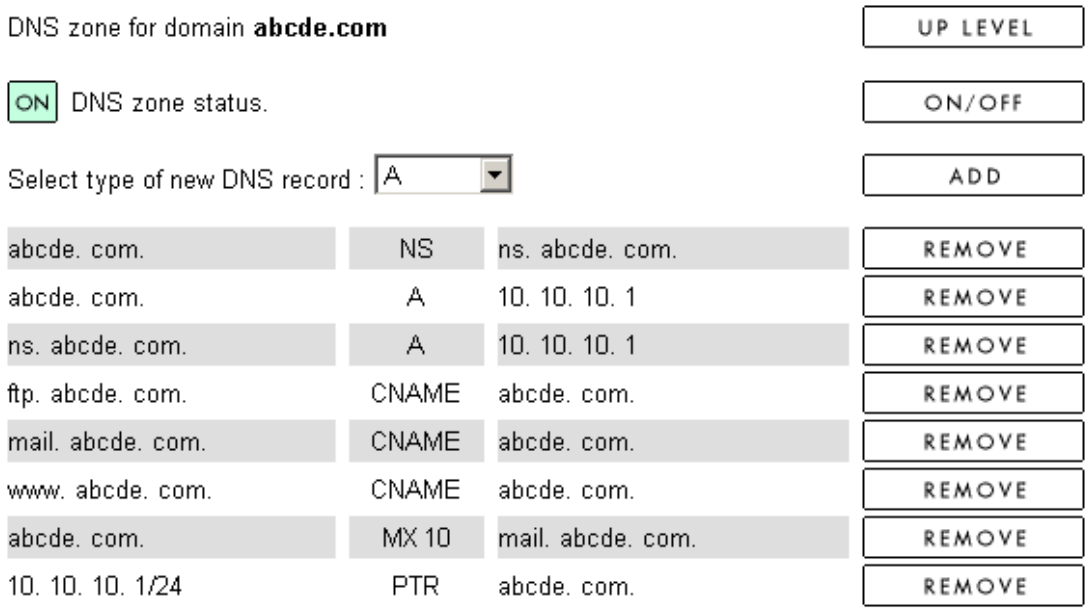
DNS Example Setups

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

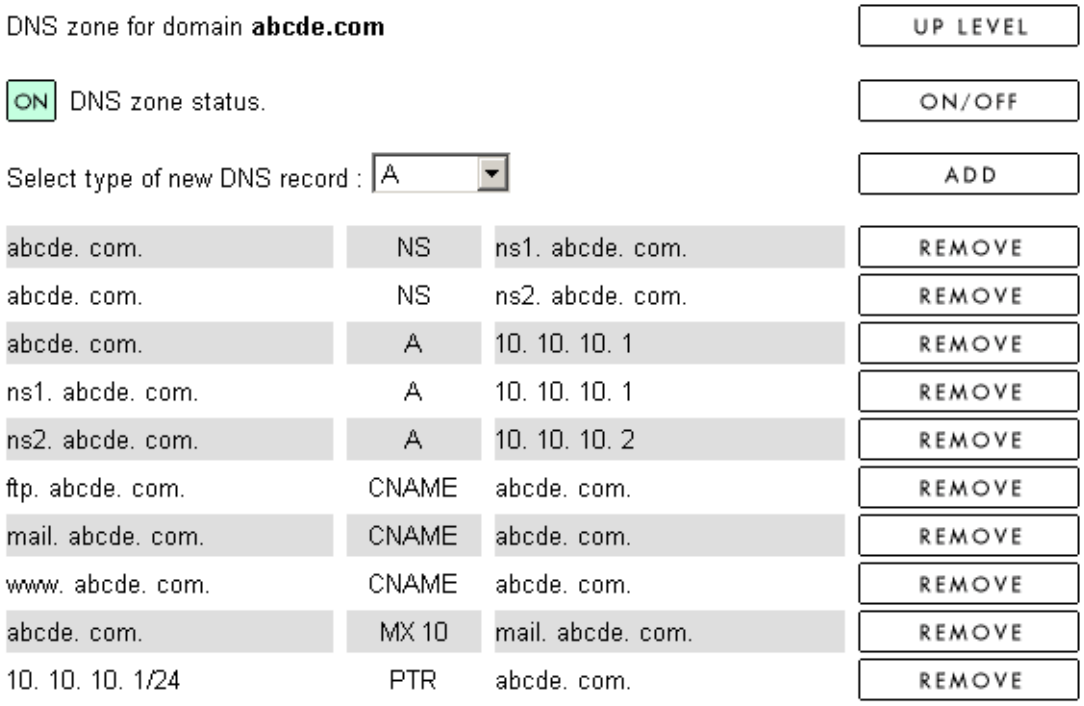
an IP address of *10.10.10.2*. These addresses will be used for *ns1.abcde.com* and *ns2.abcde.com* respectively. IP address *10.10.10.1* is also the main server IP address that was set up during PSA installation.

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. Although a properly registered domain will resolve at this point, 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 DNS settings for a domain named *abcde.com* are as follows:

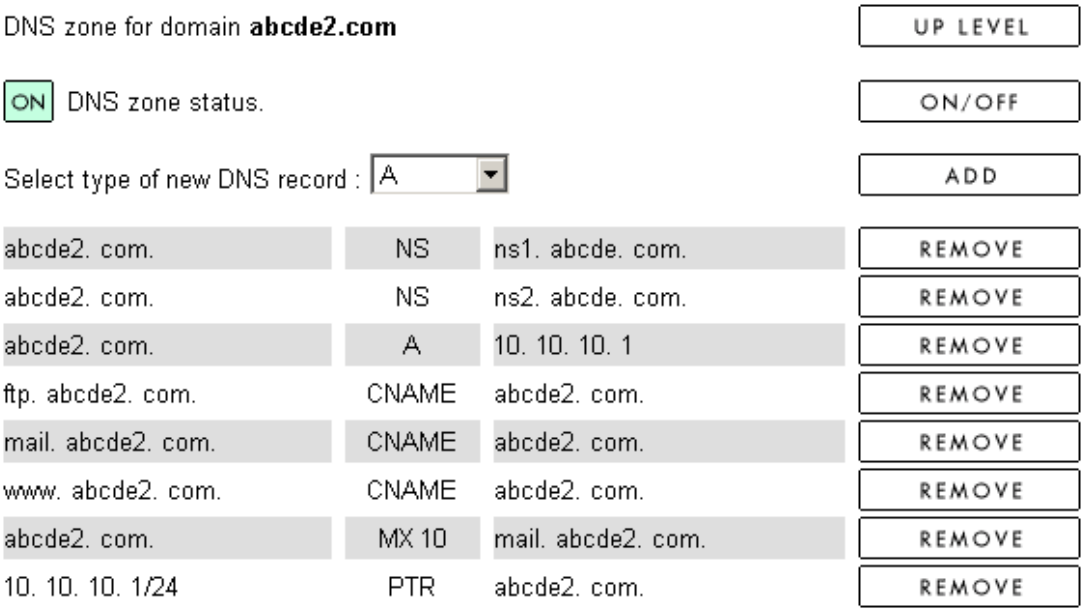


*The next step is to create A records for the name server names you will be using. Every name server name must have a specific IP Address associated with it. Manipulate the DNS records for *abcde.com* to reflect the following. Exact instructions for adding and removing DNS records are described earlier 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:



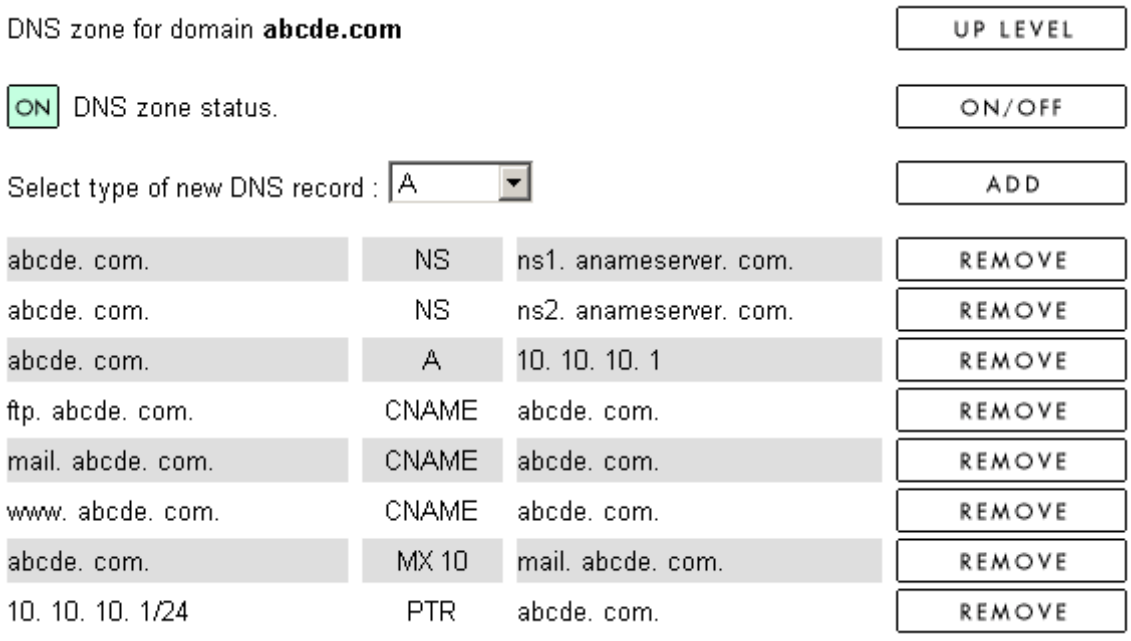
This would be repeated for all the domains created on the server.

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 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 notation schedules, and enable/disable FTP 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.

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. Depending upon the type of hosting service the administrator has established, the selected hosting page displays.

Physical Hosting Configuration

There are several physical hosting services for your domain:

- 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.
- 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.
- 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://**.
- MySQL - MySQL is a free, multi-user SQL database. When mySQL is selected for a domain, it creates a mySQL database with a name and password that matches the FTP username and password for the domain. IMPORTANT: Changing the FTP password also changes the mySQL password.

Follow these instructions to manage your virtual host (physical hosting account) services:

1. Click in the **FTP password** text box and enter or edit a password for security purposes.

2. Check or uncheck the **FrontPage Support** check box. FrontPage is Microsoft's Web publishing tool. It is one of the most commonly used tools for creating a client's Web site. FrontPage includes several extensions that provide special functionality. If you want to maintain your website with FrontPage, make sure a check mark appears in the **FrontPage** check box.
3. Check or uncheck the Authorization ENABLED checkbox. You can authorize or disable remote editing of your website using FrontPage. If you support FrontPage, you can disable authorization for additional security; then, if you know that someone needs to remotely edit your website, you can always enable authorization and then again disable authorization when the edits are complete. To activate FrontPage authorization, make sure the check box is checked. If you want to turn off FrontPage authorization, select the **Authorization DISABLED** checkbox.
4. If you want to support SSI, make sure a check mark appears in the **SSI** check box. If you want to support PHP scripting in HTML documents, make sure a check mark appears in the **PHP** check box.
5. If you want to support CGI, make sure a check mark appears in the **CGI** check box.
6. If you want to support Perl, make sure a check mark appears in the **Perl** check box.

7. SSL certificates provide additional security for Web sessions. If you want to implement an SSL certificate, make sure a check mark appears in the **SSL Support** text box.
8. To turn on MySQL support, make sure a check mark appears in the **MySQL Support** check box.
9. When you are satisfied that you have fully defined your Web services, if any changes were made, click **UPDATE**.

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

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*. You can select any web user name to edit the web user password. You can delete a web user by clicking the **REMOVE** button next to the corresponding web user name. Confirmation will be required before removing the user.

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. On the top of the screen, the number of web users displays for the selected domain.
4. To add a web user, enter the **New Web User name** in the text box provided next to "**New web user:**" and click **ADD**.
5. You are taken to the *New Password Page*, where you must enter and confirm the password for your new web user. To do this, enter a password in the **Password** text box, and then re-enter it in the **Confirm** text box, then click on **UPDATE** to enter the information.
6. As you create web users, the user names appear on this page in the web user list.
7. To change web user passwords, click on the user name in the web user list. This takes you to the *New Password page*.
8. Click the **REMOVE** button next to any web user name you want to delete. A warning appears, click **OK** to delete the user name.
9. When you are done, click **UP LEVEL** to return to the *Domain Administration page*.

Important Notes on web users:

- For security purposes, the password must be between 6 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.

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. Follow these steps to create a secure directory for your domain:

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 List page* appears. The top of the page states how many protected directories there are for a given domain.
3. To create a new protected directory, click in the **Create new protected directory** text box and then enter a new directory name.
4. Click the **ADD** button.
5. This takes you to the *Protected Directory Control page*. The name of the new directory and the domain in which it has been created are listed at the top of the page.
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 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.
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 password screen. Here you must enter your new password in the **New Password** text box, and then enter it again in the **Confirm** 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.
13. To remove a directory user, click the **REMOVE** button.
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 password screen. Here you can edit the password.
15. Click **UP LEVEL** to return to the *Protected Directory List page*.

Changing a Protected Directory

You can edit a protected directory definition to:

- Delete the directory
- Add a user
- Change a password
- Delete a user
- 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 List 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 Protected Directories** section.
6. Click **UP LEVEL** to return to the *Protected Directory List page*.

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.

Certificate Generating and Requesting

PSA enables you to upload a Secure Socket Layer (SSL) Certificate, generate a Certificate Signing Request (CSR), and 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:

- In order to use SSL certificates for a given domain, the domain MUST be set-up for IP-Based hosting.
- 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.
- 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.
- 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 who 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. 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, 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 **Organization Unit Name:** click in the ext box 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 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 upload a new certificate:

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, the **CERTIFICATE** button will be enabled.
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.
7. 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.
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*.

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. 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, the **CERTIFICATE** button will be enabled.
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.

5. Appendices

5.1 Appendix I – Apache Notes

5.1.1 Httpsd.conf: The Apache Configuration File

The httpsd.conf file is used to define your Apache configuration. The PSA software creates this file upon installation along with an Apache configuration definitions file; httpsd.conf.def. Httpsd.conf is broken into three sections: Global Settings, Main Server Configuration, and Virtual Hosts. The httpsd.conf.def file is used by PSA during all Apache updates to define the first two sections of the configuration file. The third section is created using the virtual host information housed in the Plesk Database within mySQL.

Within the first two sections of the httpsd.conf file there are several Include statements. These Include statements are used to point Apache to an external file to look for Apache customizations. Apache will read the contents of the files and will incorporate any changes that were inserted within the given Include file. Since the definitions file will be used to recreate the first two sections each time a change is made within Apache, the administrator must utilize these Include files for any and all modifications they wish to make to Apache. By doing this, the administrator ensures that their customizations will not be overwritten at any time, even if performing an upgrade of the entire PSA system. (see Include Directive for Sections 1 and 2 description below)

The third section of the httpsd.conf file, the Virtual Hosts section, is dynamically created with the addition of each virtual host. You can also use Include files within each individual virtual host for vhost specific modifications to Apache that will not be overwritten with the addition of new vhosts. (see the Include Directive for Virtual Hosts below)

File Descriptor Settings / Limitations

The PSA installation of Apache comes with the following default settings:

HARD_SERVER_LIMIT = 2048
FD_SETSIZE = 16384

FD_SETSIZE equates to the actual Kernel limit on the number of file handles that a program can have open at one time.

HARD_SERVER_LIMIT equates to the Apache limit on the number of file handles that can be open at any given time.

These settings are not changeable. If a change is needed to these settings, this would require the recompilation of Apache which must be performed by Plesk, Inc. Support Staff only. Charges of $150/hr. would apply. Because of the inherent problems that can occur when performing this operation, Plesk, Inc. will not be able to offer support to customers who attempt this on their own.

Also, within the configuration file you will find a setting for the MaxClients directive which is set depending on the processor being used on the system. The MaxClients directive sets the limit on the number of simultaneous requests that can be supported. No more than this number of child server processes will be allowed. The default settings are as follows:

Celeron or Cytrix: 254
Pentium II or higher: 640
Multiprocessor: 1024

This number can be modified using the global.include file made reference to in the httpsd.conf file. It should be noted however that the MaxClients value cannot exceed the HARD_SERVER_LIMIT of 2048.

5.1.2 Include Directives for Sections 1 and 2

Because of the need for customization within Apache PSA has included within its httpsd.conf file the callout of nine specific files that can be used to customize the configuration file.

All of the Inlcude files are located in the /usr/local/plesk/apache/conf/ directory. The administrator would apply any directives they wished within the appropriate Include file, and those changes will be immediately realized by Apache. **It should be noted that these files are intended for use by administrators with advanced knowledge of Apache**. Changes are likely to require testing and possibly troubleshooting.

<u>httpsd.conf Include Files:</u>

php.include – user-defined PHP directives
global.include – user-defined Global Environment
dso.include – user-defined DSO support
module.include – user-defined Add Module

server.include – user-defined Server configuration
dir.include – user-defined Directory configuration
icon.include – user-defined Add Icon
type.include – user-defined Add Type
additional.include – user-defined Additional parameters

5.1.3 Include Directive within the Virtual Host

The third section of httpsd.conf file contains information about all of the virtual hosts under apache. For each virtual host there is a block of commands that describe all of the options for that virtual host. If you have SSL enabled, there is a separate block just for the SSL connections. Apache treats the two as separate virtual hosts (http and https). When you create a new virtual host, PSA sets up a lot of different options to make everything work properly, however you may have occasions when the settings set up by PSA need to be changed. This is possible by adding the Include directive at the end of each virtual host block to call for an external configuration file.

The location of these custom configuration files is:
/usr/local/plesk/apache/vhosts/<vhostname>/conf

To enable the Include directive the administrator must create a file vhost.conf for http, or vhost_ssl.conf for https, and include all of the desired virtual host specific directives for the given domain. Once the file, or files, have been created the admin must then run the my_apci_rst utility within the usr/local/plesk/admin/utils/ directory, which will detect these files and rewrite the httpsd.conf file including a reference to the newly created files within the specific virtual host setup.

NOTE: For administrators who want to set up the same vhost Apache settings for every domain they create, this should be done using the Skeleton Directory on the server. This is located at /usr/local/plesk/apache/skel/. Add in the conf directory here along with the specific default Include file that is desired. (see Skeleton Directory described below)

5.1.4 Skeleton Directory

Another interesting utility for Virtual Host setup is the Skeleton Directory. The Skeleton Directory is a set of directories and files that get copied into each newly created virtual host directory structure at the time the virtual host is created. It can be used to include a standard set of CGI scripts which you wish to include in each vhosts cgi-bin, to have a customized index.html file within httpdocs, and/or to set up customized log formats using the vhost.conf file within the conf directory.

The location of the Skeleton Directory is /usr/local/plesk/apache/skel/. PSA has already created an httpdocs, httpsdocs, and cgi-bin directory within skel as these are the most likely to be used. However, you are not limited to only these directories. You are able to add directories and/or subdirectories as needed. For example, if you wanted to create a vhost.conf file to customize your vhost log formats as described above, you would first need to create the conf directory itself within the Skeleton Directory.

The administrator must be careful with regard to the settings of file permissions on files, directories, and subdirectories that are created within the Skeleton Directory. With the exception of the index.html files the file permissions that are set on the files within the Skeleton Directory will be passed on to the subsequent files that get created within the individual virtual hosts. Therefore file permission settings should be reviewed prior to the creation of new virtual hosts.

5.2 Appendix II – Sample Domain Setup

Sample Setup for New Client and New Domain

After setting up the Server settings the Admin is ready to start setting up Clients and Domains on the server. Below is a listing of the steps in the process of setting up a typical domain within PSA.

In this case the admin is creating a domain "bogus.domain" for his new Client "Brad Noname". This domain is going to be an IP-based physical hosting account, and it will utilize the local DNS server (ns1.localdns.server) as its primary name server. Its secondary DNS is handled on a remote server (ns2.remotedns.server). See **Customizing DNS Settings** for more information and examples regarding DNS setup.

The steps we will be going through are as follows:

Step 1: Create New Client
Step 2: Create New Domain
Step 3: Modify DNS Records
Step 4: Setup Physical Hosting
Step 5: Set Preferences

Step 1: Creating New Client

To create a new Client, from the *Client List Page*, select the **NEW CLIENT** option.

From the *Client Creation Page*, fill in all the appropriate information on the Client. It is obviously better to fill in as much as possible on the Client, however the only required fields are: Contact name, PLESK login name, and PLESK password.

Once all the appropriate fields are filled select **UPDATE**. PSA then returns to the *Client List Page* where the Admin can select the Client that he/she has just created.

Step 2: Create a New Domain

To create a new domain, click on the desired client name on the *Client List Page*. Once inside the *Client Home Page*, select **NEW DOMAIN**. In the field provided enter in domain.bogus and select **UPDATE**. The 'www' checkbox is left checked so the domain will be reachable with or without the use of the 'www' prefix.

After selecting **UPDATE** PSA returns back to the *Client Home Page* where bogus.domain is now visible and selectable. Select bogus.domain to start the process of setting up the domain.

Step 3: Modify DNS Records

DNS services for a domain can be handled a number of different ways. The most common, and recommended, way of handling DNS in a PSA system is to use the PSA installation of BIND for primary DNS services and to utilize an external name server for secondary DNS services.

Since PSA is not aware of how the Administrator plans to handle DNS it sets up a default zone file for each domain that requires some modification. All the required changes are achievable through the PSA interface.

NOTE: Domains that are registered properly will normally resolve without changes to the default zone file, however it is recommended that the zone file be updated.

It is assumed here that the setup of the actual name server records themselves has already been handled. For detailed information on how to setup records for your name server within PSA be sure to read the Customize DNS Settings section of the manual.

Select **DNS** from the *Domain Control Page*. PSA will open the DNS Management Page showing the default setup of bogus.domain's zone file. Since we would like to use the name servers ns1.localdns.server and ns.remotedns.server, both of these need to be added as NS records within the domain. Also, since ns.bogus.domain is not a true name server, the records defining ns.bogus.domain need to be removed.

First add NS records within bogus.domain for both ns1.localdns.server and ns.remotedns.server. To do this, select NS from the drop down list of available DNS records and select ADD. Since bogus.domain is the name for which we are defining the NS record, the field listed as "Enter domain name:" is left blank. Enter the primary name server name in the field provided and select UPDATE. This should be repeated for the secondary name server as well.

NOTE: PSA uses the first name server record entered within the SOA record for the domain. To assure that this record is created properly, the primary name server should always be entered first.

Once both the records have been entered and appear on the screen, then remove the NS record for ns.bogus.domain and also the A record that was created specifically for ns.bogus.domain. Then select **UP LEVEL** to go back to the Domain Control Page.

Step 4: Setup Physical Hosting

Select **HOSTING** from the Domain Control Page. This is where a domain is given it's physical space and traffic limitations as well as the activation of other services within the domain.

For domain bogus.domain we are going to create an IP-Based Hosting account with 10 MB's of diskspace and 1 GB/mo of allowed traffic. We will also be setting up a mySQL database for the domain and creating support for PHP, CGI, Perl, and SSL within Apache.

This is all done by simply filling in the appropriate fields and selecting the appropriate checkboxes. Once all of the options have been selected, use the **UPDATE** button to submit all settings and create the physical account.

Step 5: Set Preferences

Once the account has been created the admin now needs to set the domain level preferences for the account. Select **PREFERENCES** from the *Domain Control Page*.

For this domain we will set a limit of 5 for mail postboxes, redirects, groups, and autoresponders, and also a limit of 10 web users.

Since the Client has the ability to select whether or not they want to use a Catch To address or a Bounce Message for invalid mail requests sent to their domain, these fields should probably be left as is.

Lastly, as the Admin of the server an option is given as to whether the Client in question should have the right to control the DNS settings and/or Log deletion schedule for their domain. In most instances, the Admin will decide to leave these capabilities under the Admin control only.

5.3 Appendix III – Server Reconfiguration Utility

Brief PLESK 1.3.1 Reconfigurator description:

PLESK version 1.3.1 introduces a new utility "Reconfigurator".
This utility resides in the /usr/local/plesk directory.

The full name is /usr/local/plesk/reconfigurator.sh
This is the shell script.

The Reconfigurator provides the ability to change the admin email, hostname, domain name, and the IP address that is used for name-based hosting. Please note that the Reconfigurator does **not** add new IP addresses, it allows the admin to choose one currently configured on the NIC. If you want to change the IP address used for name-based hosting, you need to add a new IP address to the interface before starting the Reconfigurator.

Use of the Reconfigurator is similar to the Installer. Just run the Reconfigurator under the root account and answer a few questions about new admin email, hostname, and domain name. Then choose one of the available IP addresses to use as the IP for name-based hosting.

The full Reconfigurator work example is here:

```
user@host# /usr/local/plesk/reconfigurator.sh

        This script will reconfigure Plesk software on your
system /usr/local/plesk directory will be used as a root for
this product

Do you want to continue? [N] y <ENTER>



        So, it's time to reconfigure plesk.
        All files will be extracted into /usr/local/plesk
directory
        This operation takes some time,
        please, wait...

===> Extracting configuration into /usr/local/plesk
directory...
```

```
 It's necessary to know e-mail address of Plesk
administrator
 Please don't use mail address of the root on this system,
 this is one restriction of Qmail system

Enter Plesk administrator e-mail address: user@plesk.com

===> Accepting Plesk admin e-mail as user@plesk.com

Guessing that hostname of this machine is user.plesk.com

 Is this correct? [Y] N <ENTER>

Enter hostname: user

===> Accepting hostname of this machine as user

Guessing that domain name of this machine is
nsk.bsgdesign.com

 Is this correct? [Y] N <ENTER>
Enter domain name: plesk.com

===> Accepting name of the domain as plesk.com


===> Accepting full name of this machine as user.plesk.com



===> Installing MySQL Server
 Trying to start MySQL server... done
 Trying to make localization stuff...
 MySQL server starts Ok. Now shutting it down...

 Trying to stop MySQL server... done


===> Installing Admin Server
 Inserting local information into config files... done
 Trying to start Admin server... done

 Admin server starts Ok. Now shutting it down...

 Trying to stop running Admin server... done


===> Installing Apache Server
Host's networks interface(s) has(ve) the next assigned IP
addresses:
```

```
1) 192.168.2.71
2) 192.168.2.14
Which one IP would you like to use for name-based virtual
hosting? [1] 2 <ENTER>
 Trying to start MySQL server... done
 Trying to insert given IP to the MySQL database... done
 Copying apache files... done
 Trying to stop MySQL server... done
 Trying to start Apache server... done

 Apache starts Ok, now shutting it down

 Trying to stop running Apache server... done


===> Installing FrontPage extension for Apache Server
 Making chown and chmod under FP stuff

===> Installing Qmail server
 Configuring Qmail...
 Trying to start Qmail services...

 Qmail server starts Ok. Now shutting it down

 Trying to stop Qmail services... done
 Trying to restart inetd daemon... done


===> Installing and configuring Named Server

 Trying to start MySQL server... done
 Trying to stop MySQL server... done
 Trying to start Internet Domain Name Server... done

 DNS server starts Ok. Now shutting it down...

 Trying to stop DNS (named) server... done
 Trying to start MySQL server... done
 Trying to stop MySQL server... done

 Do you want to start Plesk now? [Y] Y <ENTER>
plesk: named has been started
plesk: MySQL has been started
plesk: admin server has been started
plesk: Apache has been started
plesk: Qmail has been started
plesk: stunnel has been started
```

```
                              Congratulations!
        All stages of reconfiguration were successfully
completed
        If you answered "yes" to the previous question then
        the Plesk system is already running on your host
                  Otherwise, you can start it later

        You can access Plesk Server Manager via URL:
        https://user.plesk.com:8443/
        or
        https://192.168.2.14:8443/

        login is 'admin'
```

5.4 Appendix IV - 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.

5.5 Appendix V - Copyrights, Trademarks, and Registered Trademarks

While this User's Manual is kept as current as possible, there may be information that differs slightly from the latest version of the software, which is under continual development. However, the concepts and procedures described in the User's Manual are up-to-date and valid.

Adobe™ and Acrobat™ are trademarks of Adobe Systems Incorporated.
The Internet Super Server and the BSD/OS operating system are products of Berkeley Software Design, Inc.
Debian is a free, open source operating system available from www.debian.org.
LINUX™ is a trademark of Linus B. Torvalds.
The Linux Kernel© is copyright L Linus B. Torvalds and is copyrighted under the terms of the General Public License, or GPL.
Netscape® is a registered trademark of Netscape Communications Corporation.

To check for the latest appendices for this manual Logon to

http://www.plesk.com/products/doc.php