5. Domain-Level Administration

- 5.1 Introduction to Domain Usage

- 5.2 Domain Administration Page

  - View the Domain Preferences

  - Accessing the Domain Report

  - Managing Mail

    - Mail Names page

    - Manage Mail Name Properties

      - Manage Mailbox Accounts

      - Manage Mail Redirects

      - Manage Mail Groups

      - Manage Mail Autoresponders

  - View DNS Settings

    - DNS Settings Page

  - View Hosting Settings

    - Physical Hosting Configuration

    - Forwarding Configuration

  - Web Users Management

  - Protected Directories

    - Creating a Protected Directory

    - Changing a Protected Directory

    - Searching the Protected Directories List

    - Removing a Protected Directory

  - Manage the Domain SSL Certificate

  - Anonymous FTP

  - Databases

- Searching the Database List

- Creating a New Database

- Editing an Existing Database

o Domain User

- Logging in

- Changing the password

5.1 Introduction to Domain Usage

Domain User is also a Plesk server client. The only difference is that the Domain User is limited to a single domain and is not capable of managing matters that influence system's functioning (i.e.: limits and quotas for the domain). The Domain User is however able to manage mail accounts at the owned domain, create Certificate Signing Requests (CSR) or generate self-signed certificates. Other than that the Domain User is granted all the nice things that make life easier, such as interface, that the Client does. Accessing the PSA through the web browser (Netscape 4.x+ or Microsoft Internet Explorer 4.x+), you can:

- View settings and preferences for the domain

- Change your Control Panel password

- Manage mail accounts

- Create CSR's or self-signed certificates and/or install SSL certificates (IP-based hosting only)

- Create Web Users

- Create Protected Directories

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

5.2 Domain Administration Page

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

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

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

- View the Domain Preferences

- Access the Domain Report

- Manage Mail for the Domain

- View DNS settings

- View Hosting settings

- Create Web Users

- Create Protected Directories

- Manage the Domain SSL Certificate

- View Anonymous FTP settings

- Manage Databases

- Change the Domain Level Control Panel password

View the Domain Preferences

The *Domain Preferences page* displays the preferences that the Plesk administrator or/and Client have set up for this domain. It also allows you to edit few parameters.

The parameters available for viewing from at this page are:

- **Disk Space Limit** – the amount of disk space allocated for this domain.

- **Maximum Mailboxes** - the maximum number of mail accounts allowed for creation at this domain.

- **Mailbox quota** – the limit set for the size of the mail accounts (mailboxes).

- **Maximum Mail Redirects** - the maximum number of mail allowed for setting up at this domain.

- **Maximum Mail Groups** - the maximum number of mail groups allowed for creation at this domain.

- **Maximum Autoresponders –** the maximum number of mail autoresponders allowed for setting up at this domain.

- **Maximum Web Users** – the maximum number of web users allowed for creation at this domain.

- **Maximum Databases** – the maximum number of databases allowed for creation at this domain.

- **Allow Scripting for Web Users** – enables the Web Users to download and execute scripts.

- **WebMail** – allows utilizing access to mailboxes via web-interface. If the option is provided, the mailbox can be accessed by means of a web-client , which is made available from the URL: webmail.<domain.name>

The following parameters you are able to set up:

- For **Mail sent to non-existent users**, you are able to select either a mail bounce message to return to the sender, or a catch-all email address to which the messages are sent.

- The **WWW prefix** checkbox determines whether the given domain will require the www prefix in order to be accessed.

To adjust the settings, follow these steps:

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

2. Click the **PREFERENCES** button to access the *Domain Preferences page*.

3. To utilize a mail bounce message, select the radio button for **Bounce with phrase** and enter the text that the mail bounce message is to contain.

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

5. Check or uncheck the **WWW prefix** checkbox to determine whether the given domain will allow the www prefix to be used to access the domain. If the box is checked, Internet users will be able to access a domain (i.e. domain.bogus) by

utilizing either the domain name itself or the domain with the 'www' prefix. If the box is unchecked it will not be accessible with the 'www' prefix (i.e. www.domain.bogus).

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

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

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

Accessing the Domain Report

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

- Domain owner (client)
- Domain status
- Creation date
- Hosting type
- Virtual host type
- IP Address
- FTP Login
- FTP Password
- Disk space limit
- Real disk space
- Traffic
- Real Traffic
- FrontPage support
- SSI support
- PHP support
- CGI support
- mod_perl support
- Apache ASP support

- SSL support

- Web statistics

- Web users

- Apache error docs

- Anonymous FTP

- Mailboxes

- Redirects

- Mail Groups

- Autoresponders

- Domain user

- Databases

To access the domain report, follow these steps:

1. Click the **REPORT** button at the *Domain Administration page* to see the domain's data and statistics.

2. From this screen, you can do several things:

   o 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.

   o You can access graphical site statistics for the domain by selecting the **WEBALIZER** option. This opens a separate window where you will see the site statistics for the given domain. It should be noted that Webalizer, by default, is set to update statistics for the domain once every 24 hours. If you attempt to access Webalizer before it has operated its first update you will receive a notice that Webalizer is either not running or has not yet been started.

   o To print a copy of the report, select **File/Print** in your browser and a paper copy of the report will print.

   o To return to the domain record, click **UP LEVEL** to close the report and to return to the *Domain Administration page*.

Managing Mail

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

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

- Create, edit or delete email boxes and edit individual mailbox quotas.

- Redirect or forward messages from one email address to another email address

- Create, edit or delete email groups (several individual accounts grouped together under one email address for convenient multi-copy messaging).

- Create, edit, or delete email autoresponders (automatic reply to email sent to the given mail name)

Mail Names page

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

1. Click the **MAIL** button at the *Domain Administration page*. The *Mail Names Management page* appears. From this page, users can:

    o Create a new mail name.

    o View a list of mail names currently existing under the specified domain. To the left of each domain name on the list there are four icons representing different mail account types. They are:

        ▪ Mailbox (represented by the "mailbox" icon)

        ▪ Redirects (represented by the "outgoing envelope" icon)

        ▪ Mail groups (represented by the "people" icon)Mail

        ▪ Autoresponders (represented by the "revolving envelope" icon)

    o Click on a specific mail name to access to the *Mail Name Properties Page* for that given name.

    o Search the mail names list for a certain pattern. It may help you in case you have a great number of mail names in the system and you need to work with a particular one. To search the list, type the pattern string in the text input field and click **SEARCH**.

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

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

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

3. The new mail name appears on the mail names list.

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

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

1. Click the **MAIL** button at the *Domain Administration page*. The *Mail Names page* appears.

2. In the **Mail names list**, click on the name you want to edit. You then access the *Mail Name Properties page*.

3. The mail name is listed at the top of the page. To change the mail name, click in the name field, change the name, and click **UPDATE**.

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

*   Mailbox Accounts and Quotas

*   Mail Redirects

*   Mail Groups

*   Mail Autoresponders

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

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

NOTE: An administrator or/and Client can limit the number of mailboxes a Domain User can have for a given domain.

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

1. Click in the check box provided next to **Mailbox**.

2. When enabling a mailbox for the first time for a mail name account, you must enter a password.

3. The **Old Password** will say "NONE" if you have yet to enter a password. Once it is entered, the password cannot be viewed from this screen.

4. To enter a password, click in the **New Password** text box and enter the selected password.

5. To properly update the password, you must re-enter the password in the **Confirm Password** text box.

6. To set up the mailbox quota, select the **Default for domain** radio button to set the limit to the maximum available in the given domain, or select **Enter size** and enter the quota you wish to set, in KiloBytes, for the given mailbox. Note that this limit may not exceed the default set for the domain.

7. Once you have enabled the mailbox, entered the passwords and set up mailbox quota, click **UPDATE** to submit the information.

8. To change a password, simply re-enter the new password in the **New Password** text box, re-enter this password in the **Confirm** text box, and click **UPDATE**.

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

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

- Temporarily forward mail when someone is unavailable to receive it

- Send mail to a new mail box if a mail box user is leaving the organization

- Forward mail to a new account which will eventually replace an old mail box (e.g. someone is changing their mailbox name but hasn't had time to inform all correspondents of the change yet)

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

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

1. Click in the check box provided next to **Redirects**.

2. In the text field to the right, enter the appropriate address to which to forward mail sent to this mail name.

3. To change the redirect address for a given mail name, click on the existing entry in the **Redirects** box and change it to the new address.

4. Click the **UPDATE** button to enter these changes.

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

Manage Mail Groups

A mail group is a list of several email accounts that are grouped together under one email address for convenient multi-copy messaging. For example, if you want to send the same message to 5 people in the programming department, you can create a "Programming" email group that includes the individual email addresses for all 5 staff members. So, when someone sends a message to the Programming email group, he/she only types and sends one message. Copies of the message are emailed to all 5 individuals. By using mail groups, the sender does not need to know each individual's email address, just the group name. In this way, mail groups save time.

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

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

1. Click in the checkbox provided next to **Mail Groups**.

2. To create a new mail group, ensure the box is checked, then click the **ADD** button.

3. The **Add Mail Groups** box appears.

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

4. To add an external mail address to a Mail Group, fill in the correct address in the **enter external recipient mail** text box, and click **ADD**.

5. To add an existing account from the same domain, click on the desired address in the **Select registered users** list, and click **ADD**.

6. The selected addresses will appear in the box to the right of the mail groups checkbox on the *Mail Name Properties page*.

7. To delete one or more group members, highlight the selected group member in the box to the left of the mail group check box. Click the **REMOVE** button.

8. A warning will appear. Click **OK** to confirm that you want to delete the address from the mail group.

9. After completing your changes, click **UPDATE** to submit all changes.

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

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

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

1. To first enable autoresponders for a mail name account, click in the checkbox provided next to **Mail autoresponders.** When the check appears, autoresponders are enabled for the mail name. If you click again, it will uncheck the box, and autoresponders will be disabled.
2. For the Autoresponder feature you have the option to include file attachments. To include a file to be selectable within the set up of autoresponders for the given mail name, use the **Browse** button to search for and select the desired file(s). (File sizes should be limited to no more than 1MB.)
3. Click the **SEND FILE** button. The attachments will then appear in the **Repository.**
4. These files will be available for any autoresponders that are set up for the given mail name. To delete one or more files highlight the desired file(s) and click the **REMOVE** button. A warning will appear prior to deleting the selected file(s).
5. To add a new mail autoresponder, click the **ADD** button.
6. A pop-up screen prompts you to enter a name for the autoresponder. Enter the desired identification name, and click **OK** to submit.
7. The *Edit Mail Autoresponder page* appears.
   - The selected autoresponder name is listed for the given mail name account. You can click in the text box where the autoresponder name is listed, and edit the name. Click **UPDATE** to submit.
   - The ON/OFF status for the autoresponder is shown. **[ON]** indicates that the autoresponder is on. **[X]** indicates that the autoresponder is off. You can adjust this setting by clicking the **ON/OFF** button. This status icon also appears on the autoresponders list on the *Mail Names Properties page*.
   - Beneath the Request text input box, you can determine whether an autoresponder responds to specific text found within either the subject line or body of the incoming email, or if it responds to ALL incoming requests
   - To set up the autoresponder to always respond, regardless of the contained text, click the bottom radio button for **always respond**.

- Using the **Request text** input box and radio buttons, you can set up the autoresponder to send an auto response when an incoming request contains defined text in its subject line or body.
- Click the **in the subject** radio button to respond to specific text in the subject of the request, or click the **in the body** radio button to respond to specific text in the body of the request.
- You can select a specific subject to appear in your autoresponder using the **Answer with subject** optoin. To simply respond with the same subject as was received from the incoming request select the radio button for the default setting. To specify a specific subject line select the radio button beside the text box and enter the desired text.
- You can enter text to be included in the autoresponder in the **Answer text** field.
- Using the **ADD** and **REMOVE** buttons, you can attach files to be included in the autoresponder. These files must be uploaded into the **Repository** on the *Mail Names Properties page*. Select the uploaded file from the **Attach files** list, and use the **ADD** button to attach the file to the autoresponder. Click **REMOVE** to remove a file.
- You can specify the frequency at which the autoresponder responds to the same unique address, after receiving multiple emails from it. By clicking in the appropriate radio button next to **Reply To Unique Email Address**, you can set the autoresponder to **always** respond, to respond **once**, or to respond once per a specified number of **days**. The default setting is to respond once in one day to unique mail addresses. It is highly recommended that you leave this setting, or set to respond once in a given number of days. Selecting always respond can potentially overload your mail server. If the days value is defined as "0", then the autoresponder will respond each time a request is received.
- You can define the number of unique addresses that the autoresponder will remember. Enter the desired number in the **Store up to:** field.
- This memory enables the system to implement the answer-frequency and respond-once functionality. In the event of extremely high mail volume, to protect server performance, you can limit the address memory of the system database.
- To specify an email address to which incoming requests are forwarded, enter the new email in the **Forward request to e-mail** field. Email requests meeting the properties established on this page will be forwarded to this alternate email address.
- Click the **UPDATE** button to submit all changes.

View DNS Settings

Through PSA, a Domain User can view the DNS settings for the owned domain set by the Administrator or the Client.

DNS Settings Page

There are five types of accessible DNS records:

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

You can access the DNS Settings page by clicking the **DNS** button at the *Domain Administration page*.

View Hosting Settings

You may have hosting privileges established in your domain so that you can provide various Internet services (e.g. software applications, a forwarding address, and FTP transfers). PSA allows three different types of hosting services:

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

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

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

The system administrator has already performed all the technical system administration for hosting services relating to your domain; however, the type of hosting service set up for your domain determines the extent to which you can manage your hosting parameters. If you have physical hosting, you can use FTP software to access your hosting directions. Additionally, you can change the FTP password. If frame or standard forward hosting is set for this domain, than you can change (or toggle between these two types) forwarding for the given domain.

Follow these steps to administer your hosting services:

1. Click the **HOSTING** button at the *Domain Administration page*.

2. If you have a forwarding hosting set up for you, a page with a choice of types of hosting appears. Choose the type and click **NEXT** to proceed.

3. If the type of hosting is physical then you will be taken directly to the Physical *Hosting Configuration page*.

Physical Hosting Configuration

There are several physical hosting services for your domain. They are configurable only by the Administrator or the Client:

- FTP services. You may want to change the password occasionally for security purposes.

- FrontPage support

- SSI

- PHP

- CGI

- mod_perl

- Apache ASP

- SSL

- Web statistics

- Apache ErrorDocs

Forwarding Configuration

If you have either of the two forwarding options defined for your hosting services, standard or frame, then you can change between the two types of forwarding. Also, you can edit the URL to which domain transactions are re-directed or forwarded.

1. To change the type of forwarding you have, from the *Hosting page*, click on the type you want to change.

   NOTE: Confirm that you really need to change the type of forwarding before actually changing it. Only a Plesk administrator can change a forward hosting account to physical hosting. A Domain User cannot make this change.

2. Click **NEXT** to access the URL page.

3. To change the forwarding address, click in the **URL** text box and enter or edit an Internet address to which you wish to re-direct all domain traffic.

4. Click **UPDATE** to submit changes.

Web Users Management

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

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

- Select any web user name to edit the web user password and/or to add or remove different scripting options.

- Search the web users' list for a certain pattern. It may help you in case you have a great number of web users in the system and you need to work with a particular one. To search the list, type the pattern string in the text input field and click **SEARCH**.

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

To create a new web user:

1. Click the **WEB USERS** button at the *Domain Administration page*. The *Web Users page* appears.

2. To add a web user, enter the **Web User name** in the text box provided next to **Web user name:** and click **ADD**.

3. You are taken to the *Web User Password Entry Page*, where you must enter and confirm the password for your new web user and select from the available scripting options for the given domain (availability of scripting options is set in the Domain Preferences). To do this, enter a password in the **New password** text box, and then re-enter it in the **Confirm password** text box. Then select from the available scripting options if applicable. Once you have completed all entries, click on **UPDATE** to enter the information. Selecting **UP LEVEL** will return you to the *Web Users page* without assigning a password or scripting capabilities to the given web user. Although the directory will be created, it will not be accessible via FTP using the web user name.

4. As you create web users, the user names appear on the *Web User Management page* in the web user list.

5. To change web user passwords or edit scripting options, click on the user name in the web user list. This takes you to the *New Password page*.

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

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

Important Notes on web users:

- For security purposes, the password must be between 5 and 14 characters and cannot contain the user name.

- Each web user creates a system account within Apache; therefore, you cannot have two web users with identical names on the same server.

- New web users can access the directory using FTP software by entering the domain name under which the web user account was created and using the appropriate web user name and password.

- Your administrator CAN limit the number of web users you can create. You will receive a warning if you try to exceed this number, and will not be able to do so.

Protected Directories

This feature is active if virtual hosting (physical hosting account) has been configured for your domain. It creates secure directories in your virtual domain, in which to place documents. Secure directories are recommended to ensure security of confidential and private information. It is possible to create directories under either the standard virtual host accessible via http protocol, or if applicable for the given domain, under the SSL virtual host accessible via https protocol. Icons are used next to each directory name in the directory list to define which virtual host type (SSL or non-SSL) the directory resides within. An open lock depicts non-SSL; a closed lock depicts SSL.

Creating a Protected Directory
Follow these steps to create secure directories for the domain:

1. Click the **DIRECTORIES** button from the *Domain Administration page*. The *Protected Directory Management page* appears.

2. To create a new directory, click the **ADD** button.

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

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

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

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

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

8. Click the **ADD** button.

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

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

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

12. To access a directory user in order to edit the user password, click on the user name in the list, and you will again be taken to the directory user password screen. Here you can edit the password.

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

14. Click **UP LEVEL** to return to the *Protected Directory Management page* without saving any changes.

Changing a Protected Directory
You can edit a protected directory definition to:

- Add a user

- Change a password

- Delete a user

- Rename the directory

- Change header text

- Change the SSL status

Follow these steps to edit protected directories:

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

2. Click the **DIRECTORIES** button. The *Protected Directory Management page* appears.

3. Click on any directory from the list that you wish to change.

4. You will be taken to the *Protected Directory Control page*.

5. From here, you can edit the directory by following the same steps outlined above, in the **Creating a Protected Directory** section.

6. Click **UPDATE** to complete all changes to the system and to return to the *Protected Directory List page*.

Searching the Protected Directories List

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

- Select the input field and type in the pattern string.

- Click the **SEARCH** button.

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

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

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

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

Removing a Protected Directory

To remove one or more directories, follow these steps:

1. Check the checkboxes in the **Del** column of the Protected Directories List corresponding to the directories you wish to remove.

2. Click on **REMOVE SELECTED**. The *Protected Directory Removal page* appears.

3. For every directory you chose to remove the name of the directory and the names of this directory users will be displayed.

4. If you are certain that the displayed information is correct and wish to proceed with deleting, check the "Yes, I have read, understood, and agree to remove protect from these domains" checkbox. Then click **SUBMIT**. If you decide to not delete these directories or wish to modify the list of directories chosen for deletion, click the **CANCEL** button.

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

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

Manage the Domain SSL Certificate

PSA enables you to upload a Secure Socket Layer (SSL) Certificate, generate a Certificate Signing Request (CSR), generate a Self-signed Certificate, and/or purchase a SSL certificate through a registered certificate authority. Each certificate represents a set of rules used when exchanging encrypted information between two computers. Certificates establish secure communications; this is especially important when handling e-commerce transactions and other private transmittals. Only authorized users can access and read an encrypted data stream.

Notes on Certificates:
- In order to use SSL certificates for a given domain, the domain MUST be set-up for IP-Based hosting.
- When an IP-based hosting account is created with SSL support, a default SSL certificate is uploaded automatically. However, this certificate will not be recognized by a browser as one that is signed by a certificate signing authority.
- The default SSL certificate can be replaced by either a self-signed certificate or one signed by a recognized certificate-signing authority. The self-signed certificate is valid and secure, but many clients prefer to have a certificate signed by a known Certificate Signing Authority.
- If using a SSL certificate issued by a certificate authority other than Thawte or Verisign, a rootchain certificate is required to appropriately identify and authenticate the certificate authority that has issued your SSL certificate.
- If the given domain has the **www** prefix enabled, you must set-up your CSR or self-signed certificate with the **www** prefix included. If you do not, you will receive a warning message when trying to access the domain with the **www** prefix.

- Remember to enter your certificate information in PEM format. PEM format means that the RSA Private Key text must be followed by the Certificate text.
- All certificates are located in the ../vhosts/<domain name>/cert/httpsd.pem file. Where this directory reads <domain name> , you must enter the domain name for which the certificate was created.

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

1. If you have established an IP based hosting account with SSL enabled, the **CERTIFICATE** button at the *Domain Administration page* will be enabled.

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

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

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

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

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

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

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

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

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

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

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

1. Click the **CERTIFICATE** button at the *Domain Administration page*. The *SSL Certificate page* appears.

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

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

To upload a new certificate:

1. Click the **CERTIFICATE** button from the *Domain Administration page*. The *SSL Certificate page* appears.

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

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

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

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

   EXAMPLE FORMAT:

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

   [[ECRYPTED BLOCK OF TEXT]]

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

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

   [[ECRYPTED BLOCK OF TEXT]]

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

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

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

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

1. Click the **CERTIFICATE** button at the *Domain Administration page*. The *SSL Certificate setup page* appears.

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

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

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

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

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

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

Anonymous FTP

Within PSA there can be an Anonymous FTP access set up by the Client or the Administrator, for IP-based virtual host only though. Anonymous FTP is used to allow an open, yet controlled, environment for visitors to the domain to download and/or upload files to and from the domain account. Users will be able to log into ftp.<domain name> with the standard anonymous user name and any password. PSA allows the setup and limitation of incoming file space, connected users, and bandwidth usage throttling. Administrators should take care when allowing the use of anonymous FTP and be sure to use all the limitation capabilities within the interface wisely. If setup with excessive limits, it could lead to problems with server resources as well as excessive bandwidth usage. As the Domain User you can view the status of Anonymous FTP for your domain. To do that, click the **ANONYMOUS FTP** button at the *Domain Administrator page*.

Databases

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

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

Searching the Database List

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

- Select the input field and type in the pattern string.

- Click the **SEARCH** button.

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

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

- The button **SHOW ALL** will revert to displaying the whole list of databases.

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

Creating a New Database

1. Click the **DATABASES** button at the *Domain Administration page*. The *Databases Feature Management page* appears.

2. To add a new database select the **Database name** field, enter the desired name, and select **ADD**. The *Database Editing page* appears.

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

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

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

6. To add further databases, follow the steps outlined in 1-5 above. To return to the *Domain Administration page* select **UP LEVEL**.

Editing an Existing Database

1. Click the **DATABASES** button at the *Domain Administration page*. The *Databases Feature Management page* appears.

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

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

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

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

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

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

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

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

10. To edit further databases, follow the steps outlined in 1-9 above. To return to the *Domain Administration page* select **UP LEVEL**.

Domain User

Logging in

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

Changing the password

As the Domain User you can change the password that you use to log in to PSA. To do that, click the **DOMAIN USER** button. The *Domain User Properties page* appears.

There, to change password, enter the new password into the **Password** input field and confirm it in **Confirm password** input field.

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.