4. Client-Level Administration

- Introduction to Client Usage
- The Client Home Page Overview
- Managing Your Client Account
    - Editing Your Client Record
- View Account Status Report
- Domain Administration Page
    - Turning Your Domain On or Off
    - Managing Domain Preferences
    - Accessing Domain Reports
    - Managing Mail
        - Mail Names Page
        - Mail Name Properties Page
            - Manage Mailbox Accounts
            - Manage Mail Redirects
            - Manage Mail Groups
            - Manage Mail Autoresponders
    - DNS Settings
        - DNS Settings Page
        - DNS Definitions
        - Changing DNS Settings
        - DNS Example Setups
    - Changing Hosting Settings
        - Physical Hosting Configuration
        - Forwarding Configuration
    - Web Users
    - Directories
        - Creating a Directory
        - Changing a Directory
    - Certificate Generating and Requesting

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 **HOME** 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:

11. From the *Client Home page,* click the domain name that you need to work with from the list provided. The *Domain Administration page* appears.
12. Click the **PREFERENCES** button to access the *Domain Preferences page*.
13. 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.
14. 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.
15. To utilize a catch-all email address, select the radio button for **Catch to address** and enter the appropriate email address.
16. 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).
17. The **UPDATE** button is used to submit any and all changes.
18. 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.
1. 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:

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.

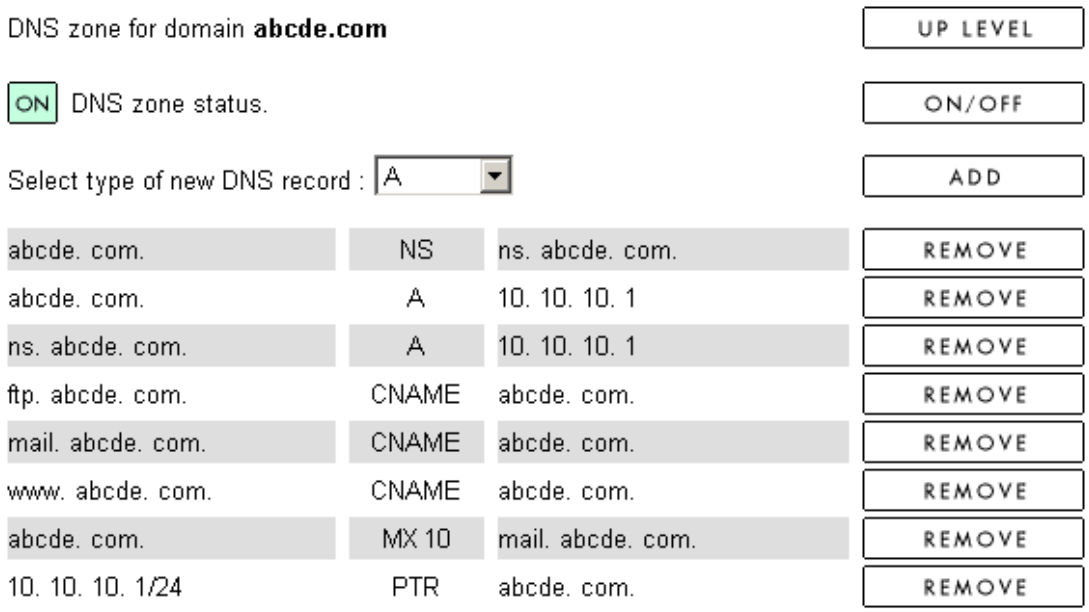
DNS Example Setups

Example 1: A hosting company (for our examples 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 both the primary and secondary DNS server for all the domains that they create. They have two IP addresses, *10.10.10.1* and *10.10.10.2*. These addresses will be used for *ns1.abcde.com* and *ns2.abcde.com*

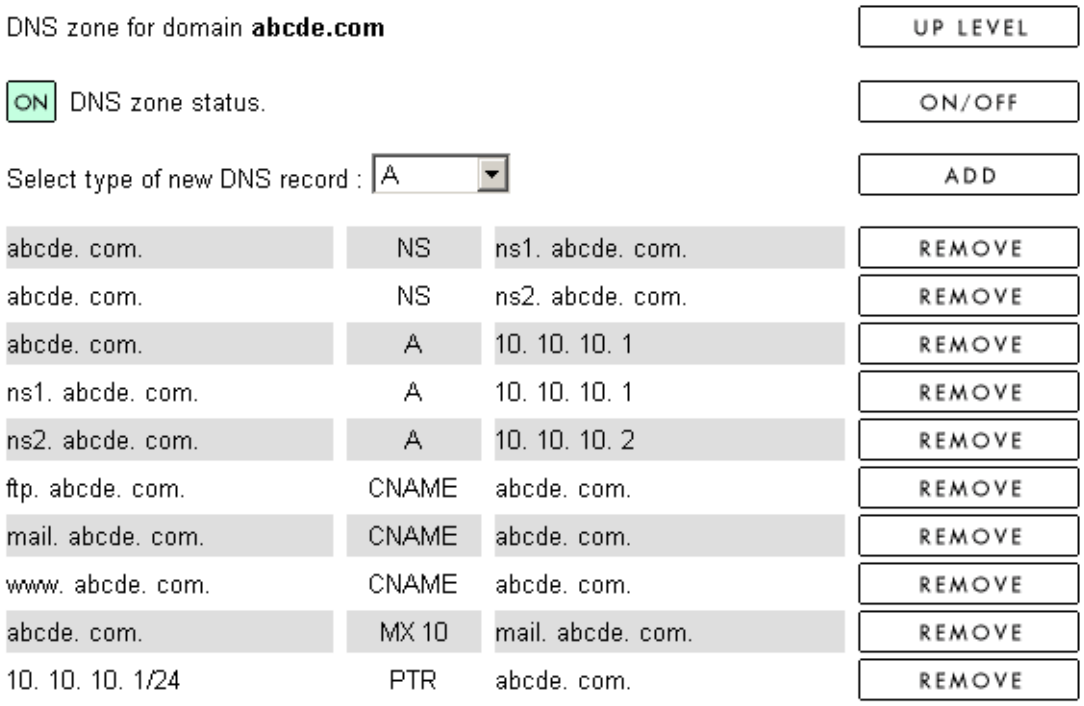
respectively. IP address *10.10.10.1* is the main server IP address that was set up during PSA installation.

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 DNS for the domain. 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:

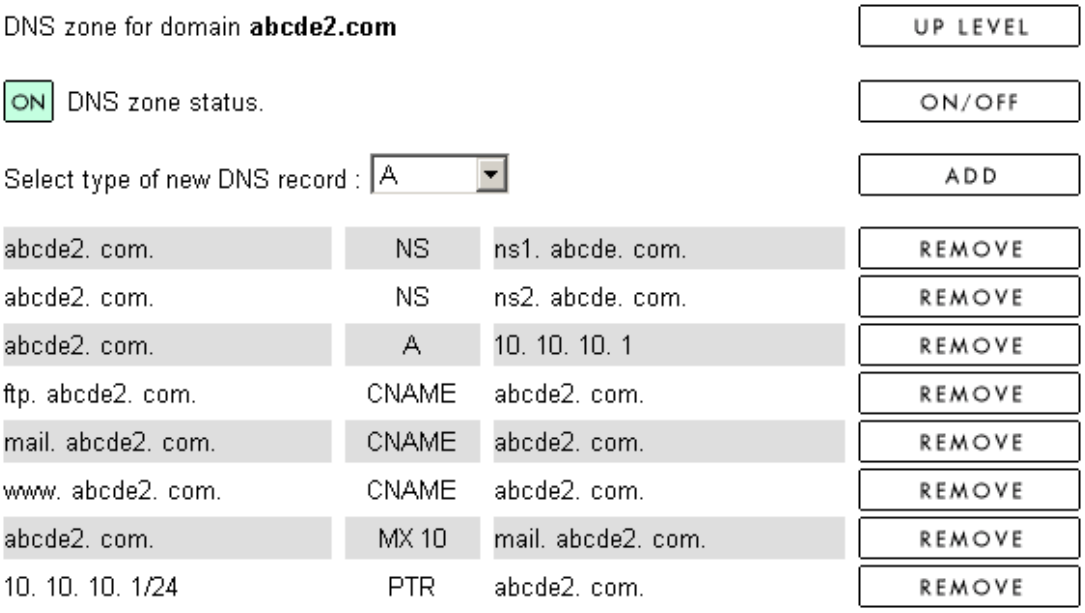


*The next step is to create the name servers to be used for all domains on this specific server. To create name servers of *ns1.abcde.com* and *ns2.abcde.com*, then you would need to make the following modifications to your DNS record for *abcde.com*.



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:



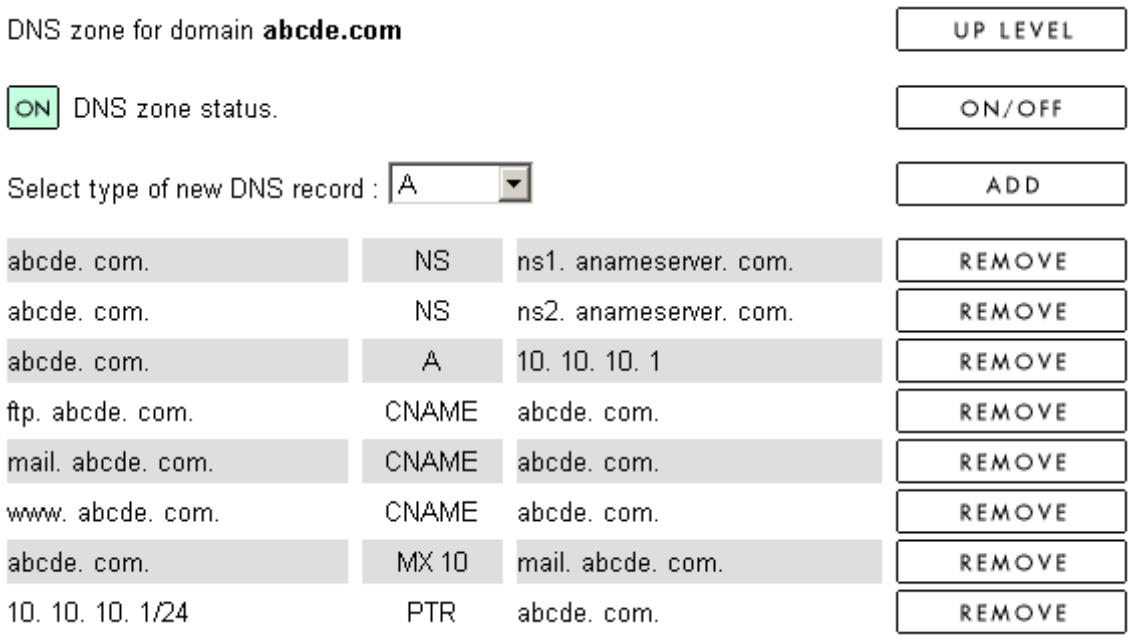
This would be repeated for all the domains created on the server.

NOTE: PSA creates the Primary Zone Files for every domain on the server. It does not create the Slave Zone Files for the secondary DNS. If you plan to run both locally on your machine there really is no point to having the Slave records. If DNS is down on the server, the use of the secondary DNS will be as useless as the primary. The setup of Slave Records is left to the administrator to control. In most cases secondary DNS is run remotely, so the Administrators are setting up the Slave Zone Files on a separate machine from the Plesk software and simply noting the secondary DNS server in the domain DNS records (in NS ns2.whatevername.com).

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.