

cPANEL USER MANUAL

CPANEL USER MANUAL

Welcome to your cPanel Manual.

The purpose of this manual is to provide as much information as possible to you on the features of cPanel.

The titles in the Table of Contents follow the same structure as the cPanel user interface.

Note that this manual has been compiled from information taken from official cPanel documentation. The relevant articles were adapted to fit with what is available on your cPanel.

The original articles may be found at

http://twiki.cpanel.net/twiki/bin/view/11_24/CpanelDocs/WebHome

Your cPanel version is 11.24.5 stable.

Table of Contents

WHAT IS cPANEL?	1
ACCESSING cPANEL	2
cPANEL HOME SCREEN	3
PREFERENCES	
<i>Getting Started Wizard ...an easy way to start if you're new to cPanel.</i>	
Language	4
Introduction to Web Hosting	4
Web Disk Accounts	5
Note for Windows® Vista Users	5
New Email Account Setup	6
Set Default Address	7
Webmail	8
Contact Info and Preferences	9
Manage SSH keys	10
<i>Other features</i>	
Change Style	11
RVSkin Theme Changer	11
Video Tutorials.....	12
Change Password	12
Update Contact Info	13
Shortcuts	13
MAIL	
<i>Email Accounts</i>	
Change the Quota Limit	14
Configure an Email Client	15
<i>Spam Assassin™</i>	
Automatically Delete Spam.....	16
Enable the Spam box	16
Configure SpamAssassin	17
Set Required Spam Scores	17
Add Addresses to the Black List	17
Set Individual Test Scores	17
Add Addresses to the White List	18

Table of Contents

<i>Forwarders</i>	
Add a Mail Forwarder.....	19
Using the Pipe to Program option.....	20
Remove a Mail Forwarder	20
Add a Domain Forwarder	20
Delete a Domain Forwarder	21
<i>Auto Responders</i>	21
Add an auto responder	21
Delete an auto responder	22
<i>Mailing List</i>	22
Add a mailing list	22
Modify a Mailing List	23
Change Mailing List Password	23
Delete a Mailing List	23
<i>User Level Filtering</i>	24
Add a User Level Filter	24
Test a Custom Filter	25
Edit a Custom Filter	25
Remove an Existing Filter	25
<i>Account Level Filtering</i>	
Add an Account Level Filter	26
Test a Filter	27
Edit a Custom Filter	28
Delete an Existing Filter	28
<i>Email Delivery Route</i>	29
Test a Delivery Route.....	29
<i>Import Addresses/Forwarders</i>	29
Adding email addresses using a Spreadsheet or CSV file	30
<i>Email Authentication</i>	31
Set up Domain Keys	31
Set up SPF	31
Advanced Settings	32

Table of Contents

MX Entry.....	33
Configure Email Routing	33
Add a New MX Entry	34
Delete an MX Entry	34
Edit an MX Entry	34

FILES

Backups

Full Backups.....	35
Create a Full Backup	35
Download a Full Backup	36
Store a Backup File Remotely	36
Partial Backups	36
System Backups	36
Restore the Site from the Backups Link	
Excluding Files from Backup	

Backup Wizard

Back up Your Entire Site	37
Create a Partial Backup	38
Restore a Portion of Your Site	38

File Manager.....	39
--------------------------	-----------

Legacy File Manager.....	40
---------------------------------	-----------

Web Disk

Configure the Web Disk	41
Note for Windows® Vista Users	41
Access a Web Disk Account	42
Change the Web Disk Password	42
Delete a Web Disk Account	42
Password Protect a Web Disk Directory	43
Create a User to Access a Protected Web Disk Directory	43
Remove an Authorized User	43

Disk Space Usage.....	44
------------------------------	-----------

Delete Files.....	44
Drop Down Menu	45

Table of Contents

<i>FTP Accounts</i>	45
Add an FTP Account	46
Configure an FTP Client	47
FTP Session Control	48

LOGS

<i>Latest Visitors</i>	48
<i>Bandwidth</i>	49
<i>Webalizer</i>	
Webalizer FTP.....	50
<i>Raw Access Logs</i>	51
Configure Logs	51
Download and View Raw Access Logs	51
<i>Analog Stats</i>	52
View Analog Stats.....	52
<i>Error Log</i>	52
<i>Choose Log Programs</i>	52
<i>AWStats</i>	52

SECURITY

<i>Password Protect Directories</i>	53.
Remove a User	53
Remove Password Protection	53
<i>IP Deny Manager</i>	
Deny/Ban an IP Address	54
Unban an IP Address	54
<i>SSL/TLS Manager</i>	
Add a Private Key	55
Upload an Existing Key	55
Generate a new Key	56
Add a Certificate Signing Request	56
Add a Certificate	56
Upload an Existing Certificate	56
Generate a new Certificate	57

Table of Contents

<i>SSH/Shell Access</i>	57
Connecting with Putty	58
Connecting with Mac OS X or Linux	58
Manage SSH Keys	58
Generate a new Key	59
Import an Existing Key	59
Connect using Java SSH.....	60
Connect using Java Telnet Applet	60
 <i>HotLink Protection</i>	
Enable Hotlinks Protection.....	61
Disable Hotlinks Protection	61
 <i>Leech Protect</i>	
Enable Leech Protect	62
 <i>Add a GnuPG Key.....</i>	63
Add a Key	63
Import a GnuPG Key.....	63
Delete or View a GnuPG Key	63
 DOMAINS	
<i>Subdomains.....</i>	64
Add a Subdomain	64
Enable or Disable Subdomain Redirection	65
Remove a Subdomain	65
Search Subdomains	65
 <i>Addon Domains</i>	66
Create an Addon Domain	66
Enable or Disable Addon Domain Redirection	66
Remove an Addon Domain	67
Search Addon Domains	67
Addon vs. Parked Domains.....	67
 <i>Parked Domains</i>	68
Create a Parked Domain	68
Enable or Disable Parked Domain Redirection	68
Remove a Parked Domain	69
Search Parked Domains	69

Table of Contents

Redirects —

Create a Redirect	70
Remove a Redirect	71
Search Existing Redirects	71

DATABASES

<i>MySQL® Databases</i>	72
Create a Database	72
Check a Database for Errors	72
Repair a Database	73
Create a Database User	73
Define a User's Privileges	74
The Current Databases Table	74
Search Databases	74
Modify a User's Privileges	75
Remove a User from a Database	75
Delete a Database	75
Delete a MySQL User	75
<i>MySQL Database Wizard</i>	76
<i>phpMyAdmin</i>	76
<i>Remote MySQ</i>	77
<i>PostgreSQL Database</i>	77
<i>PostgreSQL Database Wizard</i>	77
<i>phpPgAdmin</i>	77

SOFTWARE/SERVICES

<i>CGI Center</i>	78
Simple CGI Wrapper	78
Random HTML Generator	79
Simple Guestbook	80
Add a Guestbook	80
View a Guestbook	80
Delete Guestbook Entries	81
The Edit Default CGI and Edit Guesbook Template Links.....	81
Counter (Add a Counter, Clock or Date)	81
Clock.....	82
Countdown	83
CGI Email	83

Entropy Search	84
Entropy Banners	84
Configure Rotating Banners	84
Control a Banner's Schedule	85
Add Rotating Banners to a Page	85
<i>Site Software</i>	85
<i>Perl Modules</i>	86
View Available Perl Module	86
Search Available Perl Module	86
Install a Perl Module.....	86
The Installed Perl Module Table	86
System Modules	87
<i>PHP PEAR Packages</i>	87
View Available PEAR Packages	87
Search Available PEAR Packages	87
Install a PEAR Package	88
The Installed PHP Extensiion(s) and Application(s) Table	88
System Modules	88
<i>PHP Configuration</i>	88
PHP Directives	89
PHP Configuration	89
Select a PHP version	90
<i>RubyGems</i>	90
<i>Ruby on Rails</i>	90
<i>Optimize Website</i>	91
<i>RVSite Builder</i>	92
<i>Fantastico deLuxe</i>	92

ADVANCED

<i>Apache Handlers</i>	93
<i>Image Manager</i>	94
Thumbnailer	94
Convert Images to Thumbnail	94
Image Scaler	95
Scale an Image	95
Rescale an Image	95
Convert an Image Format	96
<i>Index Manager</i>	97
<i>Error Pages</i>	97
<i>Cron Jobs</i>	98
<i>FrontPage® Extensions</i>	99
<i>Network Tools</i>	100
<i>Submit a Support Request</i>	101

<i>Virus Scanner</i>	101
<i>MIME Types</i>	101
 Password Generator	 102
 cPANEL GLOSSARY	 103

SYMBOLS USED IN THIS MANUAL:



Take Note



A suggestion or idea



Warning!



Remember or Important

Disclaimer:

While every care has been taken in the compilation of this cPanel User Manual, no responsibility is taken if there are errors contained herein. If in doubt about any of the information given herein, please Google to find answers or go to the the source, at http://twiki.cpanel.net/twiki/bin/view/11_24/CpanelDocs/WebHome

What is cPanel?

cPanel is an easy to use graphical interface for website maintenance. cPanel is the leading web hosting control panel available today. Even a user completely new to web hosting can easily manage his/her own website. With the cPanel hosting interface, you'll have complete control over your website. When looking for a hosting package, cPanel is also a good indicator of the reliability of the hosting provider. The most well known and reliable web hosts would normally provide web hosting plans that are powered by cPanel control panel. cPanel hosting plans that are on the market predominantly support PHP and MySQL, FrontPage, Fantastico and RVskins (as do our hosting plans.)

Essentially, what cPanel does is that it condenses the dozens of commands needed to complete one task to a single mouse click. cPanel takes care of tedious and complicated tasks, such as a simple change to the content of your web page, password protecting portions of your web site, or deleting a table in one of your databases. All these can easily be done just by some minor input from within cPanel.

In summary, cPanel is an integrated program that combines the requirements of basic to advanced users in one user-friendly interface. It definitely will save you a lot of time as well as the hassle of completing your tasks manually. The best fact is that it is directly linked to Fantastico, enabling users to access, with often just one click, a multitude of programs that are extremely useful for managing websites.

Accessing cPanel

To access cPanel:

1. Type: <https://IP:2082> into your preferred Internet browser.
 - o **IP** is meant to stand for your website's [IP address](#).
 - o After approximately one week of starting your website, you will be able to access your cPanel interface by replacing the [IP address](#) with your [domain name](#).
2. Enter your cPanel username into the *Name* field.
3. Enter your password into the *Password* field.
4. Click *Login*.
 - o You will be greeted by a cPanel startup page on your first login. We strongly recommend completing the [Getting Started Wizard](#).



A colon symbol following an [IP address](#) or domain name denotes a specific port number. These port numbers are responsible for guiding data packets transmitted between 2 computers to specific processes taking place on either machine.



If you bookmark the *Login* page before you actually log in, you will be able to find it easily later.

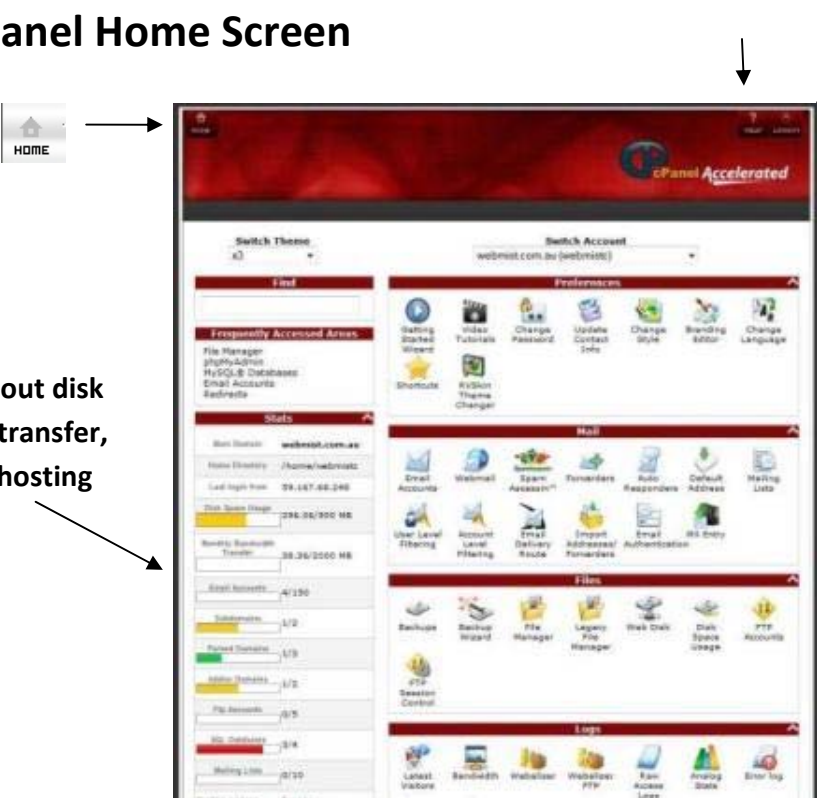


Alternatively, click on [Shortcuts](#) on cPanel. You will see you can drag the text to your desktop.

If choosing to drag to your desktop you'll see it becomes a browser icon. If you think you'll get it confused with your browser, how about an actual cPanel icon? You can right click and save the one below as an easier- to-identify link.



The cPanel Home Screen



The screenshot shows the cPanel Home Screen with several annotations:

- An arrow points from a **HOME** button to the top-left corner of the main window.
- An arrow points from a **LOGOUT** button to the top-right corner of the main window.
- An arrow points from the text "Info here about disk space, data transfer, databases, hosting package etc" to the "Disk Space Usage" section on the left side of the screen.
- An arrow points from the text "The main window" to the right side of the main window.

Info here about disk space, data transfer, databases, hosting package etc

LOGOUT button at the top right corner of the main screen, and the **Logout** link at the bottom of the screen, allow you to log out of your cPanel account. **IMPORTANT:** Be sure to log out if you are using a computer with shared access.


The main window

The cPanel home screen provides access to all of your cPanel functions. You can reach the cPanel home screen from anywhere in the interface by clicking the **Home** button at the top left corner of the screen, or the **Home** link at the bottom of the screen. From the Home screen, you can reach any of cPanel's features.


Clicking the **Help** button (or the Help link at the bottom of the screen) opens a pop-up window with information regarding the feature you have accessed within the cPanel interface. The contents of the **Help** menu change, depending on where you are in the interface.

Help should be consulted any time you have trouble using a feature in cPanel. The **Help** link offers 2 options at all times: (see the bottom of the Help window)

[Video Tutorials](#) — Click to view a list of the video tutorials available from cPanel.

 You will not hear sound while viewing the videos.

[Full Interface Documentation](#) — Click to access this documentation.

 This documentation may also be found by clicking the Documentation link at the bottom of the cPanel window.

PREFERENCES –

Getting Started Wizard

The Getting Started Wizard appears on your first login to cPanel and will guide you through configuring some basic preferences. **We strongly recommend completing this process.**

This wizard functions as a guide to setting up a new account. If, for whatever reason, the start-up wizard is not presented on the first login, or if it is necessary to reconfigure your account, you can access the start-up wizard by clicking the *Getting Started Wizard* icon in the *Preferences* area of the cPanel interface.



The icons covering the following subjects are shown separately in the cPanel window. We have shown them here as they also appear in the *Getting Started Wizard*.

Language/Change Language

This feature defines the default display language of the cPanel interface. To change the default language:

1. Select a language in the pull-down menu.
2. Click *Change*.

Introduction to Web Hosting

These screens contain information and set-up help on an array of topics including the disk directories, getting files to your website, the [File Manager](#), [Web Disk](#), and [FTP Accounts](#). **If this is your first website, we strongly recommend reading through these pages to get gain a better understanding of web site management.**

PREFERENCES – *Getting Started Wizard* *continued* -

Web Disk Accounts

cPanel offers a **Web Disk** application wherein files can be managed and manipulated using your operating system's interface. Newer users may be most comfortable with this file management method.

The **Web Disk** will open a window on your computer, allowing new files to be moved, deleted, or added to the **server**, just as you would manage files on your personal computer.

To log into a **Web Disk** account:

1. Click the *Access Web Disk* button.
2. Choose your operating system (OS): *Windows*®, *Mac*®, or *Linux*.
 - **Remember:** Choose the version or distribution of your operating system using the pull-down menu.
3. Click *Go* under the appropriate operating system to download the script file.
4. Open and run the script file, accepting any certificates.

When the **Web Disk** configuration is completed successfully, a new window containing your website's content will be opened on your computer. From this window, your website's files can be managed just like you would manage files on your personal computer.

Once you have added a **Web Disk** account to you **server**, it can be accessed quickly in the future by clicking the *Access Web Disk* button at the main **Web Disk** page. You are also able to change the password, delete, or password protect directories for existing **Web Disk** accounts under the *Actions* heading in the **Web Disk Accounts Management** list.

Note for Windows® Vista Users

If you are running Windows Vista on your desktop, you will need to download a patch from Microsoft's website in order to use Web Disk. You can find the patch [here](#).

PREFERENCES – *Getting Started Wizard* *continued* -

New Email Account Setup

This feature allows you to set up any new email accounts you would like to use. To begin with, set up an account by which visitors to your site can contact you. This can be changed later of course.

To create a new email address:

1. Enter the address you would like to use into the Email field.
 - o Don't forget to set the domain with the pull-down menu, to the right of the Email text field.
2. Enter the new password into the Password field.
 - o You can use the Generate Password link to have a strong password generated for you. For more information, read our [Password Generator](#) documentation.
3. Confirm the password in the Password (Again) field.
4. Set the maximum amount of disk space this email address will be allowed to use in the Mailbox quota field.



Remember: This setting is optional.

5. Click Create Account.



The quota defines how much hard drive space the account will be allowed to use. If you redirect your mail to your private email address, and clear the inbox regularly, you will not exceed your quota.

PREFERENCES – *Getting Started Wizard* *continued* -

Set Default Address

Your default email address is listed under the *Default Email Account* heading. This is a special email account set up when your cPanel account is created by your web host. **The account's username and password are the same as your cPanel account name and password.**

This address will receive any mail sent to an invalid email address for the current domain. The default address is also commonly called a “catch-all address.”

It is possible to define how the default address handles the incoming messages.

To set up your default address:

1. Click one of the following options:
 - *Forward to email address* — Enter the address in the text box.
 - *Discard with error to sender* — Enter an error message for the sender to read.
2. You can also click *Advanced Options* to:
 - Discard incoming messages without an automatic response. (Note that this option is not recommended since the sender will be unaware that the delivery failed.)
 - Automatically forward messages to a program by defining a path to the program, for example `/home/$utility`, in the *Pipe to a Program* field.
3. Click the *Change* button.
4. Click *Next Step*.



If your domain is targeted by spammers, forwarding mail to a default address is likely to yield a large amount of **spam**. Make sure you read the information on Spam Assassin.



You can check and delete the mail received by this account. To do this via webmail, click *Access Webmail*.



The default address cannot be deleted or renamed, and it has no quota. It cannot be used for sending email. For this reason, we recommend creating an email account for daily use.

PREFERENCES – *Getting Started Wizard* *continued* -

Webmail

Webmail allows you to access your email accounts through a web browser such as Internet Explorer® or Safari®. The main advantage to checking your email via the web, rather than an email application on your computer, is that you can easily access your email account from any computer with an Internet connection and a web browser.

To use webmail:

1. Click *Webmail* then *Go to webmail login*.
2. Enter your password.
3. Select a webmail client.

The email account will be opened through your browser. The webmail client will then retrieve all read and unread messages associated with your email account.

You may also log into webmail without accessing cPanel by entering `https://example.com:2096` into your web browser, where your domain name would be entered in place of `example.com`. Once you provide your username and password, you will be able to select a webmail client.



To create a shortcut, drag the *Access cPanel Webmail* link to your desktop or bookmarks.

When you are finished configuring webmail, return to this screen and click *Next Step*.

PREFERENCES – *Getting Started Wizard* *continued* -

Contact Info and Preferences

This function allows you to define the email address(es) at which the server should send you updates. These email addresses will function as the main contact point for notifying you of new information regarding your website.

It is recommended that you use an email address not affiliated with your website, as this could be useful if your website's email stops working.

To configure these preferences:

1. Enter the email address through which you would like to be contacted by the [server](#) into the first text field.
2. You may enter another email address through which you would like to be contacted by the [server](#) into the second text field.



Remember: This step is optional.

3. Use the 3 checkboxes to select when the [server](#) should contact you. An email can be sent when:
 - **Your disk quota is almost full:** This means that your website is close to reaching the maximum amount of disk space that you are allowed. A full disk quota results in you being unable to modify existing files or add new files to your website. Delete old or unused files, or upgrade your hosting plan, to fix this issue.
 - **Your bandwidth is reaching its limit:** This means that your website has received the maximum amount of traffic it is allowed. When your maximum bandwidth has been reached, people will no longer be able to access your website. You must upgrade your hosting plan to fix this issue. Otherwise, you must wait until the limit is reset. Usually this occurs at the end of the month.
 - **Your email accounts approach the quota:** This means that one of your email addresses is close to using the maximum amount of disk space it is allowed. Delete old email, or upgrade your hosting plan, to resolve this issue.
4. Click *Save*.
5. Click *Next Step*.

PREFERENCES – *Getting Started Wizard* *continued*

Manage SSH Keys

SSH keys are used when confirming a specific computer has the right to access your website's information through an **SSH** session.

Use the *Generate a new Key* and Import **Key** links to generate or import a **key**, respectively.

To generate a new **key**:

1. Click the *Generate a new key* icon.
2. Fill in the appropriate information.



It is important to consider your needs when choosing a **key** type, bearing in mind that **RSA** keys yield a faster confirmation of identity, while using **DSA** keys will speed up **key** generation and signing times. Select a **key** size using the pull-down menu.



Remember: A larger **key** size is more secure, but will yield a longer authentication time.

3. Click *Generate Key* to generate the new **SSH key** and automatically install it to the server.
4. Click *Next*.

To import a **key**:

1. Click the *Import Key* icon.
2. Choose a name for the **key**.
3. Paste the private and public keys into the 2 text boxes.
4. Click *Import*.
5. Click *Next*.

Once a **key** has been installed onto the **server**, it can be edited, deleted or downloaded using the appropriate links in the lists on the **Manage SSH Keys** page. Keys that are new to the **server** need to be authorized by using the *Manage Authorization* link. Please remember, the **key** will not work until it is authorized. The **key**, once authorized, can be unauthorized by using the *Manage Authorization* link and clicking *Deauthorize*.

Once you have finished setting up your cPanel account, click the *Home* button at the upper left corner of the screen to return to the home screen and begin using your cPanel account.

PREFERENCES – Other features

Style

Your cPanel offers 14 styles for you to choose from, including a style optimized for mobile web browsers.

To change your style:

1. Click the *Switch Style to ...* button corresponding to the style you wish to use.
2. Click *Next Step*.

RVSkin Theme Changer

Three options will appear, one of which is your current theme. To change the look of your cPanel check a different option and then click *Change*.

PREFERENCES – Other features

Video Tutorials

Clicking this icon will open a web page where various video tutorials can be accessed. This feature can be beneficial to new users who would like to get a feel for cPanel's workflow process.

The subject matter of the tutorials is divided into 3 categories:

- **cPanel 11** — Contains tutorials on many **key** features of cPanel, including **MySQL, Shortcuts, Subdomains**, and more. It is important to note that older versions of cPanel may cause a slightly different title to display here; for example, cPanel 10.
- **Branding** — Contains a number of video tutorials that will describe how to customize the look of your cPanel interface.
- **Mail** — Contains video tutorials about the general setup and maintenance of the cPanel mail features including **BoxTrapper, Forwarders, Mailing Lists**, and more.

The interface offers a high- and a low-quality version of each video. The *High Quality* link is intended for users with faster broadband connections, while the *Low Quality* version is intended for users on slower connections.

Change Password

This feature allows you to change your cPanel interface's main password. To change your password, you need to know your original password.

To change your password:

1. Key in the original password under *Old Password*.
2. Key the desired password into the *New Password* field.
 - Remember to use a secure password that contains no dictionary words, and is comprised of upper- and lower-case letters, as well as numbers and symbols.
 - You may use the cPanel **password generator** to generate a secure password by clicking the *Generate Password* button.
3. Confirm the new password by entering it into the *New Password (again)* field.
4. Click *Change your password now!* to save the new password

PREFERENCES – Other features

Update Contact Info

This feature allows you to change your primary contact email addresses. These email addresses will function as the main contact points for notifying you of new information regarding your website.

It is recommended that you use an email address not affiliated with your website, as this could be useful if your website's email stops working. A second contact email address can be added, if you have one.

The series of checkboxes below your email address(es) will determine the reasons you could be contacted. An email can be sent when:

- **Your disk quota is almost full** — This means that your website is close to reaching the maximum amount of disk space that you are allowed. A full disk quota results in you being unable to modify existing files or add new files to your website. Delete old or unused files, or upgrade your hosting plan, to fix this issue.
- **Your bandwidth is reaching its limit** — This means that your website has received the maximum amount of traffic it is allowed. When your maximum bandwidth has been reached, people will no longer be able to access your website. You must upgrade your hosting plan to fix this issue. Please [contact](#) me if this occurs and I will upgrade you as a matter of urgency.
- **Your email accounts approach the quota** — This means that one of your email addresses is close to using the maximum amount of disk space it is allowed. Delete old email, or upgrade your hosting plan, to resolve this issue.



Be sure to click *Save* to store the changes.

Shortcuts

A shortcut is an icon on the desktop or browser that will access a desired feature or application with a single click. You can create a shortcut to the cPanel by clicking, holding, and dragging the link(s) on this page to your desktop or browser toolbar. The shortcut will automatically be added to your toolbar or desktop.

If you'd like a cPanel icon you can use this one



(right click and save as image)

MAIL - Email accounts:

If you click on *Email Accounts*, you will see that existing addresses are displayed in a table. Using this table, it is possible to:

- See how much disk space the account is using.
- Change a password.
- Change a quota limit (that is, the size you want that mailbox to be).
- Delete an email address.
- Access an account through webmail.
- Configure a mail client.

Some of the above are explained earlier under the Getting Started Wizard heading – see the Table of Contents. Following is information on Changing Quota and Configuring an Email Client.

Change the Quota

The quota limit for an address defines the amount of mail (in Megabytes) that can be stored to its mailbox. Once this limit is exceeded, any incoming mail will be returned to the sender with a message stating that the recipient's mailbox is full.

When the quota is reached, new incoming messages will be stored on the server for a 48-hour period before being deleted. They will **not** be delivered to your inbox until you delete old emails.

Since a full quota will prevent you from receiving mail, it is important to keep track of quota usage.



You will not be able to exceed the total quota set by your web host for your email accounts.

To change a mail quota:

1. Click *Change Quota*.
2. Type the new email quota (in Megabytes) into the appropriate field. For an unlimited account, click *unlimited*.
3. Click *Change Quota* to store the new value.
 - If you do not wish to change the quota, click *cancel*.

MAIL - Configure an Email Client

This feature will automatically configure your email client to access your cPanel email address(es). An email client allows you to access your email account from an application on your computer. Outlook® or Outlook Express® and Apple® Mail are examples of email clients.



You must already have an email client installed on your computer in order to automatically configure it using cPanel.

To configure your mail client:

1. Select and download the appropriate configuration file from the list.
2. Run the script file to automatically configure a mail client for the selected address.

When completed properly, your email client should open automatically and log into your email account(s).



Note: If you wish to use an email client that is not listed in this interface, you will need to manually configure it. For more information on manually configuring an email client, review the documentation of the client you wish to use. Documentation can generally be found on the client's website.

Webmail

Webmail allows you to access your email accounts through a web browser such as Firefox, Internet Explorer® or Safari®. The main advantage to checking your email via the web, rather than an email application on your computer, is that you can easily access your email account from any computer with an Internet connection and a web browser.

To use **webmail**:

1. Enter your password.
2. Select a **webmail** client.

The email account will be opened through your browser. The webmail client will then retrieve all read and unread messages associated with your email account.

MAIL - SpamAssassin

SpamAssassin is an email utility that attempts to [filter spam](#) by examining every email, testing for [spam](#) characteristics. This results in an overall score. If a predefined score is reached, the message is discarded.

To enable SpamAssassin:

- Simply click the Enable SpamAssassin button on the SpamAssassin home screen.

Automatically delete spam

This function automatically deletes messages that meet or exceed the score limit. Activating this function can be accomplished using the *Auto-Delete Spam* button under the *Filters* heading.

Click the *Disable Auto-Delete Spam* button to disable this feature.



Enabling this feature could cause you to lose email that is not spam if a message meets or exceeds the defined score. Make sure SpamAssassin is configured properly for your account before using this feature.

Enable the spam box

Enabling the **spam** box will create an additional folder, named “**spam**,” where **spam** mail will be sent. This can be useful in preserving mail that may have mistakenly been filtered by SpamAssassin. It is recommended that you enable this feature.

This feature also comes with a *Clear* function that will delete the messages in the **spam** box.

It is possible to disable the **spam** box by returning to the SpamAssassin page and clicking *Disable Spam Box*.



If you check your mail via a **POP3** client, you must access and empty your **spam** box using the username `youraddress@example.com/spam` and your email account password. Otherwise, **spam** may accumulate in the **spam** box and cause you to reach your email account quota.

- Only the **spam** box may be accessed using the above address format; no other folders on your account are accessible in this way.

- While this is not an issue for **IMAP** and **webmail** users, all users should periodically check and delete the contents of the **spam** box.
- If you are unsure whether you use **POP3** or **IMAP** to receive mail, you may be able to find this information on your email application's *Preferences* screen.

Configure spam assassin

When you click *Configure SpamAssassin*, you can add email addresses that should be filtered automatically by typing the address into the `blacklist_from` box. A whitelist can be created in the same way at the bottom of the page. It is also possible to specify scores that SpamAssassin should use for each particular test.

Set required spam score

SpamAssassin examines every email message for **spam** characteristics, then assigns it an overall score. Enter the score required for a message to be considered **spam**.

5.0 is the default setting, and is aggressive. It would be suitable for a single user, but an ISP should set the default to be more conservative (8.0 or 10.0).

Add addresses to the blacklist

Enter addresses whose email is often allowed past the **spam filter**, but from whom you do not wish to receive email.

You may use `*` as a wildcard for multiple characters, or `?` as a single-character wildcard.

- `user@example.com` — Blacklists a single email address.
- `*@example.com` — Blacklists all the addresses at example.com.
- `?ser@example.com` — For example, `User@example.com` would be blacklisted, but `AUser@example.com` would not be blacklisted.

Set individual test scores

You can precisely tailor SpamAssassin for your **server** by assigning scores to individual tests. SpamAssassin uses hundreds of tests; please see the SpamAssassin documentation at <http://spamassassin.apache.org/tests.html> for more information. You will need to know which version of SpamAssassin is running on your **server**. To check your version of SpamAssassin, execute the following line of code on your **server**:

```
# perl -MMail::SpamAssassin -e 'print $Mail::SpamAssassin::VERSION."\n";'
```

You can enter individual test scores in the following format:

- “score” “TEST_NAME” “1 to 4 positive or negative numbers”

For example, you could enter:

- score INVALID_DATE 3.2 3.3 2.5 2.1

This example sets the scores that SpamAssassin assigns to a message with an invalid date in its header.



If only one number is listed, that score is always used for the test.

- Setting a score to 0 will disable the test.

In the example above, 3.2 is the first score, 3.3 is the second, 2.5 is the third, and 2.1 is the fourth. If you enter four numbers, as in the example, then the score that is used depends on whether Bayes and network tests are enabled in your installation of SpamAssassin.

- The first score is used when both Bayes and network tests are disabled.
- The second score is used when Bayes is disabled, but network tests are enabled.
- The third score is used when Bayes is enabled and network tests are disabled.
- The fourth score is used when Bayes is enabled and network tests are enabled.

Add addresses to the whitelist

- Enter addresses whose email is often blocked, but from whom you wish to receive email.
- You may use * as a wildcard for multiple characters, or ? as a single-character wildcard.
- user@example.com — Whitelists a single email address.
- *@example.com — Whitelists all the email addresses at example.com.
- ?ser@example.com — For example, User@example.com would be added to the whitelist while AUser@example.com would not be added.



Remember: Click *Save* to store the configuration changes.

- A whitelisted address is automatically allowed past the [filter](#). A blacklisted address will automatically be filtered by SpamAssassin. More details about configuring SpamAssassin can be found at <http://spamassassin.apache.org/>

MAIL - Forwarders

- This feature allows a copy of any email sent to one address to be forwarded to another address. This lets you use one account to check mail sent to several email addresses. You can also discard email or send (pipe) mail to a program.
- Please note that any email account with [BoxTrapper](#) enabled should use the *Box Trapper Forward List* feature. See the [BoxTrapper article](#) for more details.
- To view forwarders for a specific [domain](#) on your account, click the *Managing:* menu and choose the domain for which you wish to set forwarders.

Add a mail forwarder

To add a mail **forwarder**:

1. Click *Add Forwarder*.
2. You can choose from 3 options:
 - To forward mail, enter the address to which mail should be forwarded.
 - It is also possible to discard incoming messages and automatically send a failure notice to the sender. (Incoming messages can also be discarded without an automatic response under the *Advanced Options* link. That option is not recommended, however, since the sender will be unaware that the delivery failed.)
 - Messages can also be automatically forwarded to a program by defining a path to the program, for example `/home/$utility`, in the *Pipe to Program* field.
3. Click *Add Forwarder*.

To view the route a forwarded message takes, select *Trace* in the list of forwarded addresses. This makes it possible, for example, to locate a mail routing error.

★ Important: If you wish to forward mail to another account *without* receiving mail at your cPanel account, simply create a **forwarder** from an address that does not have a corresponding account in cPanel. Alternatively, if the account already exists, you can **delete it in cPanel**. Afterward, all mail will be forwarded to the destination you have configured using the Forwarders feature.

If you do not delete the cPanel account whose mail is being forwarded, then both accounts will receive mail.

Using the pipe to program option

When using the option to pipe incoming messages to a program, make sure your script uses the proper file permissions (755). To change your script's file permissions:

- **chmod 755 myscript.php** where myscript.php is meant to stand for your script's location and file name.

You will also need to ensure that you are using the correct hash bang.

- **#!/usr/bin/php -q** — For **PHP**.
- **#!/usr/bin/perl** — For **Perl**.

Remove a mail forwarder

To delete a **forwarder**:

1. Click *Delete* next to the appropriate forwarded address.
2. Confirm that this **forwarder** should be deleted on the following page.

Add a domain forwarder

This feature will allow all mail sent to a domain to be forwarded to another domain. Adding a domain **forwarder** will override the **default address** for the selected domain.

To add a domain **forwarder**:

1. Click *Add Domain Forwarder*.
2. Enter the domain to which you would like to forward email.
3. Click *Add Domain Forwarder*.

Remove a domain forwarder:

To remove a domain **forwarder**:

- Click the button under the *Delete* heading that corresponds to the domain **forwarder** you would like to remove.

MAIL – Auto Responders

This feature can be configured to automatically send response messages. This can be useful when the recipient is unavailable. To view auto responders for a specific domain on your account, click the **Managing:** menu and choose a domain.

Add an auto responder

To add or edit an **auto responder**:

1. Click *Add Autoresponder* to create a new **auto responder**. Or, find a current **auto responder** and click *Edit*.
 2. Choose a character set.
 3. Specify the interval, in hours, you wish for the autoresponder to wait between responses to the same email address.
 - For example, if you set up an autoresponder with an interval of 24, and you receive an email from john@example.com at 8 am on Monday, the autoresponder will respond to his message immediately. If, however, john@example.com continues to email you throughout the day, the autoresponder will not send him another response for 24 hours after his initial email (in this case, 8 am Tuesday). If he emails you again after the 24-hour interval expires, he will receive an auto response.
 4. Define the email address whose mail you wish the system to respond to.
 5. In the *From* and *Subject* fields, type the username and subject you want to appear in the response.
 6. If the message includes **HTML** tags, click the *HTML Message* checkbox.
 7. In the *Body* field, type the text of the response.
 8. Click *Create/Modify* to store the new **auto responder**.
- **In the message body, you can include tags, enclosed in percent signs (%). You can use these tags to insert information, such as the incoming email's sender or subject, into the body of the email. Available tags are:**
 - **%subject%** — **The subject of the message that was sent to the** auto responder.
 - **%from%** — The name of the sender of the message received by the **auto responder**, if available. (If the sender's name was not received, %from% will print the sender's email address.)
 - **%email%** — The sender's email address.

Delete an auto responder

To delete an [auto responder](#):

1. Click *Delete* next to the appropriate [auto responder](#).
2. Click *Yes* to confirm that the responder should be deleted.
 - If you wish to keep the [auto responder](#), click *No*.

MAIL- Mailing Lists

This feature simplifies sending mass mail, allowing you to type a single address to send mail to multiple email addresses. It is important to note that the mailing lists are handled by an application called Mailman. For more information regarding Mailman, please visit <http://www.list.org/>.



Mailman lists are made public by default. To protect any information sent through a list, it is recommended that the list be made private through the Mailman interface.

Add a mailing list

cPanel comes complete with an interface for defining a name, password, and domain name for the **mailing list** you are creating.

To add a new **mailing list**:

1. Enter the list name in the appropriate field.
2. Key-in and confirm a secure password.
3. Select a domain from the pull-down menu.
4. Click *Add Mailing List* to create the new **mailing list**.

Once a **mailing list** has been created using cPanel, it can be modified, deleted, or the password can be changed using the functions below the Current Lists heading.

Modify a mailing list

To quickly find the **mailing list** you wish to modify, type a keyword into the *Search* box and click *Go*. cPanel displays the lists whose names contain the keyword.

To modify an existing **mailing list**, you will need to enter the administrator password. If you have lost or forgotten your administrator password, the password can be changed, without the original password, using the *Change Password* feature.

Once you have entered the Mailman modification menu, you are free to define the various configuration options in Mailman. Consult the Mailman documentation for more information regarding these configuration options: <http://www.list.org/docs.html>.

Change mailing list password

Using the cPanel interface, it is possible to change the password for a **mailing list** without the old password. This can be very useful in recovering control of your **mailing list** in the event the password is forgotten or lost.

A secure password is one that contains no dictionary words and is comprised of upper- and lower-case letters, numbers, and symbols.

To change a mailing list password:

1. Key-in and confirm the new password.
2. Click *Change* to activate the new password.

Delete a mailing list

To delete a mailing list:

1. Click the *Delete* link next to the appropriate name in the list.
2. Confirm that the list should be deleted on the following page.

MAIL – User level filtering

cPanel lets you [filter](#) email sent to a specific user's address. This can be useful for discarding [spam](#), redirecting mail, or piping messages to a program.

Add a User level Filter

It is important to give the [filter](#) an appropriate name, as it will make the task of managing existing filters easier in the future.

Filter Name: Rule 1

The Filter name must be unique. If you give the filter the same name as another filter, it will be overwritten.

Rules

From equals

Actions

Discard Message

Activate

To create a new [filter](#):

1. Click *Create a new Filter*.
2. Type a name for the [filter](#) in the *Filter Name* box.
3. Select a message characteristic from the first pull-down menu.
4. Select an operator from the next pull-down menu.
5. Enter the characters or words you wish to use as a [filter](#).
6. You can add and subtract rules by clicking the + and - buttons.
7. Select an action from the pull-down menu under the Actions heading. You can add and subtract actions by clicking the + and - buttons.
8. Click *Activate* to initialize the [filter](#).

For a comprehensive list of options available to configure your [filter](#), click [here](#).

★ **A word about operators:** When you create a [filter](#) using several operators, it may be useful to note that cPanel will always process the "and" operator *before* the "or" operator. As a result, email filters will be processed as follows:

- **A or B and C** will be processed as **A or (B and C)**.
- **A and B or C** will be processed as **(A and B) or C**.

If you wish to create a **filter** such as **(A or B) and (C or D)**, you would have to create it like so:

- **(A and C) or (A and D) or (B and C) or (B and D)**.

Test a custom filter

Once a **filter** has been created, it can be tested. To test your **filter**:

1. Type a test email message in the text box below the *Filter Test* heading.
 - Be sure to include the characters or words that you have set your **filter** to catch.
2. Click *Test Filter*. When the test is run, the next screen should display a similar result to the screenshot below.

```
Filter Trace

Filter Trace Results:

Return-path copied from sender
Sender      = example@server1
Recipient   = example@server1
Testing Exim filter file "/home/example/etc/example.com/

Filtering did not set up a significant delivery.
Normal delivery will occur.
```

Filter Test Results.

3. Filter test results
4. This screen summarizes the actions taken by the **filter**. It is important to read over the data to ensure that the **filter** produces the desired result.

Remove an existing filter

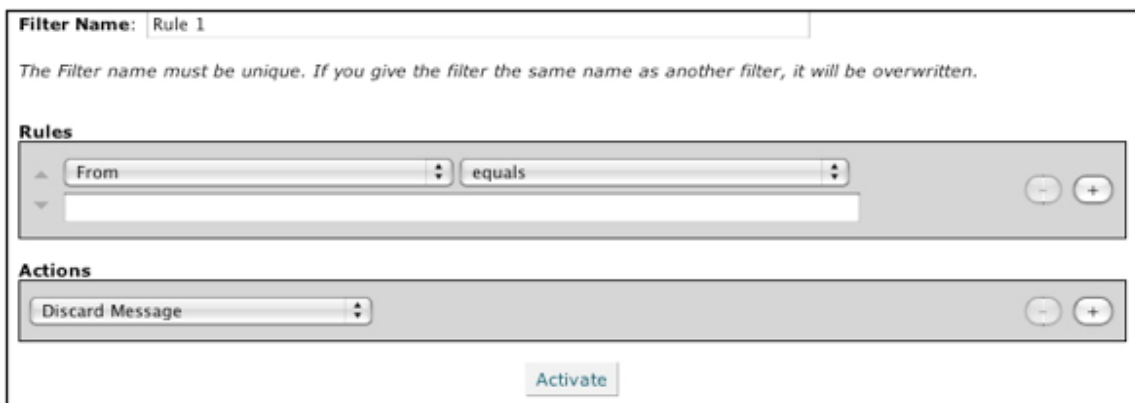
- To delete a **filter**:
- Click *Delete*.
- Confirm that the **filter** should be deleted on the following page.

MAIL- Account level filtering

Add an account level filter

It is important to give the [filter](#) an appropriate name, as it will make the task of managing existing filters easier in the future.

It is important to give the [filter](#) an appropriate name, as it will make the task of managing existing filters easier in the future.



Filter Name: Rule 1

The Filter name must be unique. If you give the filter the same name as another filter, it will be overwritten.

Rules

From equals

Actions

Discard Message

Activate

The *Edit Filter for All Mail on Your Account* screen.

To create a new [filter](#):

1. Click *Create a new Filter*.
2. Type a name for the [filter](#) in the *Filter Name* box.
3. Select a message characteristic from the first pull-down menu.
4. Select an operator from the next pull-down menu.
5. Enter the characters or words you wish to use as a [filter](#).
6. You can add and subtract rules by clicking the + and - buttons.
7. Select an action from the pull-down menu under the *Actions* heading. You can add and subtract actions by clicking the + and - buttons.
8. Click *Activate* to initialize the [filter](#).

For a comprehensive list of options available to configure your [filter](#), click [here](#).

MAIL- Account level filtering *continued*

★ **A word about operators:** When you create a [filter](#) using several operators, it may be useful to note that cPanel will always process the "and" operator *before* the "or" operator. As a result, email filters will be processed as follows:

- **A or B and C** will be processed as **A or (B and C)**.
- **A and B or C** will be processed as **(A and B) or C**.

If you wish to create a [filter](#) such as **(A or B) and (C or D)**, you would have to create it like so:

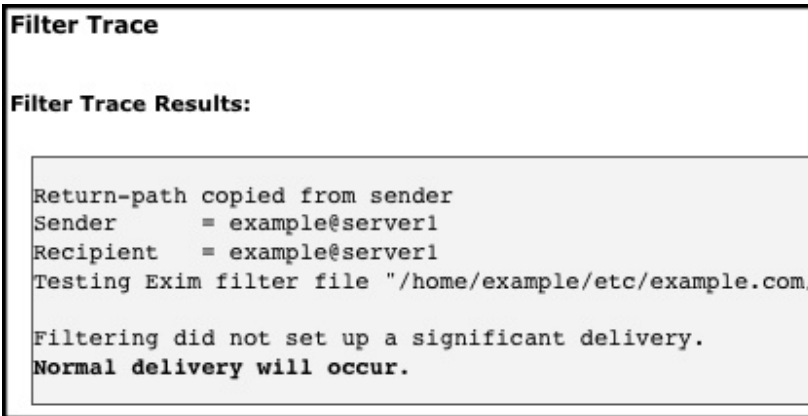
- **(A and C) or (A and D) or (B and C) or (B and D)**.

Test a filter

Once a [filter](#) has been created, it can be tested.

To test your [filter](#):

1. Type a test email message in the text box below the *Filter Test* heading.
 - Be sure to include the characters or words that you have set up your [filter](#) to catch.
2. Click *Test Filter*.
3. When the test is run, the next screen should display a similar result to the screenshot below.

4. 

```
Filter Trace
Filter Trace Results:
Return-path copied from sender
Sender      = example@server1
Recipient   = example@server1
Testing Exim filter file "/home/example/etc/example.com/
Filtering did not set up a significant delivery.
Normal delivery will occur.
```

MAIL- Account level filtering *continued*

Edit a custom filter

You can also modify an existing [filter](#).

To edit an existing [filter](#):

1. Click *Edit* next to the appropriate [filter](#) name.
2. You can adjust any of the fields displayed — the message characteristic, operator, term to [filter](#), or resulting action.
3. Click *Activate* to initialize the [filter](#).

Delete an existing filter

To delete a [filter](#):

1. Click *Delete*.
2. Confirm that the [filter](#) should be deleted on the following page.

MAIL- Email Delivery route

This feature shows the specific path that will be taken by an outgoing message, which can be useful for locating problems with email delivery.

Test a delivery route

To see your mail delivery route:

1. Key-in the desired email address.
2. Click *Show Route*.

The resulting screen will show the delivery route from web **server** to **server**. Under the *Legend* heading appear four icons with their corresponding meanings. The icons will show you what error, **filter**, destination or local mailbox was encountered while your email was en route.

MAIL - Import Addresses/Forwarders

This feature allows you to use 2 types of files to create multiple email addresses or forwarders for your account simultaneously. You may use Excel spreadsheet files (.xls) or comma-separated values sheet, aka CSV, files (.csv), to import the data. (A CSV file is a plain text file that has been given a .csv extension.)

To create this file, you will need to add a series of email addresses and passwords to your spreadsheet or CSV file.

When using a CSV file, you will need to separate your email addresses and passwords consistently, using commas (,), periods (.), or any character of your choosing. These separators are known as delimiters and separate the pieces of information that will be imported for each account.


You should separate each account or forwarder you would like to create using a new row in the spreadsheet or a new line in a CSV file.

You may import the following information:

- Email address usernames (Example: `user1` — you can, but are not required to, include `@example.com`).
- Passwords for email addresses.
- Email quotas (Example: `10` stands for 10 Megabytes).

A sample CSV file might contain:

```
user1@example.com, Password, 10
user2@example.com, Password, 10
user3@example.com, Password, 10
```

 **Note:** You do not have to use a comma (,) as your delimiter.

Adding email addresses using a spreadsheet or CSV file

1. In *Step 1*, select whether you would like to import email accounts or forwarders.
2. In *Step 2*, click *Choose File* to select the file you wish to upload.
3. In *Step 3*, select the delimiter you have chosen to use in your file.
 - If you have used a delimiter that is not contained in the list, select the *Other* option and define the delimiter in the text box on the right.
4. Click *Treat first row as column headers* if you have placed column headers in the first row of the file.
5. Click *Next*.
6. Use the pull-down menus on the following page to assign the properties of each delimited value.
 - For example, if you chose to use a comma and input the line `account, password, domain`, assign `account` to **Email**, `password` to **Password**, and `domain` to **Domain** using the pull-down menus above each value.
 - You can select **Ignore** for a column that contains unnecessary data.
7. From the pull-down menu, choose the domain you would like to use for these accounts.
8. Click *Next*.
9. Review the information and click *Finish*.

You can click *Import More* to return to the first screen and import additional addresses.

MAIL – Email authentication

To combat **spam**, or unwanted email, cPanel's email authentication features attempt to provide information so that recipients know the nature of incoming messages. This enables you to discard unnecessary messages.

Set up domain keys

This authentication function works to verify the origins of incoming mail, ensuring that the mail was sent by the address from which it claims to have originated. This tool is useful against spammers that "spoof," or falsely send from, one or more of your domain's email addresses.


- To use DomainKeys, click Enable.
- To disable DomainKeys, click Disable.

Set up spf

This function attempts to prevent spammers from sending email while forging your domain's name as the sender (**spoofing**). This authentication function works by adding IP addresses to a list, specifying computers that are authorized to send mail from your domain name. It verifies that messages sent from your domain are coming from the listed sender, reducing the amount of **backscatter** you receive.

To use **SPF**, click *Enable*.

To disable **SPF**, click *Disable*.

 **Note:** Both the DomainKeys and **SPF** authentication functions require the **server** to be a **DNS server** for the domain name. For more information about **DNS** servers review the terms of your hosting contract.

MAIL – Email authentication *continued*

Advanced settings

The advanced settings section of this screen includes a number of ways to improve the authentication process. The available options are as follows:

- *Add hosts that send mail from the current domain.* The additional hosts will automatically be approved to send mail to the domain. Hosts can be added and removed using the appropriate buttons.
- *Add MX servers to the current domain under the appropriate heading.* All MX entries specified here will be permitted to send mail to the current domain.
- *Add IP addresses that will be approved for sending mail.* The main server IP will automatically be added to the list. Any additional IPs must be added in CIDR format. (Example: `192.168.0.1/32`)
- The *Include List* allows additional hosts to be specified and included in the SPF settings. This is useful when sending mail with another service.
- *All Entry*, when checked, excludes domains not included in the lists defined above.
- *Overwrite Existing Entries* will overwrite existing SPF entries when checked.

Remember: Click the *Update* button at the bottom of the screen to store your changes.

MAIL – MX entry

This feature allows you to route a domain's incoming mail to a specific [server](#). Please note that changing the [MX entry](#) will result in the [DNS](#) records being changed.

This feature can be useful in creating a [backup](#) mail exchanger to handle mail during [server](#) downtimes.

Configure email Routing



Misconfiguring your MX entries can completely disable your ability to receive mail. If you are unsure which option to choose, contact your system administrator.

To determine how mail will be routed for a domain:

1. Select the domain from the pull-down menu.
2. Select an option under *Email Routing*:
 - **Automatically Detect Configuration** — The [server](#) will automatically detect, and use, the configuration set below and detailed under the *MX Records* heading at the bottom of the page.
 - **Local Mail Exchanger** — The domain will accept mail, regardless of whether a higher-priority mail exchanger has been designated. (If a higher-priority mail exchanger exists, mail will be routed to both [domains](#).)
 - **Backup Mail Exchanger** — The domain will act as a [backup](#) mail exchanger, holding mail in queue if the primary exchanger becomes unavailable.



You will need to configure the primary [MX entry](#) to point to the appropriate exchanger.

- **Remote Mail Exchanger** — The domain will not accept mail, instead sending it to the primary mail exchanger.




You will need to configure the primary [MX entry](#) to point to the appropriate exchanger.

3. Click *Change*.

MAIL – MX entry *continued*

Add a new MX entry

1. Select a domain from the pull-down menu.
2. Under *Add New Record*, set the priority for the new [MX entry](#), keeping in mind that 0 is the highest priority. Here are some key points to consider when assigning priority to MX entries:
 - Lower values denote higher priority, with 0 being the highest possible priority.
 - The primary mail [server\(s\)](#) (with the lowest-numbered priority) will receive mail sent to your domain.
 - Backup, or secondary, mail servers (those with higher priority values) can be used for [backup](#) or other purposes.
 - If you assign multiple mail servers the same priority, when that level of mail [server](#) is needed, mail will be distributed to those servers randomly.
3. In the *Domain* text box, type the hostname of the new mail exchanger.
4.  **Important:** This must be a fully qualified domain name ([FQDN](#)). You **cannot** specify an [IP address](#) here.
5. Click *Add Domain* to store the changes

Delete an MX entry

1. To delete an MX entry:
2. Click Delete next to the appropriate MX entry, in the Current MX Entries list.
3. Confirm that the entry has been deleted by clicking Delete again.

Edit an MX entry

1. Click Edit next to the appropriate MX entry.
2. Change the Priority or Destination as needed.
3. Click Edit to save the changes.
4. Confirm that the entry is correct by clicking Edit again.

FILES

Backup

After you click on the Backup icon, you will see options for generating and downloading a Backup of your whole site and/or for downloading the most recent System [backup](#) made at daily, weekly, or monthly intervals.

Full Backup

A full backup includes all of the files in your home directory, your MySQL Databases, and your email forwarders and filters. You can backup your account to preserve your data or use a backup file to move your account to another cPanel server.

[Download or Generate a Full Web Site Backup](#)

System Backups

Select a system backup to download:

[weekly](#)

[daily](#)

[monthly](#)

Download Options for System Backups

Create a full backup

To save a copy of your website to the web [server](#):

1. Click the *Download or Generate a Full Web Site Backup* button.
2. Select *Home Directory* from the *Backup Destination* heading.
3. Enter your email address.
4. Click the *Generate Backup* button. You will receive an email once the [backup](#) is complete.
 - o The date the [backup](#) was created appears in the filename (which begins with [backup](#)-MM-DD-YYYY). The file will be stored as a “tar ball,” or compressed data file, with the file extension [.tar.gz](#).

FILES – Backup continued

Download a full backup

To download a full [backup](#) to your computer:

1. Click the Download or Generate a Full Web Site Backup button.
2. Under Backups Available for Download, select the [backup](#) file you'd like to save to your computer.
 - o It will be saved as a “tar ball,” or compressed data file with the filename extension [.tar.gz](#). The date the [backup](#) was created appears in the filename (which begins with [backup-MM-DD-YYYY](#)).

Store a Backup file Remotely

The Full Backup screen can also utilize [FTP/SCP](#) to log into a remote computer and store the [backup](#) files there. This feature is intended for more advanced users.

When you fill out the required information, the [backup](#) file can be stored in a specified directory on a remote machine. Once the process has completed, an email will be sent to the email address you specified.



You cannot use a full [backup](#) to restore your site via the cPanel interface. The file must be downloaded and decompressed prior to restoration. Once the file has been decompressed, you will be able to upload and restore the individual pieces of your website contained within the full [backup](#).



If something you do affects your site, please [contact us](#) so that we can put it right for you.

Partial Backup

The *Backups* link also allows you to store individual pieces of your site. It is possible to download and store the entire **/home** directory, the SQL database(s), as well as email forwarders and filters by clicking the appropriate links under the *Partial Backups* headings. This method will download the [backup](#) file(s) to your computer, saving them to a specified directory.

FILES

Backup Wizard

The *Backup Wizard* is a user-friendly interface for creating a [backup](#) of the entire site, a partial [backup](#), or allowing a site restoration from the last [backup](#) saved. This tool may be useful to new users.

Using the Backup Wizard, you can back up and save your entire website or a portion of your website. You can also use the *Restore* link to select files to restore portions of your site. To begin, first select whether you would like to back up or restore your website.

Backup your entire site

To create a full [backup](#):

1. Select *Backup* from the first page.
2. Select *Full Backup* from the second page.
3. Select the destination for the [backup](#) files. You have 3 options:
 - You can store the files in your home directory on your web [server](#) by selecting *Home Directory* from the pull-down menu.
 - cPanel can also utilize [FTP](#) or [SCP](#) to store the files to a remote machine. To do this, fill in the appropriate information and select the method for file transfer from the pull-down menu.
 - If you wish to download the file to your computer, skip to the next step.
4. Click *Generate Backup*.
 - If [FTP](#) or [SCP](#) was used, an email will be sent to the email address that you specified at the beginning of the process.
5. To download a copy of the [backup](#) file to your computer, click the filename under *Backups Available for Download*.

The date the [backup](#) was created appears in the filename (which begins with [backup](#)-MM-DD-YYYY). The file will be stored as a “tar ball,” or compressed data file, with the filename extension [.tar.gz](#).

You cannot use a full **backup** to restore your site via the cPanel interface. The file must be downloaded and decompressed prior to restoration. Once the file has been decompressed, you will be able to upload and restore individual pieces of your website contained within the full **backup**.

FILES - Backup Wizard *continued*

To back up a portion of your site:

1. Select *Backup* from the first page.
2. Select the portion of your site to back up by clicking *Home Directory*, *MySQL Databases*, or *Email Forwarders & Filters*.
3. Click the appropriate link or button on the following page to store the required information to your computer or web [server](#).



The type of the [backup](#) file will depend on what portion of your site you are saving to your computer. For a list of backups and their corresponding file types, see Table A.

<u>Part of Site</u>	<u>File Type</u>
Home Directory	*.tar.gz
Email Forwarders	*.net, *.com
Email Filters	*.net, *.com
SQL Database	*.sql

Table A

<u>Part of Site</u>	<u>File Type</u>
Home Directory	*.tar.gz
Email Forwarders	*.net, *.com
Email Filters	*.net, *.com
SQL Database	*.sql

Table B

Restore a portion of your site

To restore a portion of your site:

1. Select *Restore* from the first page.
2. Select the portion of your site you would like to restore by clicking *Home Directory*, *MySQL Databases*, or *Email Forwarders & Filters*.
3. Select the file from your computer that should be used to restore the portion of your website that you have selected.
4. Click *Upload* to finish the restoration process.



The type of the [backup](#) file will depend on what portion of your site you are restoring. For a list of backups and their corresponding file types, see Table B above.

FILES –

File Manager

The File Manager is cPanel's built-in web application for managing and manipulating your website's files from your personal computer. Most users will feel comfortable using this file management tool.

cPanel provides a number of ways files can be manipulated within the File Manager. Its main interface, the File Manager toolbar, can be seen in the screenshot below.



- The *New File* button creates a new file with a user-defined file extension.
- The *New Folder* button creates a new folder in which files can be stored.
- The *Copy* function copies selected items to a directory you specify.
- The *Move File* button allows selected files to be moved to a new directory.
- The *Upload* button allows new files to be uploaded to a specified directory.
- The *Download* button downloads selected files to your computer.
- The *Delete* button deletes selected files from the [server](#).
- The *Rename* button allows a selected file to be renamed.
- The *Edit* file opens an editor for the selected text or [HTML](#) files.
- The *Code Editor* button opens a code editor for the selected [HTML](#) or [PHP](#) files.
- The *HTML Editor* button opens an editor specifically intended for [HTML](#) files.
- The *Change Permissions* button allows the read/write permissions to be changed for selected files.
- The *View* button will open the selected files for viewing.
- The *Extract* button will decompress and extract a compressed file to a specified directory.
- The *Compress* button will compress selected files to a single [*.zip](#), [*.Gz](#), [*.Bz2](#), or [*.tar](#) archive and store the zipped file to a specified directory.



Certain functions of the File Manager are designed for use with 1 file at a time. Any attempt to rename, edit, or view multiple files at once will open only one file — the file listed first in the directory

FILES

Legacy File Manager

The Legacy File Manager offers file manipulation options in an older web-based interface. Users already familiar with an older version of cPanel's File Manager may find the Legacy File Manager more comfortable.

When an existing file is clicked from the list, a menu in the upper right-hand corner of the window appears, showing the options for file manipulation. (The options are specific to the type of file selected; as a result, not all options will appear for all files.)



The Legacy File Manager

- The *Copy* function copies selected items to a directory you specify.
- The *Show File Contents* link displays the file's contents for viewing only.
- The *Move File* link allows selected files to be moved to a new directory.
- The *Download* link downloads selected files to your computer.
- The *Delete* link places selected files from the [server](#) into the trash. From there, you can restore or permanently delete the files.
- The *Rename* link allows a selected file to be renamed.
- The *Edit* link opens an editor for the selected files.
- The *Code Editor* link opens a code editor for the selected files.
- The *HTML Editor* link opens an editor specifically intended for [HTML](#) files.
- The *Change Permissions* link allows the read/write permissions to be changed for selected files.
- The *URL* link displays the selected file as it would be seen on the Web.

FILES

Web Disk

cPanel offers a Web Disk application where files can be managed and manipulated using your operating system's interface. Newer users may be most comfortable with this file management method.

The Web Disk uses your computer's operating system for file manipulation. Accessing the [web disk](#) will open a window on your computer, allowing new files to be moved, deleted, or added to the [server](#), just as you would manage files on your personal computer, as shown in the screenshot below.

To configure the Web Disk:

1. Enter a username in the *Login* field.
2. Enter your desired password into the *Password* field.
3. For help generating a strong password, click *Generate Password*.
4. Confirm the password in the *Password (Again)* field.
5. Specify the directory that you want the [web disk](#) to connect to on startup.
6. Click *Create*.

Your new account should appear in the *Web Disk Account Management* table.

When the Web Disk configuration is completed successfully, a new window containing your website's content will be opened on your computer. From this window, your website's files can be managed just like you would manage files on your personal computer.

Once you have added a Web Disk account to you [server](#), it can be accessed quickly in the future by clicking the Access Web Disk button at the main Web Disk Accounts page. You are also able to change the password, delete, or password protect directories for existing [web disk](#) accounts under the Actions heading in the Web Disk Accounts Management

Note for Windows® Vista Users

If you are running Windows Vista on your desktop, you will need to download a patch from Microsoft's website in order to use Web Disk. You can find the patch [here](#).

FILES - Web Disk *continued*

Access a Web Disk Account

To log into a Web Disk account:

1. Click the Access Web Disk button corresponding to the Web Disk account to which you would like to access.
2. Choose your operating system (OS), Windows®, Mac®, or Linux.
 - ★ **Remember:** Choose the version or distribution of your operating system using the pull-down menu.
3. Click Go under the appropriate operating system to download the script file.
4. Open and run the script file, accepting any certificates

To change a Web Disk's password:

1. Click the *Change Password* link corresponding to the account whose password you would like to change.
2. Enter the new password into the *New Password* field.
3. Click *Change*.

Delete a Web Disk account:

To delete a Web Disk account:


1. Click the *Delete* link corresponding to the account you wish to delete.
2. Confirm that the account should be deleted on the following page by clicking *Yes*.
 - If you would like to keep the account, click *No*.

FILES - Web Disk *continued*

Password Protect a Web Disk Directory

Important: If you choose to protect a [web disk](#) directory you must create a user to access that directory.

To password protect a Web Disk directory:

1. Click the *Password Protect* link corresponding to the Web Disk account you would like to protect.
 - o  **Note:** This feature will affect the directory that the Web Disk account is configured to access.
2. Ensure that the *Password protect this directory* checkbox is checked.
3. Enter a name for the protected directory into the *Name* the protected directory field.
4. Click *Save*.

Create a User to Access a Protected Web Disk Directory

To create a user that will be able to access the protected directory:

1. Enter a desired username into the *Username* field.
2. Enter the desired password into the *Password* field.
3. You may use the *Generate Password* button to generate a secure password.
4. Confirm the password in the *Password (Again)* field.
5. Click *Add/modify authorized user*.

This will allow users to access the protected directory using the username and password you have selected.

Remove an Authorized User

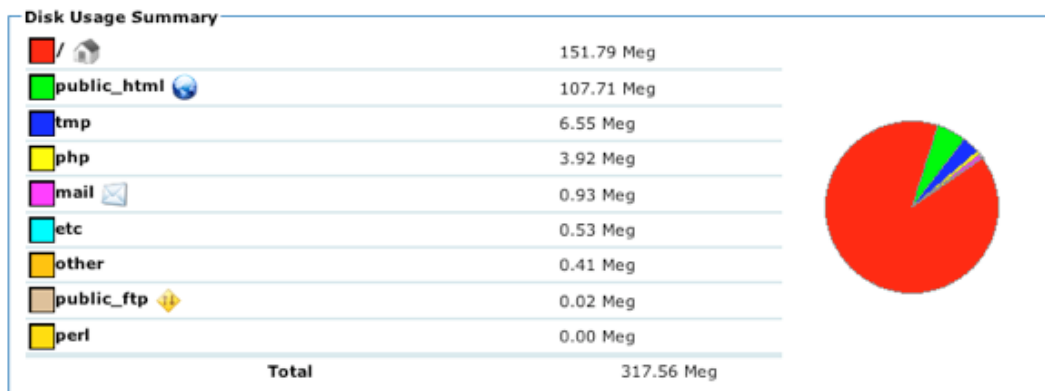
To delete an existing user:

1. Select the username you would like to delete from the text field under the *Authorized Users* heading.
2. Click *Delete User*.

FILES

Disk Space Usage

This function shows you information about the available free space for your website. At the top of the main screen is a graph displaying the basic disk usage information by directory in Megabytes, seen in the screenshot below. This tells you what directories use the most space on your website's hard drive.



Disk Usage Summary

When you click the *Increase* and *Decrease Depth* buttons, cPanel will display subfolders in the defined magnitude. For example, if the / (root) directory is being displayed and the depth is set to 2, cPanel will display the subfolders of / and the subfolders of /\$dir. If the depth is set to one, only the subfolders of / will be displayed.

To delete files:

1. Select the checkbox for the file(s) you want to delete.
2. Click *Delete Selected*.
3. You are able to select all of the files by clicking the *All* link next to the *Select:* heading.
 - o You can deselect all the files by clicking *None*.
 - o You can also sort the list by size or directory by clicking the corresponding header.
 - o You can narrow the list by clicking on a directory. This will cause its contents to appear.

FILES - Disk Space Usage continued

The Drop-down Menu

The drop-down menu on the right-hand side of the page contains actions that you can select to navigate the directories and subdirectories of your website. These options include:

- *Show/Hide the Parent Directories*
- *Show Top Level*
- *Clear File Usage Cache*
- *Show/Hide Small Files*
- *Show File Size as Bytes/Megabytes*

FTP Accounts

[FTP](#) stands for File Transfer Protocol and is another method of website file management. cPanel comes complete with an [FTP](#) server that is pre-configured and easy to use.

To begin using [FTP](#), you need to create a user account. Once the account is created, you can log into your website with an [FTP](#) client such as [FileZilla](#) .



For help on using Filezilla check out my Support Portal.

When entering your [FTP](#) login information to your [FTP](#) client, remember to enter the username as `username@example.com` where `example.com` is meant for your domain name. Requiring that the login information be entered in this way allows your [server](#) to have multiple [FTP](#) accounts across multiple websites.

FILES – FTP Accounts *continued*

Add an FTP Account

Adding an [FTP](#) account will allow access to the domain's folder on the [server](#)'s hard disk.

To create an [FTP](#) account:

1. Enter a username.
2. In the *Password* box, type the account's password.
 - o Remember that a secure password should be used. A secure password does not contain dictionary words and is comprised of letters, numbers, and symbols.
 - o For help generating a strong password, click the *Generate Password* button.
3. Retype the password in the *Password (Again)* box.
4. Specify a directory you wish to access via [FTP](#).
 - o The *Directory* field defines the default directory and the top level of directory access that will be granted to the new account. In other words, an account with a *Directory* assignment of */ \$dir* will not be allowed to access the */* (root) directory; however, it will be able to access all of its sub-folders.
5. Set the disk space quota. The *Quota* field determines how much disk space will be allocated to the [FTP](#) account.

If you have trouble uploading files via [FTP](#), you may need to adjust the quota to allow more disk space for your account.



You will not be able to exceed the disk space quota allocated by your hosting plan; if you are currently using the maximum disk space allowed by your plan, you may need to upgrade your hosting account or delete old or unused files. **If you need more space** [contact me](#)

Upon creation, the new account should be displayed in the list below. This list contains 4 functions for existing accounts. You can:

- Delete an account.
- Adjust a quota.
- Change a password.
- Configure an [FTP](#) client. To search through several [FTP](#) accounts, enter a keyword in the *Search* box. cPanel will show only the accounts that contain the keyword.

FILES – FTP Accounts continued

Configure an FTP Account

When an [FTP](#) client is configured using cPanel, a script will be downloaded to your computer. When this script is run, the [FTP](#) client will automatically be opened, configured, and connected to your [FTP](#) server. To configure an [FTP](#) account, use the appropriate link under the Account Management heading.



Remember: The [FTP](#) client needs to be installed on your computer **before** you download and run the script file.

To configure an [FTP](#) client:

1. Select the appropriate [FTP](#) client. The options include, FileZilla, Core [FTP](#)[™], and Cyberduck. cPanel only supports these 3 [FTP](#) clients for auto-configuration. Other clients can be used; however, you must configure the client yourself.
2. Click the appropriate [FTP](#) or SFTP configuration link.
 - We recommended that you use SFTP for a secure file transfer.
 - SFTP stands for Secure File Transfer Protocol and uses [SSL](#) encryption for all of its operations.
3. Open and run the configuration script file that has been downloaded to your computer.

The [FTP](#) client should automatically open, configure itself, and connect to your [FTP](#) server. There, you will be free to manage your website's content. If you encounter problems when trying to automatically configure your [FTP](#) client, make sure your client is properly installed on your computer. If problems persist, consult your [FTP](#) client's documentation.



If you experience problems logging into your [FTP](#) account, consult the *Manual Settings* shown on the [FTP](#) Accounts screen to ensure that you are using the correct data to log in.



Remember: If the [FTP](#) client you wish to use is not listed, it cannot be automatically configured. In this scenario, you must configure your [FTP](#) client yourself. Consult your [FTP](#) client's documentation for more information.

FILES – FTP Accounts *continued*

FTP Session Control

This function displays general information about who is logged into your [FTP](#) server. This information includes the account name, [IP address](#), login time, current status, and process ID of the current user.


To disconnect users from an [FTP](#) session:

- Click the *Disconnect* button corresponding to the account you wish to disconnect.
- This should be used when you suspect malicious activity from a user, or if the user is idle.

You can use the *Reload* button to refresh the list of [FTP](#) sessions, to see if any other users have logged onto your [FTP](#) server since you last viewed the list.

LOGS

Latest visitors

This function will show information regarding the last 300 people to visit your website. To begin, click the  button under the *View* heading next to the desired domain name.

The records here will show the visitor's [IP address](#), the [HTTP](#) code the visitor received, the date and time of the visit, the [HTTP](#) version, and the amount of information accessed in bytes. You will also see the referrer (the site from which the visitor was linked, if any), and the agent, or browser.

This information can be useful in monitoring repeat visitors to your website, allowing you to tailor the content to fit your visitors' needs.

LOGS *continued*

Bandwidth

This function shows the monthly [bandwidth](#) usage, traffic for the day the function is accessed, and traffic information for the entire year. The function is intended to allow you to monitor the heaviest traffic times for your site as well as to help you to decide whether you should purchase more [bandwidth](#) for your website.

The information is displayed over 3 sets of graphs and a status bar. The status bar shows the percentage of monthly [bandwidth](#) that has been used. The graph below displays the traffic for today while the next graph shows the [bandwidth](#) usage for the entire year.

The [bandwidth](#) information is divided into six categories:

- [HTTP](#) (web traffic)
- POP (receiving email)
- [IMAP](#) (receiving email)
- [FTP](#) (file transfer)
- SMTP (sending email)
- All



The *All* category, displayed in green, provides the combined total of all the aforementioned categories.

The next area displays pie graphs showing [bandwidth](#) usage by domain on a monthly basis. The pie charts show the proportion of monthly [bandwidth](#) used by each domain.

- When you click the domain name on the left side of the screen, cPanel displays a series of graphs showing the amount of [bandwidth](#) used by each type of traffic: [HTTP](#), POP, [IMAP](#), [FTP](#), and SMTP.



Below these graphs is a chart showing the proportion of [bandwidth](#) used by each type of traffic for each day of the month.

- To see a graphic representation of this data, click the day number on the left side of the chart.


LOGS *continued*



In certain circumstances, you may notice discrepancies between the data in [bandwidth](#) graphs and that displayed in other areas of cPanel. To learn more about this, read our [documentation about how bandwidth graphs are generated](#).

Webalizer

[Webalizer](#) is a complex statistical analysis program capable of producing charts and graphs about who is visiting your website.

To begin, click the  button under the View heading next to the appropriate domain name. Here, the information is displayed in a series of bar graphs relating to a [key](#) below the graphs. The summary is displayed by month and by day over several different categories. These categories are:

- Hits
- Files
- Pages
- Visits
- Sites
- Kilobytes

When you click a month, [Webalizer](#) shows more details, including referrers (sites visitors link from), [HTTP](#) codes, and facts about your visitors, including their usernames, browsers, and countries of origin. For more information about [Webalizer](#), please visit <http://www.webalizer.org>.

Webalizer FTP

Accessing this feature will display stats regarding the use of your [FTP](#) site. The information is displayed in bar graphs relating to a [key](#) below the graph. The data is divided into monthly and daily averages.

To begin using *Webalizer FTP*:

- Select the link corresponding to the domain you wish to view.

For more information about [Webalizer](#), please visit <http://www.webalizer.org>.

LOGS *continued*

Raw Access Logs

Raw access logs are text files that contain information about your visitors and what content on your website they have accessed.

Configure Logs

At the main screen, the checkboxes at the top of the page allow archive logs to be included in the **/home** directory each time the system processes your website's statistics. You can also set up cPanel to remove the previous month's log.



Remember: Click *Save* to store your changes.

Download and View your Raw Access Logs

To download a raw access log, click the desired link under the *Domain* heading. This action will automatically download the log file to your computer. Once the text file is on your computer, you can open it with your preferred text editor.


Under the *Archived Raw Logs* heading are the archived logs contained in your **/home** directory. To download an archived log, click the filename. You can also open the file in your **/home** directory by accessing it in your [CLI](#) and using a text editor.

LOGS *continued*

Analog Stats

[Analog](#) is a program that lets you monitor your website's traffic. The information is compiled into months so that it is easier to manage and interpret. Once a monthly log is accessed, the information is divided into a number of categories and graphs.

View Analog Stats

1. Click the  button under the *View* heading next to the desired domain name.
2. Select the month for which to view the desired stats.

The next page will be an [Analog](#)-generated web page displaying information about the traffic accessing the domain name's content.

For more information regarding the [Analog](#) application, please visit their website at <http://www.analog.cx>.

Error Log

This feature displays the last 300 errors that have occurred on your website. This can be useful for finding and fixing broken links and misconfigured web applications. Checking it often will aid in keeping your website running smoothly.

*******Choose Log Programs is not enabled*******

AWStats

AWStats (Advanced Web Statistics) displays information about who is accessing your website. The information is displayed in graphs and tables, and divided into monthly, daily, and hourly averages. **AWStats** also shows details about your visitors, including referers (sites visitors link from), **HTTP** error codes, and facts about your visitors, including their operating systems, browsers, and countries of origin. To begin using **AWStats**, select the link corresponding to the domain you wish to view from the list on the main **AWStats** page. For more information about **AWStats**, please visit its website at <http://awstats.sourceforge.net/>.

SECURITY

Password protect Directories

Password protecting a directory restricts access to certain parts of your website by requiring visitors to enter a username and a password. This password process is also referred to as a type of “authentication” process.

While using this feature, navigate the directories by clicking the folder icon located next to the name of the directory. Clicking on the name of the directory will select the directory for password protection.



Any subdirectories inside the selected directory will also be password protected.

To password protect your directory:

1. Click the checkbox next to *Password protect this directory*.
2. Using the *Name the Protected Directory* field, assign a name to the password protected directory. (This is the name visitors will see. It can appear as anything, no matter what the directory is called.)
3. Enter the information below the *Create User* heading.
4. Click *Add/modify authorized user*.

The new user’s name will be added to the listbox under the *Authorized Users* heading, where it can be removed later.

Remove a User

To delete password protection for a user:

1. Select the desired account name in the listbox beneath the *Authorized Users* heading.
2. While the name is highlighted, click the *Delete User* button to delete the account.

Remove Password Protection

- To remove password protection from the directory, uncheck *Password protect this directory*.

SECURITY *continued*

IP Deny Manager

This feature is capable of blocking a single **IP address** or a range of IP addresses from accessing your site. Fully qualified domain names (FQDNs) can also be banned. See the [glossary](#) for more information about **FQDNs**.

Deny/ban an IP Address

1. Key-in the necessary IP to the *IP Address or Domain* field.
2. Click the *Add* button.

IP addresses can be added in 5 different ways:

- Single IP Address (Example: 10.5.3.333)
- Range (Example: 10.5.3.3-10.5.3.40)
- Implied Range (Example: 10.5.3.3-40)
- **CIDR** Format (Example: 10.5.3.3/32)
- Implied (Example: 10.)



Entering “10.” as an implied **IP address** implies 10.*.*, where * represents a positive whole number in an **IP address**. Therefore, entering “10.” will block all IP addresses that begin with 10. Please exercise discretion when implying IP addresses.

Unban an IP Address

To remove a denied **IP address**:

1. Click the *Remove* button in the list next to the appropriate **IP address**.
2. From the next screen, confirm the **IP address**'s deny-removal by clicking Yes.

SECURITY *continued*

SSL/TLS Manager

The [SSL](#) and TLS features are intended to make your website more secure. These features generate and manage [SSL](#) certificates, signing requests, and keys. This is useful for websites that will use logins and credit card numbers, since information will be sent to and from your website over the Internet as encrypted data versus plain text. This makes it difficult for malicious users to intercept communications between visitors and your website.

To begin, select a link underneath 1 of the 3 headings:

- Private Keys (KEY)
- Certificate Signing Requests (CSR)
- Certificates (CRT)

These links provide access points that generate, view, or delete keys, requests, and certificates.



Adding a private **key** is the first step in setting up an **SSL** certificate for your site. It is highly recommended that **SSL** certificates be used if your visitors will be submitting sensitive information to your website.

Add a Private Key

A new **key** can be added manually or uploaded using a *.key file.

Upload an Existing Key

To upload a [key](#), begin under the *Upload a New Key* heading:

1. Enter your domain name in the *Domain the Key is for* field.
2. Paste a [key](#) below or click the *Choose File* button to upload a *.key file.



Click the *Install* button to properly install the private [key](#) to the [server](#).

SECURITY – SSL/TLS *continued*

Generate a New Key

If an entirely new [key](#) is needed:

1. Select the desired domain name from the pull-down menu, or type it into the *Host* field.
2. Click the *Generate* button to generate the new [key](#).

The [key](#) will automatically be installed on the [server](#) and will appear in the list under the *Keys on Server* heading once it has been generated.

Add a Certificate Signing Request (CSR)

The signing request form is required for obtaining a certificate from an [SSL](#) provider. The [SSL](#) provider may require information in a specific way. If this is true for your [SSL](#) provider, take the steps to make sure the information is presented in the required way.

To generate a [CSR](#):

1. Select the host from the *Host* pull-down menu.
2. Fill in the rest of the appropriate information in the fields below the menu.
3. Click the *Generate* button.



You must have a [key](#) prior to generating a signing request.

Add a Certificate

When installing a trusted certificate obtained through an [SSL](#) provider, use the features beneath the *Upload a New Certificate* heading.

Upload an Existing Certificate

To upload the certificate:

1. Paste the certificate into the text box, or upload a **.crt* file using the *Choose File* button.
2. Click the *Upload* button to install the certificate onto the [server](#).

SECURITY – SSL/TLS *continued*

Generate a New Certificate

If the **SSL** certificate is self-signed, it can be generated under *Generate a New Certificate*:

1. Select the host from the pull-down menu.
2. Key-in the remaining information.
3. Click *Generate*.

When the certificate is generated and self-signed, it will automatically be installed on the **server**.



Self-signed certificates are generally reserved for intranet uses. To use a certificate on the Internet, you should use a third-party service. Consult your favorite search engine to shop for **SSL** providers or **contact me**.

SSH/Shell Access

SSH (secure **shell**) and Telnet are examples of network protocols that make remote **server** management possible by allowing you to control another computer (ie, your web **server**) over the Internet through a command line interface (**CLI**). This can be used, for instance, when configuring **CGI** scripts. **SSH** is included with many modern operating systems including Mac® OS X and Linux distributions.

If you are using Microsoft Windows to connect to your **server**, you will need an **SSH** client to log into the **server**. One can be obtained at <http://www.chiark.greenend.org.uk/~sgtatham/putty/>.

For Unix-based operating systems, such as Mac OS or Linux, many commands have been standardized. For a list of standardized Unix-based (**POSIX**) commands, consult your favorite search engine or visit http://www.one-serve.com/tools/unix_commands.php.

SECURITY – SSH/Shell Access *continued*

Connecting with Putty

To use PuTTY to connect to your [server](#) via [SSH](#):

1. Download and install the client from the [URL](#) above.
2. Open the client.
3. Under the Sessions menu, input the [IP address](#) of the [server](#).
 - o Make sure that the [SSH](#) button is selected.
4. Click *Open*.
5. Use **root** as the login name.
6. Enter the root password.

If the username and password were correctly entered, you should be logged into the [server](#).

Connecting with Mac OS X or Linux

To connect via [SSH](#) to your [server](#):

1. Open a terminal session.
2. Issue the following command:
 - o `ssh -p $port $user@$IP`
 - Where **\$port** is meant to stand for the port number.
 - **\$user** is meant to stand for your username.
 - **\$IP** is meant to stand for your **IP address**.


Manage SSH Keys

Using cPanel, it is possible to manage, import, create, and remove [SSH](#) keys. These keys will be used when confirming a specific computer has the right to access your website's information using [SSH](#). Use the Generate a new Key and Import Key links to generate or import a **key**, respectively.

SECURITY – SSH/Shell Access *continued*

Generate a New Key

To generate a new **key**:

1. Click *Manage SSH Keys*.
2. Click the *Generate a new key* icon.
3. Fill in the appropriate information.
4.  **Note:** It is important to consider your needs when choosing a **key** type, bearing in mind that **RSA** keys yield a faster confirmation of identity, while using **DSA** keys will speed up **key** generation and signing times.
5. Select a **key** size using the pull-down menu.
6. Click *Generate Key* to generate the new **SSH key** and automatically install it to the **server**.

Import an Existing Key

To import a **key**:

1. Click the *Import Key* icon.
2. Choose a name for the **key**.
3. Paste the private and public keys into the 2 text boxes.
4. Click *Import*.

Once a **key** has been installed onto the **server**, it can be edited, deleted or downloaded using the appropriate links in the lists on the *Manage SSH Keys* page. Keys that are new to the **server** need to be authorized using the *Manage Authorization* link.



The **key** will not work until it is authorized.

The **key**, once authorized, can be unauthorized by using the *Manage Authorization* link and clicking *Deauthorize*.

SECURITY – SSH/Shell Access *continued*

Connect Using Java SSH

cPanel comes equipped with an application called SSHTerm, which lets you connect to your website using [SSH](#) through cPanel. SSHTerm is a [Java](#) application that opens a command line interface ([CLI](#)) in an application window within the browser.

After clicking the *Connect Using SSHTerm* button, you may need to accept a certificate. Once the certificate has been accepted, the application will load after a few moments.

By specifying the web [server's IP address](#), a connection can be made. It is possible to enter a user name and password or use public keys to confirm (authenticate) your identity and log into your [server](#).

Connect using Java Telnet Applet

cPanel contains a Java application called Java Telnet Applet which lets you connect to the web server using a Telnet connection through cPanel. This application can be accessed by clicking the appropriate button at the SSH/Shell Access main screen.

A pop-up window will open that contains the Telnet Java application. Another pop-up, requesting login information, will also be opened. Enter your username and password.

Upon successfully logging in, a connection will be made, allowing the manipulation of your web server through the CLI. Please note that keys cannot be used as an authentication method; a username and password are required.



There are a number of specific Telnet commands with which you may need to familiarize yourself. Please consult your favorite search engine for more information regarding Telnet and your operating system's commands. It is also recommended that SSH be used in place of Telnet when possible, as an SSH connection is inherently more secure.

SECURITY *continued*

Hotlink Protection

A [hotlink](#) occurs when content from your site is embedded on another site, using your [bandwidth](#) to serve the files. cPanel allows you to prevent hotlinks to your site.

When disabling hotlinks, be sure to allow hotlinking for any necessary [domains](#), such as your website's subdomains.


Enable Hotlink Protection

To disable hotlinking:

1. Click the *Enable* button on the *HotLink Protection* main page.
2. To allow sites to **hotlink** to your site, add the **URL** to the URLs to allow access list.
 - Direct access to certain file extensions can be blocked by adding them to the text field under the Block direct access for these extensions heading.
 - When these file types are blocked, people will not be able to **hotlink** those types of files from your website, even if hotlinking is allowed.
3. Click the checkbox to allow users to access the content by entering the specific file's **URL** into a browser.
4. Requests for content can be redirected by entering a **URL** under the *Redirect request to this URL* heading.
5. Click *Submit*.

Disable Hotlink Protection

- To disable **hotlink** protection, click the Disable button on the main *HotLink Protection* page.

 **Note:** Clicking Disable may delete any entries you have added to the list of URLs to allow access. If you are disabling access only temporarily, you may want to save the list so that you can re-enter it later.

SECURITY *continued*

Leech Protect

Leeching occurs when users publicly post their username and password to a restricted area of your site, allowing other visitors to use the login information. cPanel can be configured to handle leeching, redirecting and potentially suspending the user. The protection function works by setting the maximum number of logins that can occur within a 2-hour time limit. If the login limit is exceeded, the user is presumed to be allowing other visitors to use his or her login information.

Enable Leech Protect:

To protect your website from leeching:

1. Click the name of the directory you want to protect.
 - To navigate directories, use the folder icon located next to the name of the directory.
2. Enter the maximum number of logins you want to allow each user within a 2-hour period.
 - To **redirect** users exceeding the maximum number of logins, enter a **URL to redirect** them to.
 - If an email alert should be sent to your email address, click the *Send Email Alert* to checkbox and enter the email address.
3. To disable an account that exceeds the maximum number of logins in 2 hours, click the *Disable Compromised Accounts* checkbox.
4. Click *Enable*.

This page also provides a *Manage Users* button. Clicking this button takes you to the **Password Protect Directories** screen, where users can be added, edited, and deleted.

SECURITY *continued*

Add a GnuPG Key

GnuPG keys use the “public **key** approach” to encryption. Messages are sent once they have been encrypted by a public **key**. The messages can only be decrypted by a private **key**, held by the intended recipient.

Add a Key

To add a **GnuPG key**:

1. Fill in the fields below the *Create a New Key* heading.
2. Click *Generate Key*.

Make sure to use an appropriate expiration date. The expiration date is defined in years and describes when the **key** will no longer work; 1 year is the default.



Use a secure password. A secure password is one that is not a dictionary word and contains upper- and lower-case letters, numbers, and symbols.

Import a GnuPG Key

An existing **key** can be imported using the *Import Key* button.

To import a **GnuPG key**:

1. Copy and paste the **key** into the available text box.
2. Click *Import*.

The **key** will automatically be installed onto your web **server**.

Delete or View a GnuPG Key

Once a **key**-set has been added to the **server**, it can be deleted or viewed for copy from the main *GnuPG* page under the *Public Keys and Private Keys* heading.

DOMAINS

Subdomains

A **subdomain** is a subsection of your website that exists as a subdirectory in your **public_html** folder. Subdomains use a prefix in conjunction with the domain name. For example, if the registered domain name was example.com, the **subdomain** will be prefix.example.com.

It is important to remember that it takes time for the **subdomain** to become recognized by other computers on the web. Visitors will not be able to view your **subdomain** immediately; the process takes anywhere from 2 days to a week.

Subdomains can be useful for creating unique user accounts for “vanity **domains**.” This is helpful if, for example, you have a blog, or any other type of website that uses a domain specifically titled for a user.

Add a Subdomain

To create a **subdomain**:

1. Enter the desired prefix in the *Subdomain* field.
2. Select the desired main domain from the pull-down menu.
3. Enter the home directory for the **subdomain** into the *Document Root* field.
 - This directory will be where files pertaining to the **subdomain** will be placed.
4. Click *Create*.

To open the **subdomain**'s main directory with the File Manager:

- Click the link under *Document Root* that corresponds to the **subdomain** you would like to view in the *File Manager*.

DOMAINS - Subdomains *continued*

Enable or disable subdomain redirection:

To enable or disable redirection of a **subdomain**:

1. Click the *Manage Redirection* link corresponding to the **subdomain** you wish to manage.
2. If you wish to **redirect** the **subdomain**, enter the link you would like to **redirect** the **subdomain** to in the available text field.
3. Click *Save*.
4. To disable the **redirect**, click *Disable Redirection*.

Remove a Subdomain

To remove an existing **subdomain**:

Click the *Remove* link corresponding to the **subdomain** you would like to remove.

Confirm that you would like to remove the **subdomain** by clicking *Yes*.

To keep the **subdomain**, click *No*.

Search Subdomains

You may also search through existing **domains**:

1. Enter the search criteria into the *Search* field.
2. Click *Go*.

Results matching your search criteria will populate the list.

DOMAINS

Addon Domains

When allowed by your web host, an **addon domain** allows a new domain name to link to subdirectory of your account. The **addon domain's** files will be stored in a subdirectory of your `public_html` folder. Creating an **addon domain** gives you the ability to control multiple **domains** from a single account.

Create an Addon Domain

To add an **addon domain**:

1. Enter the domain for the new **addon domain** into the *New Domain Name* field.
2. Enter the main **FTP** username for the **addon domain** in the *Subdomain/Ftp Username* field.
3. In the *Document Root* field, enter the directory that will contain the **addon domain's** files.
4. Enter the password for the **addon domain** into the *Password* field.
 - o Make sure you use a secure password.
 - o You can have cPanel generate a secure password for you using the *Generate Password* feature.
5. Confirm the password in the *Password (Again)* field.
6. Click *Add Domain!*
7. To add files to the **addon domain's** home directory, click the **File Manager** link.



You can also access this **addon domain's** home directory in the **File Manager** by clicking the link under *Document Root*.

Disable or enable add-on Domain Redirection

To disable or enable redirection of an addon domain:

1. Click the Manage Redirection link corresponding to the addon domain you wish to manage.
2. If you wish to redirect the domain, enter the link you would like to redirect the addon domain to in the available text field.
3. Click Save.

To disable the redirect, click Disable Redirection.

DOMAINS – Add-on Domains *continued*

Remove an Add-on Domain

To remove an existing addon domain:

1. Click the Remove link corresponding to the addon domain you would like to remove.
2. Confirm that you would like to remove the addon domain by clicking Yes.
3. To keep the addon domain, click No.

Search Add-on Domains

4. You may also search through existing **domains**:
5. Enter the search criteria into the *Search* field.
6. Click *Go*.
7. Results matching your search criteria will populate the list.

Addon vs Parked Domains

	Addon Domains	Parked Domains
Main domain appears in the address bar	Yes	No
Apache directive used	VirtualHost	ServerAlias
Separate logs	Yes	No
Separate stats	Yes	No
Treated as a subdomain (other than URL)	Yes	No
Ideal for multiple domains sharing the same address	No	Yes

DOMAINS *continued*

Parked Domains

Parked [domains](#) function as pointing devices. When a user enters the address for a [parked domain](#), it redirects to the main domain on which it is parked.

For example, if [example1.com](#) is parked on [example.com](#), [example.com](#) will be accessed when [example1.com](#) is entered into the web browser. Once the [parked domain](#) has been added to the [server](#), it can be removed or used as a redirector when you click the appropriate links under the *Actions* heading in the list.

Create a Parked Domain

To add a **parked domain**:

1. Enter the domain you wish to park in the available text field.
2. Click *Add Domain!*

To open the **parked domain's** home directory with the **File Manager**:

- Click the link under *Document Root* that corresponds to the **parked domain** you would like to view in the File Manager.

Enable or Disable Parked Domain Redirection

To enable or disable redirection of a parked domain:

1. Click the Manage Redirection link corresponding to the parked domain you wish to manage.
2. If you want to redirect the domain, enter the link you would like to redirect the parked domain to in the available text field.
3. Click Save.
 - To disable the redirect, click Disable Redirection.

DOMAINS – Parked Domains *continued*

Remove a Parked Domain

To remove an existing **parked domain**:

1. Click the *Remove* link corresponding to the **parked domain** you would like to remove.
2. Confirm that you would like to remove the **parked domain** by clicking *Yes*.

To keep the **parked domain**, click *No*.

Search Parked Domains

You may also search through existing parked **domains**:

1. Enter the search criteria into the *Search* field.
2. Click *Go*.

Results matching your search criteria will populate the list.

DOMAINS *continued*

Redirects

This feature allows for the redirection of users visiting a particular page. This can be useful when redirecting a short [URL](#) to a necessarily long [URL](#).

Create a Redirect

To add a **redirect**:

1. Use the pull-down menu to select the type of redirection needed; temporary or permanent.
 - The *Temporary 302* setting will not update the visitor's bookmarks.
 - The *Permanent 301* setting will notify the visitor's browser to update its records.
2. Specify the **URL** you would like the **redirect** to affect using the pull-down menu and corresponding text box.
 1. You may use the *All Public Domains* option to **redirect** all **domains** controlled by your cPanel accounts.

Specify where you would like the users accessing the **URL** specified above to land in the redirects to field.

- You must specify a protocol in this field, such as *http://*, *https://*, or *ftp://*.

Using the buttons below the redirects to field, specify whether to **redirect** with or without *www.* preceding the **URL**.

- When you select *Only redirect with www*, only users who type *www* in front of the page name will be redirected.
- When you select *Redirect with or without www.*, you will **redirect** all users regardless of whether the *www.* prefix is included with the **URL**.
- When you select *Do Not Redirect www.*, users who type *www.* with the **URL** will not be redirected.

Click the *Wild Card Redirect* box if you wish to **redirect** all files within a directory to the same filename in the new directory.

0. Example: When wild card redirects are active, if *example1.com* redirects to *example.com*, then a visitor trying to access *example1.com/pic.jpg* will be redirected to *example.com/pic.jpg*.

DOMAINS – Redirects continued

Click *Add*.

- You may test the [redirect](#) by clicking the link under *Directory*. This will take you to the original domain, which should be redirected, if it is properly configured.

To open a [redirect](#)'s home directory with the [File Manager](#):

- Click the link under the *Directory* heading that corresponds to the [addon domain](#) you would like to view in the [File Manager](#).

Remove a Redirect

To remove an existing **redirect**:

1. Click the *X* button corresponding to the **redirect** you would like to remove.
2. Confirm that you would like to remove the **redirect** by clicking *Yes*.
 - To keep the **redirect**, click *No*.

Search existing Redirects

You may also search through existing redirects:

1. Enter the search criteria into the *Search* field.
2. Click *Go*.

Results matching your search criteria will populate the list. You may sort the list of redirects by clicking on any heading. The redirects will be sorted according to the attribute you clicked (for example, *Directory* or *Type*).

DATABASES - MYSQL DATABASES

Databases offer a method for managing large amounts of information easily over the web. They are necessary to run many web-based applications such as bulletin boards, content management systems, and online retail shops.

If you need to create a database as well as the account that will access it, we recommend using the [MySQL Database Wizard](#). Alternatively, you may create a database, add users, and link a database to an existing user account using this screen.

Create a Database

To create the database:

1. In the *New Database* field, type a name for the database.
2. Click *Create Database*.
3. Click *Go Back*.
 - o The new database will appear in the *Current Databases* table.

Check a Database for Errors

If you are experiencing problems using any database related software you have installed on the **server**, you may check your databases for errors.

To check a database:

1. In the *Check DB* drop-down menu, select the database you wish to check.
2. Click *Check DB*.
 - o cPanel will run a script that checks to make sure the database is functional. The results will appear on a new screen.
 - If cPanel detects a problem in the database, it will indicate which table is corrupted.
 - If the *Check Complete* message appears without a notification that the database is corrupted, then the database is functional.


MYSQL DATABASES *continued*

Repair a Database

If you have checked a database and found an error, you will need to repair it.

To repair a database:


1. In the *Repair DB* drop-down menu, select the database you wish to repair.
2. Click *Repair DB*.
3. cPanel will run a script that attempts to automatically repair the database.

 **Note:** This will only attempt to repair the database. A repair may not be possible; in this case, you will be able to locate the source of the corrupt data.

Create a Database User

After you create the database, you will need to add users and their privileges so that the database can be filled and managed. Please note that MySQL user accounts must be created separately from mail and web administrator accounts.

To create a new user account:

1. To quickly access the MySQL Users interface, click Jump to MySQL Users.
2. Under Add New User, enter a username.
3. Enter a password in the Password field.
 - o  **Note:** The password must be 7 letters or shorter.
 - o For help generating a strong password, click the Generate Password button.
4. Retype the password in the Password (Again) field.
5. Click Create User.

MYSQL DATABASES *continued*

Define a User's Privileges

Privileges define how the user is able to interact with the database. For example, they will determine whether or not the user can add and delete information.

To define a user's privileges:

1. Under Add User to Database, select a user from the User drop-down menu.
2. From the Database drop-down menu, select the database to which you wish to allow the user access.
3. Click Add.
4. From the MySQL Account Maintenance screen, select the privileges you wish to grant the user, or select ALL PRIVILEGES.
5. Click Make Changes.

The Current Databases Table

This table contains a list of databases on your [server](#). For each database, the table displays:

- The name of the database.
- The size of the database.
- Users who may manipulate the database.
- A link allowing you to delete the database.

Search Databases

- To search the Current Databases table:
- Type your criteria in the Search field.
- Click Go.

The table will display the search results.

MYSQL DATABASES *continued*

Modify a User's Privileges

To modify a user's privileges for managing a database:

1. Click the user's name where it appears in the appropriate row.
2. On the *MySQL Account Maintenance* screen, select the actions you wish to allow the user to perform, and deselect the actions you wish to prohibit.
3. Click *Make Changes*.

Remove a User's Privileges

1. To disallow a user from managing a database:
2. Click the X icon next to the user you wish to delete.
3. If you are sure you want to remove the user's privileges to manage the database, click Yes.

Delete a Database

To delete a database from the **server**:

Locate the row corresponding to the database you wish to delete.

1. Click *Delete Database*.
2. If you are sure you want to permanently delete the database, click Yes.

Delete a MySQL User

To delete a MySQL user account:

1. Click *Delete* in the appropriate row of the *Current Users* table.
2. If you are sure you want to permanently delete the account, click Yes.

To enter new information into a database, you can use the phpMyAdmin client installed with cPanel. For more information regarding phpMyAdmin visit <http://www.phpmyadmin.net>.

DATABASES – MySQL DATABASE WIZARD


cPanel can guide you through the process of setting up a MySQL database, along with the requisite accounts and privileges, step by step.

To set up a database using the *MySQL Database Wizard*:

1. In the *New Database* field, enter a name for the database.
2. Click *Next Step*.
3. In the *Username* field, enter a name for the user allowed to manage the database.
4. In the *Password* field, type the user's password.
 - The password must be 7 letters or shorter.
 - For help generating a strong password, click the *Generate Password* button.
5. Retype the password in the *Password (Again)* field.
6. Click *Next Step*.
7. Select the privileges you wish to grant the user, or select *ALL PRIVILEGES*.
8. Click *Next Step*.

Next, cPanel will display a message stating that the database and user account were successfully set up. From here, you may select 1 of 3 options:

- **Add another database** — Returns to the start of the *MySQL Database Wizard*.
- **Add another user using the MySQL Databases Area** — Opens the [MySQL® Databases](#) page, wherein you may create additional user accounts and assign them to a database.
- **Return to Home** — Opens the [cPanel home screen](#).

 **Note:** When you add a user and database using the MySQL Database Wizard, the user is automatically given access to the database; there is no need to use the [Add User to Database](#) feature.

phpMyAdmin

phpMyAdmin is a third-party tool included with cPanel, used for manipulating MySQL databases over the Internet. Using phpMyAdmin, you can add and drop databases, create, alter, and delete tables, add, edit, and delete fields, execute SQL statements, and manage users, keys, and permissions.

For more information regarding all of phpMyAdmin's functions and a complete guide on how to use them, visit http://www.phpmyadmin.net/home_page/docs.php.

DATABASES – REMOTE MySQL®

Databases in cPanel can be accessed remotely, by other web servers. This can be useful if you wish to allow applications such as shopping carts or guestbooks on your other servers to access the databases.

Allow a Remote Server to Access your Databases

To specify remote servers able to access MySQL databases on your [server](#):

1. Type the host's name or [IP address](#) into the *Host* field.
 - o You may enter a fully qualified domain name ([FQDN](#)) or an [IP address](#).
 - o You may use % as a wildcard. For instance, to allow access from all IP addresses beginning with 208.77.188, you can enter 208.77.188.%.
2. Click *Add Host*.

Prevent a Remote Server from Accessing your Databases

To disallow a host from accessing databases on your [server](#):

1. Click the X icon next to the host's name or [IP address](#).
2. If you are sure you wish to prevent the [server](#) from accessing your databases, click Yes.

PostgreSQL

The instructions for using PostgreSQL are identical to those for MySQL.

PostgreSQL Database Wizard

Instructions are identical to those for the MySQL database wizard

pgMyAdmin

For more information regarding all of phpMyAdmin's functions and a complete guide on how to use them, visit http://www.phpmyadmin.net/home_page/docs.php

SOFTWARE/SERVICES - CGI CENTRE

Short for “Common Gateway Interface,” **CGI** lets a web **server** run pieces of software called scripts. cPanel’s *CGI Center* provides **CGI** scripts that can do many useful things for your website, like create a guestbook, clock, hit counter, countdown clock, and banner ads


Simple CGI Wrapper

CGI scripts are pieces of software that can do many useful things for your website; for example, a **CGI** script can create a chat room or shopping cart.

The *Simple CGI Wrapper* creates a special folder, called **/scgi-bin**, inside the **/public_html** directory. When you add scripts to this folder, your web **server** knows to handle them as **CGI** scripts.

You can access the simple **CGI** wrapper in the *CGI Center* by clicking the appropriate link. **CGI** scripts will need to be placed in **/public_html/scgi-bin** for cPanel to handle them as **CGI** scripts. Once a script has been placed in this folder, it will run whenever a visitor uses a web browser to view, as an example, <http://www.example.com/scgi-bin/examplescript.cgi>. **CGI** scripts can also be embedded in a webpage using the `<action>` tag.

Please note that every **CGI** script will have unique setup needs; be sure to consult the script’s installation instructions. For example, URLs and variables may need to be defined. You can do this using cPanel’s **File Manager**, or from the command line interface (**CLI**). (To use the **CLI**, you will need **SSH** access to the web **server** as well as a command line text editor.)

 **Note:** Your web host may provide a feature called *suEXEC* that lets it run **CGI** scripts, making the *Simple CGI Wrapper* unnecessary for your website. Contact your web host or review the terms of your agreement to find out whether this is the case.

SOFTWARE/SERVICES *continued*

Random HTML Generator

If you would like to show a different fact, quote, or other piece of text every time a visitor views your website, you can use the *Random HTML Generator*.

To insert random text on a web page:

1. At the *CGI Center*, click the *Random HTML Generator* link.
2. Enter any information you would like to display into the text box.
 - o Separate each comment by line.
3. Click *Save*.
4. Add the line of **HTML** code shown on the *Editing the Random HTML Template* screen to your web page's **HTML**.
 - o `<!--#include virtual="/cgi-sys/randhtml.cgi?user"-->`
 - o Replace **user** with your username.
 - o Make sure to save the web page with a name ending in **.shtml**.

Every time a visitor views the web page, he will see a fact or quote from the text box.

Simple Guestbook

cPanel can generate a simple guestbook for your website. Guestbooks allow visitors to leave comments about your website.

The *Simple Guestbook* screen shows a sample of what the guestbook will look like on your website.

Add a Guestbook

To add a simple guestbook:

- Copy and paste the **HTML** code from the bottom of the screen into your web page.

Once this is done, visitors to your site will be able to sign your guestbook and view others' greetings.

View Your Guestbook

- To view the guestbook on your website, click the *View Guestbook* link.

SOFTWARE/SERVICES *continued*

Delete Guestbook Entries

- To delete entries or email a guest, click the *Manage Guestbook* link.

The Edit Default CGI and Edit Guesbook Template Links

These links, located at the top of the *Simple Guestbook* main page, allow you to edit the appearance of the guestbook. To accomplish this you will need to be familiar with [HTML](#). Consult your preferred search engine for tutorials and information about [HTML](#).



Remember: Click *Save* when you are finished modifying the [HTML](#) code in the text box.

Advanced Guestbook

The Advanced Guestbook is not enabled on your cPanel.


SOFTWARE/SERVICES *continued*

Counter (Add a Counter, Clock or Date)

You can add a “hit counter” to your website, which tells you how many times your site has been viewed. You can also display the current time or date on your website. From the *CGI Center*, click the *Counter* link.


1. Under *Please select functionality*, select *Counter, Clock, or Date*.
2. The next 2 items (*Please select time zone* and *TimeFormat*) only affect the clock function. If you are creating a counter please skip to step 4. For a date display, skip to step 3. If you are creating a clock,
 - o Choose the appropriate time zone. For example, if you want your website to display Eastern Standard Time (U.S.), then select *GMT-0500*.
 - o Under *Please select Format*, next to *TimeFormat*, choose a 12-hour or 24-hour clock. (For example, 1:00 PM in 12-hour format is the same as 13:00 in 24-hour format.)
3. Under *Please select Format*, next to *Date Format*, select the way you want the date to appear.
4. Under *Please select Format*, you will need to enter the thickness of the frame that will appear around your counter. To do this, enter a number into the box, or click the “+” or “-” signs to increase or decrease the frame’s thickness. (You will be able to preview and adjust this later.)
5. Under *Please select Frame Color*, enter the values for the frame’s color. To make this easier, cPanel provides a graphic tool for choosing a color. You can use this tool by clicking the multicolored box.
6. Choose the color you wish to use, then click the “x” in the upper right corner of the color selector.
7. If you are creating a counter, under *Please select Maximum digits*, choose the number of digits that will appear in your counter. If you are creating a clock or date display, skip to the next step.
8. Under *Please Select Style*, click the *See Styles* link to view the 33 different types of displays available. Then enter the letter or number of the style you want. Please note that not all styles will work with the clock or date display.
9. Under *Counter Name*, enter the name you want cPanel to use to save the counter, clock, or date display on the web [server](#).
10. The *Color Replacer* will find and replace all instances of one color with another. This is helpful if, for example, you want to replace the colors of the numbers in the display.
 - o To enter a color to be replaced, click the multicolored box next to *Source Color* and choose the color you wish to replace.
 - o Then click the multicolored box next to *Replacement Color* and choose the color you wish to change it to.
11. To view the counter, clock, or date display before it goes onto your website, click the preview button. You may preview the display as many times as you need to. Once it looks acceptable, click *html*.
12. cPanel will show the [HTML](#) code that creates the counter, clock, or date. Simply copy the text beginning with `` and paste it into the web page where you want the counter to appear.

- If, after you have created the display, you want to change its name, simply enter the new name in the *Counter Name* box and click *Commit Changes*.
- To reset the count, enter a number in the *New Count* box, and click *Commit Changes*.

 **Note:** Clicking *Clock* directly from the *CGI Center* will display a different screen; this is simply another method of creating a clock for your site.

Clock

Using this feature, you can create a clock for your website.

 **Note:** Clicking *Counter* and choosing *Clock* from the *Counter* screen is another method of creating a clock for your site.

To do so:

1. From the *Select your TimeZone* menu, choose the correct zone.
 - For example, if you want your website to display Eastern Standard Time (U.S.), then select *GMT-0500*.
2. Under *Select your Time Format*, choose a 12-hour or 24-hour clock.
 - For example, 1:00 is 12-hour format, versus 13:00 in 24-hour format.
3. Under *Border*, choose whether you would like a border around your clock (*On*) or not (*Off*).
4. Choose whether you would like your clock to show the day of the month in small numbers following the time using the *Show Date* pull-down menu.
5. Choose which color you would like the numbers to be with the *Foreground Color* pull-down menu.
6. Choose which color you would like the background to be with the *Background Color* pull-down menu.
7. Click *Create Html*.

cPanel will show the **HTML** code that creates the clock. Simply copy the text beginning with `<applet` and ending with `</applet>` and paste it into the web page where you want the clock to appear.

SOFTWARE/SERVICES – CGI Centre *continued*

Countdown

You can create a countdown clock for your website. This is useful if, for example, you want to show your visitors how much time is left until a certain event.

To add a countdown clock:

1. From the *CGI Center*, click *Countdown*.
2. From the *Select your TimeZone* menu, choose the correct zone.
 - For example, if you want your website to display Eastern Standard Time (U.S.), then select *GMT-0500*.
3. Choose the year, month, day, and hour of the event to which you want to count down. Then click the *Create Html* button to see a preview of the countdown clock.
4. cPanel will show the **HTML** code that creates the countdown clock. Simply copy the text beginning with `<applet` and ending with `</applet>` and paste it into the web page where you want the clock to appear.

CGI Email

CGI Email uses a basic script which lets visitors email comments to you. One way to create this form is by clicking *CGI email* from the *CGI Center*.

Setting up **CGI** email is complex and requires a number of steps. Please use the *cgimail user guide link* that comes up when you click on *CGI Email* to help you set up a **CGI** email form.

SOFTWARE/SERVICES – CGI Centre *continued*

Entropy Search

cPanel includes a small *Search* function that will allow your visitors to find information on your website quickly. From the [CGI Center](#), under *Entropy Search*, click *Setup Search Engine*. cPanel will show a sample search box, and the [HTML](#) code that creates it.

To add a search box:

- Copy the text beginning with `<form>` and ending with `</form>` and paste it into the web page where you want the search box to appear.

If you're comfortable working with [HTML](#) and you would like to change the appearance of the results page that visitors will see, click *Edit Search Results Template*. Here, you may change the background color, add a background image, and edit the title of the results page. Once you have made your changes to the [HTML](#) file, click *Save*.



Important: Before your search box will work, you must click the *Rebuild Search Index* link under *Entropy Search* in the *CGI Center*. This sets up an internal list of your website's contents, so they can be searched. It's a good idea to click this link whenever you add new pages to your website.



Remember: The larger your website, the longer the *Rebuild Search Index* link will take.

Entropy Banners

cPanel comes equipped with an application that is capable of managing a rotation schedule for your banner advertisements. This is useful if you would like your visitors to see different logos or advertisements each time they access your site. To begin, click the *Entropy Banners* link in the *CGI Center*.

Configure Rotating Banners

To set up rotating [banners](#), you must first add [banners](#):

1. Click the *Add Banners* button.
2. Click *Choose File* and select the image you would like to add from your computer.
 - You can repeat this process for each banner you would like to add.
 - You can choose up to 12 images at a time.

3. If you want to replace existing **banners**, click the checkbox next to *Overwrite* existing files.
 - o This will replace older ads with newer ones, as long as they have the same filename. (If you want to delete ads one at a time, see below).
4. Click *Upload*.
 - o cPanel will tell you whether the upload was successful.
Remember: that the file must end in **.shtm** or **.shtml** in order to work on your web page.

Control a Banner's Schedule

cPanel also makes it easy to control how often a certain banner ad will display.

To control the **banners'** display schedule:

1. From the *Entropy Banners* screen, click *Modify Rotation*.
2. Select *High*, *Medium*, or *Low* priority for each banner, depending on how often you want it to appear on your site.
3. Click *Save* to store your changes.
4. Under *Linked to*, enter the web address where the visitor will go when he clicks the banner.
5. Click *Save*.

Add Rotating Banners to a Page

To create rotating banners on a page: On the main Entropy Banners page, copy the test that begins with `<!--#exec cgi` and ends with `-->` and paste it into the web page's **HTML** file.

Site Software

Because there are already many programmes available through Fantastico, as well RV SiteBuilder available through cPanel, this link is not relevant.

SOFTWARE/SERVICES - Perl Modules

View Available Perl Modules

To view all available [Perl](#) modules:

1. Click *Show Available Perl Module(s)*.
2. Once you find the module you want to install, click *Install*.



Note: As this process takes time, it is not a time/resource efficient way to find [Perl](#) modules for your website.

Search Available Perl Modules

To search for a module based on a topic or keyword:

1. Type the keyword into the *Search* box and click *Go*.
2. Once you find the [Perl](#) module you want to install, click *Install*.
 - o To view the [Perl](#) module creator's documentation, click *Show Docs*.

Install a Perl Module

If you know the name of the [Perl](#) module you want to install:

1. Type it in the box under *Install a Perl Module*.
2. Click *Install Now*.

The Installed Perl Module(s) table

The *Installed Perl Module(s)* table lets you manage the modules you have installed. The table shows the name of the software (*Module Name*), its version, and what you can do with it.

- If you believe a [Perl](#) module is out-of-date, cPanel can update it for you. To update a [Perl](#) module, click *Update*.
- If you believe an installed [Perl](#) module has become corrupted or lost, you can reinstall it. To do this, click *Reinstall*.
- To uninstall a [Perl](#) module, click *Uninstall*.
- To view the [Perl](#) module creator's documentation, click *Show Docs*.

SOFTWARE/SERVICES - Perl Modules *continued*

System Modules

There are certain [Perl](#) modules that come pre-installed in cPanel. You can see a list of these by clicking [Show System Installed Modules](#).

Click [Show Docs](#) to view the documentation for the installed modules.

PHP PEAR Packages

[PEAR](#) packages are pieces of software written in the [PHP](#) scripting language. cPanel makes it easy to search for and add [PHP PEAR](#) packages to your website. Click [PHP PEAR](#) Packages to view all available [PHP](#) packages, search for a specific kind of package, or, if you know its name, add one immediately.

View Available PEAR Packages

To view all available [PEAR](#) packages:

1. Click [Show Available PHP Extension\(s\) and Application\(s\)](#).
 - o Once you find the [PEAR](#) package you want to install, click *Install*.

Search Available PEAR Packages

To search for a [PEAR](#) package based on a topic or keyword:

1. Type the keyword into the *Search* box and click *Go*.
2. Once you find the [PEAR](#) package you want to install, click *Install*.
 - o To view the [PEAR](#) package creator's documentation, click *Show Docs*.

SOFTWARE/SERVICES - PHP PEAR PACKAGES *continued*

Install a PEAR Package

If you know the name of the [PEAR](#) package you want to install:

1. Type it in the box under *Install a PHP Extensions and Applications Package*.
2. Click *Install Now*.

The Installed PHP Extension(s) and Application(s) Table

The Installed [PHP](#) Extension(s) and Application(s) table lets you manage the [PEAR](#) packages you have installed. The table shows the name of the software (*Module Name*), its version, and what you can do with it.

- If you believe a [PEAR](#) package is out-of-date, cPanel can update it for you. To update a [PEAR](#) package, click *Update*.
- If you believe a [PEAR](#) package has become corrupted or lost, you can reinstall it. To do this, click *Reinstall*.
- If you wish to uninstall a [PEAR](#) package, click *Uninstall*.
- To view the [PEAR](#) package's documentation, click *Show Docs*.

System Modules

There are certain [PEAR](#) packages that come pre-installed in cPanel. You can see a list of these by clicking *Show System Installed Modules*.

⚠ Remember: System installed modules cannot be removed. You can see the documentation for the system installed [PEAR](#) packages by clicking *Show Docs*.

SOFTWARE/SERVICES *continued*


PHP CONFIGURATION

If problems are encountered with the way your [server](#) handles [PHP](#) packages, it may be necessary to view information about the way [PHP](#) is configured. You can do this by clicking [PHP Configuration](#). Here, every configuration option from the language options to the maximum file upload size are displayed.

Please note that none of the [PHP](#) configuration information can be changed by using this feature. To change the way [PHP](#) is configured on your [server](#), please contact your web host.

PHP Directives

Following is a brief description of what each Directive in the [PHP](#) Configuration table means.

- **asp_tags:** Tells whether your [server](#) allows [PHP](#) code to include the tags <% and %> instead of the standard <?php and ?> tags. If this option is turned off, a [PHP](#) script with ASP tags will not work properly.
- **file_uploads:** Tells whether your [server](#) will allow [PHP](#) scripts to receive files via [HTTP](#) (i.e., the web).
- **include_path:** Tells where your website will look for [PHP](#) files. Be sure that all [PHP](#) scripts you want to run are saved in the folder indicated here.
max_execution_time: The number of seconds a [PHP](#) script is allowed to run before being closed. This limit prevents poorly written scripts from slowing your [server](#) down.
- **max_input_time:** The number of seconds a [PHP](#) script is allowed to process information input to it, such as file uploads. This limit prevents the script from being overloaded and slowing your [server](#) down.
- **memory_limit:** The maximum number of bytes that a [PHP](#) script can use. This limit prevents poorly written scripts from occupying all your [server](#)'s available memory. When this field is set to -1, there is no memory limit.
- **register_globals:**  **Warning:** This is an outdated feature that should be set to *Off*. Using a [PHP](#) script that requires this field to be turned on will make your site secure.

SOFTWARE/SERVICES – PHP CONFIGURATION *continued*

- **safe_mode:** This feature ensures that the user running the **PHP** script has permission to perform all the tasks the script is written to do. For example, if the script is designed to change a file, the user will need the correct permissions to modify the file. The feature is outdated, however, so your web host may have it disabled, and use another security measure instead.
- **session.save_path:** When a visitor accesses your website, he is issued a unique user ID. Information about the user ID's session, or time spent on your website, is stored to the web **server**. The **session.save_path** directive describes where that information is stored. (**PHP** allows you to make web content specific to a given visitor and session.)
 - If the *Value* column has a number in it, it refers to the number of directories the information is saved in. If your site has a lot of traffic, distributing session data among several folders makes it easier for the **server** to save and retrieve the information.
 - The text in the *Value* column tells the name of the directory that contains the subdirectories with the session information.
- **upload_max_filesize:** The maximum number of bytes that an uploaded file can contain.

Select a PHP Version

PHP Versions 4 and 5 are available on the server. You may select the version you wish to use from this screen. If everything is working correctly, it is suggested to leave it at the Default version.

To select a **PHP** version:

1. From the drop-down menu, select the version of **PHP** you wish to use, or select *System Default* to use the version your web host has chosen.
2. Click *Update* to update the selection.

Ruby Gems and Ruby on Rails

These are advanced applications – please see the **Advanced** page for links to relevant information.

SOFTWARE/SERVICES *continued*

Optimize Website

This feature allows you to automatically compress certain types of content when that content is requested by visitors.



Note: This feature may not be available to all users. If you wish to use this feature, contact your web hosting provider.

To disable compression of your website's content:

1. Select the *Disabled* option.
2. Click *Update Settings*.

To compress all your website's content:

1. Select the *Compress all content* option.
2. Click *Update Settings*.

To compress only certain types of content:

1. Select the *Compress the specified MIME types* button.
2. In the *MIME types* text box, enter the types of content you wish to compress.
 - o A list of MIME types is available [here](#).
3. Click *Update Settings*.

For more information about the software module that handles compressing content for your website, you will need to know which version of the [Apache](#) web [server](#) software is running on the [server](#). You can find this information on the main cPanel home screen, in the [Server Stats](#) box.

- [Apache 2.0 web server documentation for mod_deflate](#).
- [Apache 2.2 web server documentation for mod_deflate](#).

SOFTWARE/SERVICES *continued*

RVSite Builder

This free application can help you if you choose to build yourself a website or a blog. It has a user-friendly interface which takes you step by step through the process and will save your work if you wish to take a break at any time.. Simply click on the link to get started.

Fantastico deluxe

Fantastico De Luxe is the leading autoinstaller for cPanel servers. With more than 10.000 installations, it provides more than one million end users the ability to quickly install dozens of the leading open source content management systems into their web space.

It integrates with your cPanel and gives you the ability to install multiple instances (*) of most of the scripts :

- in add-on domains
- in subdomains
- in top level directories (root of main domain and/or any addon domain/subdomain)

(*) PHPCoin can be installed only once per user account.

Click on Fantastico to see what is available.



Note that we do not provide support for these programmes. If you wish to learn how to use them properly it is suggested you go to the relevant website which is given within the Fantastico application.

ADVANCED

Apache Handlers

[Apache](#) handlers control how your site's [Apache](#) web [server](#) software manages certain file types and file extensions. [Apache](#) comes configured to handle [CGI](#) scripts and [server](#)-parsed files. Their file extensions include: `.cgi`, `.pl`, `.plx`, `.ppl`, `.perl`, and `.shhtml`.

You can configure [Apache](#) to handle a new file type with an existing handler by manually adding the handler and extension to cPanel. For example, to have the [server](#) treat files with the extension `.example` as [CGI](#) files, you would type "cgi-script" under *Handler* and "`.example`" under *Extension(s)*.

Add an Apache Handler

To add an [Apache](#) handler:

1. Enter the handler name into the *Handler* field. The built-in handlers are as follows:
 - **default-handler:** Sends the file using [Apache](#)'s default handler for static content.
 - **send-as-is:** Sends the file with [HTTP](#) headers as they are.
 - **cgi-script:** Handles the file as a [CGI](#) script.
 - **imap-file:** Parses the file as an imagemap rule file; for more information, see [Apache](#)'s documentation.
 - **server-info:** Retrieves the [server](#)'s configuration information.
 - **server-parsed:** Parses the file for [server](#)-side includes.
 - **server-status:** Retrieves the [server](#)'s status report.
 - **type-map:** Parses the file as a type map file; for more information, see [Apache](#)'s documentation.
2. Enter the file extension in the *Extensions* field.
 - You may enter more than 1 extension at a time. Simply separate each entry with a space.
3. A file extension is made of the letters after the dot (".") in a file name.
 - For example, `filename.fileextension`.
4. Click *Add*.



Note: This interface does not allow you to create custom [Apache](#) handlers.

Remove a Handler

To remove an existing handler:

1. Click the X button under the *Remove* heading next to the appropriate handler in the list.
2. Click Yes to confirm that you wish to remove the handler.remove the handler.



Note: The file extensions automatically handled by [Apache](#) cannot be removed.

ADVANCED *continued*

Image Manager

cPanel includes 3 tools to help you manage the images you use on your website.

- The *Thumbnailer* will resize an entire directory of images to your preferred size and store them in a folder called `thumbnails`.
- The *Image Scaler* can resize individual images.
- The image converter, under the *Convert Image Format* link, can be used to convert one type of image file to another.

Thumbnailer

cPanel includes an application for creating smaller versions of images, called “thumbnails.” This can be useful in creating a photo page where smaller previews of your images can be viewed before the larger original image is accessed, saving bandwidth.


The application is known as the Thumbnailer and can be accessed by clicking Image Manager, then clicking the *Thumbnailer* link. From here, an entire directory must be selected.



Note: The Thumbnailer application will not resize individual images.

Convert Images to Thumbnails

To convert a directory of images to thumbnails:

1. Navigate to the directory you would like to change to thumbnails by clicking the  button(s).
2. Click the name of the folder in blue to create thumbnails for the images in the directory.
3. Click *Thumbnail Images* to finish the process.
 - You may use the *Scale Percent* text boxes to define how small the images should be.
 - We recommend that you keep the *Keep Aspect Ratio* checked when creating thumbnails to prevent the image from becoming distorted by keeping the height and width proportional.
 - You may click *Reset Dimensions* to return the *Scale Percent* values to the default.

ADVANCED – IMAGE MANAGER *continued*

After the application has completed the task of resizing your images, a **thumbnails** directory will be created as a subdirectory within the selected folder. The **thumbnail** images will be created with the prefix **tn_***, where ***** is meant to represent the filename and extension.


Click the *Your images have been thumbnailled into* link to open the thumbnails directory in the cPanel [File Manager](#).

Image Scaler

cPanel can resize a single image with the *Image Scaler*. The *Image Scaler* operates by allowing you to [key](#) in percentages to scale the image up or down.

Rescale an Image

To rescale an image:

1. Navigate to the directory containing the image you wish to rescale by clicking the  button(s).
2. Click on the image, in blue, you wish to resize.
3. Click *Scale Images* to finish the process.
 - You may use the *New Dimensions* text boxes to define, in pixels, how the image should be resized.
 - You may use the *Percent* text boxes to define the percentage by which the image should be resized.
 - You may click *Reset Dimensions* to return the Scale Percent values to the default.
 - We recommend that you keep the *Keep Aspect Ratio* checked when scaling images to prevent the image from becoming distorted by keeping the height and width proportional.
 - You may click the *Retain a copy of the old image* as checkbox to store a copy of the original image in the directory you specify in the field below.
 - Click the link to view the rescaled image.

ADVANCED – IMAGE MANAGER *continued*

Convert an Image Format


cPanel includes an application for converting image file formats. Once you have uploaded the image to your website, it can be selected and converted through cPanel's format converter. Any of the supported file types can be converted from one type to another using this application. Once the conversion is complete, the new file is placed in the same directory as the original by default.



Note: This feature will convert all of the images in a directory. A single image cannot be converted.

Convert Image Format

To convert the image format:

Navigate to the directory of images you wish to convert by clicking the  button(s).

1. Click on the directory, in blue, you wish to convert.
2. Select the file format to which you would like to convert the images. You may select:
 - .PNG
 - .JPG
 - .GIF
 - .BMP
3. Click *Convert*.

ADVANCED *continued*

Index Manager

When accessing a directory (rather than a page) on your site, a visitor will typically see the index page for that directory. If no index page exists, the browser will display a list (or index) of the files in that directory.

Using the *Index Manager*, it is possible to define how a specific directory index will appear to those who access it. You can also turn off indexing, if you don't want a directory's contents to be visible.

1. To navigate the *Index Manager*, click the folder icon next to the directory name.
2. Click the name of the directory for which you want to change the indexing style.
3. cPanel offers 4 options; select 1 of the following:
 - **Standard Indexing:** Contents appear only as filenames.
 - **Fancy Indexing:** Information about the files, such as the size and time last modified, appear.
 - **Default System Setting:** The default defined by your web host will be used.
 - **No Indexing:** The contents of the directory are not listed; visitors will see a message stating that the contents are "forbidden."
4. Click *Save*.

Error Pages

An error page informs a visitor when there is a problem accessing your site. Each problem has its own code (such as 404, 500, etc.) and corresponding error page.

Basic [error pages](#) are automatically provided by the web [server](#). However, cPanel allows you to define custom [error pages](#) for any [HTTP code](#).

To edit an error page:

1. Click the error code for the page you wish to edit.
 - If you don't see the error code for the page you wish to edit, click the *Show All HTTP Error Status Codes* tab.
2. Type a message into the text box.
 - You can select certain [HTML](#) tags to be added to a custom error page. These tags will display facts on the error page about the visitor accessing your website.
 - You can further customize your [error pages](#) by keying in [HTML](#) code.
3. Click *Save*.



Note: This feature is currently incompatible with the Safari® browser.

ADVANCED *continued*

Cron Jobs

Cron jobs are scheduled tasks that take place at predefined times or intervals on the [server](#). Often, a [cron job](#) is a series of simple tasks executed from a script file. cPanel offers a standard and an advanced tool for setting up cron jobs.

Both methods will require you to enter an email address if you want the [cron job](#) to email you results every time it runs.



Note: Be careful when scheduling cron jobs. Setting them to run too often may slow down your [server](#).

The Standard Interface

In this interface, the automation can be defined by entering a command into the appropriate box and using the lists to define how often the command should be run.

To set up a [cron job](#) using the standard interface:

1. If you want the results of the [cron job](#) emailed to you, enter an email address in the text box.
2. Next to *Command to run*, type the command you'd like to execute.
3. Enter the minute, hour, day, month, and weekday you'd like the [cron job](#) to run.
 - o You can click *Delete* to start over.
4. Click *Save Crontab*.
 - To return to the default settings at any time, click *Reset Changes*.

The Advanced Interface

In the *Advanced* interface, the schedule times are not pre-configured and must be defined using a series of text boxes.

To set up a [cron job](#) using the advanced interface:

1. If you want the results of the [cron job](#) emailed to you, enter an email address in the text box.
2. Enter the minute, hour, day, month, and weekday you'd like the [cron job](#) to run.
 - o Asterisk (*) stands for every instance of a given category (such as every day or every minute).
 - o Use 24-hour time to specify the hour.
 - o Under day, enter the day of the month.
 - o Under month, enter a number from 1 to 12. (1 means January and 12 means December.)
 - o Under weekday, enter a number from 0 to 6. (0 means Sunday and 6 means Saturday.)
3. Under *Command*, type the command you'd like to execute.
4. Click *Commit Changes*.
 - To return to the default settings at any time, click *Reset Changes*.

ADVANCED *continued*

FrontPage Extensions

FrontPage extensions will allow web pages to be published directly from the Microsoft® FrontPage application, eliminating the need to use FTP. This can be useful in streamlining the publishing process.



Warning: Installing Frontpage extensions will delete any .htaccess files contained within your web area. This means that any directory or web page that requires authentication (a username and password) will need to be reconfigured after the extensions are installed.

.htaccess files

.htaccess files are an integral part of any basic authentication process. The file lives within a directory on the server and is used to enact the authentication process when the directory is accessed. The .htaccess file is then checked against a file that contains an encrypted instance of the valid password for the directory.

.htaccess files also contain information about how the contents of the directory will be displayed, as well as information about how long visitors' browsers will "cache" your site, or save it in memory.

ADVANCED *continued*

Network Tools

This area of cPanel's interface contains tools for retrieving network information. For instance, you can look up an [IP address](#) or trace the route from your computer to the computer on which your website is hosted (your web [server](#)).

Domain Lookup

cPanel's *Network Tools* will execute a basic command for resolving an [IP address](#) from a specified domain name. The query will also return general [DNS](#) information about the [server](#).

To look up a domain:

1. Enter the domain you would like to lookup in the *Enter a domain to lookup* field.
 - o Example: `cpanel.net`.
2. Click *Lookup*.


The resulting page will display the domain's mail servers as well as the [IP address](#) for that domain. You can also view the domain's [DNS](#) information under the *Zone Information* heading.

Trace Route

cPanel's *Network Tools* includes a function for uncovering the route your computer takes to access your website. This function will show you how many servers your data is passed through before it reaches your website. Included in this information is the amount of time your computer took to reach the [server](#).

- To trace the route to your [server](#), click *Trace*.

The resulting page will display all of the pathways your computer took to reach your [server](#). This can be useful in pinpointing problem servers within your path.

 **Note:** This function may be disabled; contact the system administrator for more information about using the *Trace Route* function.

ADVANCED *continued*

Submit a Support Request Disabled in CPANEL. For support please click [HERE](#)

Virus Scanner

Virus Scanner powered by ClamAV™ - You can run a scan of your web files from here.

MIME Types

MIME types relay information to the browser about how to handle file extensions. Adding MIME types is useful for enabling visitors' browsers to handle new technologies as they come out. cPanel lets you add new MIME types to your web [server](#) by defining a name, directory, and corresponding file extension.

Add a MIME type

To add a [MIME type](#):

1. Enter the name of the file type's handler into the *Mime Type* field.
 - For example, *application/cgi* would be the handler for the *.cgi* extension.
2. Enter the file extension in the *Extension(s)* field.
 - A file extension is made of the letters following the dot (".") in a file name. For example, *filename.fileextension*.
3. Click *Add*.

Delete a MIME type

To delete a [MIME type](#):

1. Click the X icon under the *Remove* heading.
2. Click *Yes* to confirm that you wish to remove the [MIME type](#).

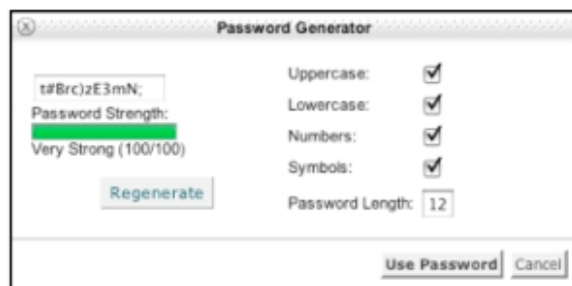
More about MIME types

A list of MIME types can be found at <http://www.webmaster-toolkit.com/mime-types.shtml>. You may also want to use your preferred search engine to research the [MIME type](#) you would like to add.

PASSWORD GENERATOR

Using the Strong Password Generator

cPanel provides a helpful tool for generating secure passwords that are difficult for malicious users to guess. You can use this Strong Password Generator by clicking *Generate Password* anywhere the button is available.



The Password Generator

When the *Generate Password* button is clicked, the new password will appear in the text box within the pop-up window. A bar graph indicating the “strength” of the password appears below it. The password’s strength is rated with a number between 0 and 100. A strength rating of 100 is recommended, as this indicates that the password is very secure.

If the password in the text box is not suitable, you can create a new one as many times as you like, until you are satisfied with the password.

To generate a new password:

1. Click the *Regenerate* button.
2. Dictate the contents of the new password:
 - o You can click the checkboxes on the right to include or leave out uppercase letters, lowercase letters, numbers, or symbols.
 - o You can specify the length of the password in the *Password Length* text box.
3. Click *Use Password* to use the password you have just generated.
 - o To close the *Strong Password Generator* without using the password displayed, click *Cancel* or the X in the upper left corner of the window.

cPANEL GLOSSARY:

Account: A record for accessing privatized information. For example, your cPanel account lets you manage your website. In cPanel, other instances of the term “account” occur in email and FTP

Account-Level Filter: A rule that determines where email, delivered to a domain's main email account and meeting certain criteria, will be delivered. See also Filter

Addon Domain: An additional domain name associated with your cPanel account. Each addon domain is stored in its own directory which you can configure. This allows you to manage multiple domains from a single cPanel account. Addon domains must be registered with a domain name registrar to work.

Analog: A program that provides information about the visitors to your website in both graphical and statistical views. More information about Analog can be found at its website:
<http://www.analog.cx/>.

Anonymous FTP: A process whereby visitors without FTP accounts may upload and download files to and from your site. Although it poses security risks, anonymous FTP can be convenient if you wish to make files publicly available for downloading. When setting up anonymous FTP, it is important to protect any sensitive information by changing file permissions and directory access permissions.

Apache: A program that receives requests from web browsers. It then responds by “serving” web pages to the browsers; for this reason, it’s called web server software.

Apache Handler: A means of telling the Apache software how to process a given type of file. By default, Apache only handles certain file types; using cPanel, you can configure Apache handlers for other file types. For more information, see Apache's handler documentation.

Authentication: A process for confirming the identity of someone with whom you want to share sensitive information. On the web, authentication usually involves either a username and password set or a public/private key pair

Auto Responder: A feature of cPanel that allows you to set up automated replies to incoming email. This feature can be useful for confirming the receipt of mail, or for informing correspondents that the recipient is unavailable (for example, while on vacation).

AWStats (Advanced Web Statistics): A program that provides information about the visitors to your website in both graphical and statistical views. More information about AWStats can be found at its website: <http://awstats.sourceforge.net/>.

Backscatter: Bounce email messages (or failed Delivery Status Notifications) erroneously sent to a domain whose name has been forged as the sender of spam. Using SPF on your mail server should reduce backscatter

Backup: A copy of your website's files, directories, databases, and email configurations. Keeping a backup copy of your website on your personal computer is a wise precaution.

Bandwidth: The amount of data transferred to and from a web server. Every time a visitor views a file (whether it's a web page, image, video, or audio file), that file has to be transferred to the visitor's computer. Bandwidth is the total size of all these files transferred to your visitors' computers. It is important to keep track of bandwidth usage, as it is limited by web hosts.

Banners: Images which appear on a website, often as advertisements at the top or bottom of a page. Often, banners alternate with each successive visit to the page.

BoxTrapper: An application included with cPanel that filters spam by requiring would-be senders to reply to a verification email (also known as challenge-response verification). Only after the sender is verified through the reply will his or her original email be accepted.

BoxTrapper Blacklist: A list of email addresses from which incoming mail will be automatically blocked. cPanel automatically sends a configurable warning message upon receipt of mail from a blacklisted address. See also BoxTrapper Ignore List and Whitelist.

BoxTrapper Ignore List: A list of email addresses from which incoming mail will be blocked. cPanel does not send a warning message upon receipt of mail from an ignored address. See also BoxTrapper Blacklist and Whitelist.

BoxTrapper Whitelist: A list of email addresses from which incoming mail will automatically be accepted. See also BoxTrapper Ignore List and Blacklist.

Build: A minor version of cPanel. Builds exist in four types which are, in order from least to most stable, EDGE, CURRENT, RELEASE, and STABLE. Please visit our installation documentation for an in-depth look at each build type.

Catch-All Address: The email address to which cPanel routes any email message sent to email accounts which do not exist at your domain. Also called a Default Address.

CGI (Common Gateway Interface): A protocol that lets a web server communicate with scripts and other software. cPanel's *CGI Center* provides an array of CGI scripts that let you generate and manage useful features for your website, including a guestbook, clock, hit counter, countdown clock, and banner ads.

CIDR (Classless Inter-Domain Routing): A routing method that assigns each Internet user to a four-part IP address, with each part separated by a decimal, followed by a slash and a number between 0 and 32.

CLI (Command Line Interface): A means of communicating with a computer by typing commands. On Unix systems, this is also often called a shell.

Client: Any application that accesses a service on another computer. Web browsers such as Internet Explorer can be called web clients. FTP clients include FileZilla and Cyberduck.

cPAddons: Pieces of software that you can install on your website through cPanel. cPAddons provide useful tools to your website. Common examples include bulletin boards, chat programs, and online shopping carts.

CPAN (Comprehensive Perl Archive Network): The main repository of Perl modules, pieces of Perl software. The CPAN library (located at <http://www.cpan.org>) contains over 12,000 modules, most of which are free of charge. cPanel allows you to search CPAN and install Perl modules.

Cron Job: A command on a server, executed at regular intervals. These commands are stored in a Unix configuration file called crontab.

CSR (Certificate Signing Request): A request, which you send to a certificate authority, for an identity certificate. cPanel can generate a CSR for you, but since authorities vary with regard to the information they require, you should check their requirements before applying for a certificate.

Default Address: The email address to which cPanel routes any email message sent to email accounts which do not exist at your domain. Also called a Catch-All Address.

Directory (Folder): A repository for files, analogous to a file folder on your personal computer. In website management, a directory will contain your web files.

DNS (Domain Name System): The component of the Internet which acts as a “phone book,” converting human-readable domain names (such as www.example.com) into computer-readable IP addresses (such as 208.77.188.166, in the case of example.com).

Domain: The name you give your website, which will appear in your website’s URL and email addresses. Usually seen as example.com, where "example" is meant for your domain’s name.

DSA (Digital Signature Algorithm): A method of generating public and private keys for encrypting data. This algorithm was developed by the U.S. government.

Entropy Banner Manager: A script, included with cPanel, that lets you manage rotating banner images on your website

.

Entropy Search: A script, included with cPanel, that creates a search engine for your website.

Error Pages: These pages display warning messages when visitors encounter problems while trying to access your site. cPanel lets you configure the error messages that display for your site. For an in-depth look at HTTP error codes, please visit our HTTP error codes documentation

.

Filter: In cPanel, a tool that processes mail according to your preferences. For example, a filter can automatically discard spam or save mail from a specified sender to its own folder. In cPanel, filters can be applied to the main email account on a domain (*Account Level Filters*), or customized for each individual account (*User Level Filters*).

Forwarder: A tool that lets you forward a copy of every email message you receive to another address. When a forwarder is set up, you will still receive mail at the original recipient address. If, however, you create a forwarder without first creating the original address, messages will be forwarded to the end address without being sent to the original address, as it does not exist.

FrontPage®: A Microsoft® application that allows you to edit your web page in WYSIWYG (what-you-see-is-what-you-get) format, rather than using HTML code. cPanel provides FrontPage extensions, so you can publish your site using FrontPage, allowing you to skip the FTP process. Newer versions of FrontPage allow you to publish your site using FTP or WebDAV. See the FrontPage User Manual for more information about publishing.

FTP (File Transfer Protocol): A method of transferring files from one computer to another. cPanel comes equipped with an FTP server that can be configured to your preference. An FTP client must be installed on your computer in order to send files to and receive files from the FTP server. Some FTP clients include FileZilla (for Windows®, Linux, and Unix), and Cyberduck (for Mac®).

FQDN (Fully Qualified Domain Name): A name that uniquely defines a domain's location. It is usually seen as host.example.com. with a trailing dot. For the purposes of cPanel, including a final dot is not necessary, but the domain name must contain at least 2 dots.

GnuPG (GNU Privacy Guard): Free encryption software that lets you generate a matching public and private key. These keys are useful for keeping files private during transfer.

gzip: A program which compresses files for quick transfer. The compressed files use the filename extension .gz.

Home Directory: Your cPanel account's highest-level directory, which contains all the files and directories used by websites managed through your account. Files placed in your home directory are not viewable online unless they reside in the public_html directory or a subdirectory of public_html.

HotLink: Also known as an "inline link." A hotlink is a direct link that embeds a file (such as an image or video) from your site into another website. When another site embeds your files, it is using your bandwidth to serve those files.

.htaccess: A file that resides in a specific directory, and contains configuration information applying to all the information in that directory. The .htaccess file may also contain authentication instructions.

HTML (Hypertext Markup Language): The language in which most pages on the World Wide Web are written.

.htpasswd: A file that resides in a specific directory, along with an .htaccess file. The .htpasswd file contains encrypted password information when authentication has been set up for the directory.

HTTP (Hypertext Transfer Protocol): The method (protocol) for transferring data over the Internet.

IMAP (Internet Message Access Protocol): Along with POP3, one of the two most widely used email transfer methods. IMAP synchronizes email account information with the mail server on a

regular basis. If you log in to multiple computers to check your email, IMAP will allow you to see what messages you have viewed, replied to, forwarded, etc. POP3 does not allow you to see this information.

Index Page: The page viewed by default when a visitor accesses a directory of your website. If no index page exists for the specified directory, the visitor will see a list of files in that directory, unless you turn off indexing in cPanel. This page is typically index.html, index.htm or index.php.

IP (Internet Protocol) Address: A number that identifies a computer on a network, making it possible for other computers to find and communicate with it.

Java: A computer programming language used by many web applications. cPanel uses the Java language to provide the SShTerm and Java Telnet features. These small applications, which run within the context of a web browser, are called applets

Key: In cryptography, a key is used to encrypt or decrypt information. Keys are an important part of encryption and security and should be guarded appropriately.

Leech: A visitor who uses another person's password to access a restricted area of a website. cPanel allows you to prevent leeching by redirecting likely offenders or disabling accounts whose passwords have been compromised.

Legacy: A term for an old software program or computer system that is still in use.

Local Host: An easy way to refer to the computer that you are currently working on.

Log: A file, automatically created by the server, that records activities performed by or on the server. For instance, error logs are lists of errors that visitors have encountered on your site.

Mailing List: A list of email addresses which list members can use to communicate. Alternatively, such a list can be used to send email messages to a large group of people. cPanel uses a program called Mailman for mailing list software; for more information, please see its website, <http://www.list.org>.

MIME (Multipurpose Internet Mail Extensions) Type: Now called an Internet media type, this component of a file identifies the file type, so that web browsers know how to handle it. cPanel lets you specify which application should be used to open files with a given extension.

MX (Mail eXchanger) Entry: A record that specifies where email should be sent for a domain. If you are using an email scanning service or custom mail delivery, you may need to change the MX record for your domain.

MySQL: This term refers to a database management tool, as well as the type of database it manages. Such databases are integral to applications like bulletin boards and retail shopping. cPanel provides an integrated MySQL interface as well as a MySQL database editing tool called phpMyAdmin.

Nameserver: A computer that contains a list of domain names and their corresponding IP addresses. These computers are spread through the Internet and allow you to find where a domain is located. Nameservers gather data about domains over time; therefore, changes to DNS records can take up to a week to reach all the nameservers on the Internet (or “propagate”).

Parked Domain: A second domain that points to your primary domain. When users attempt to access the parked domain, they will see your main website. For example, both <http://www.cpanel.net> and <http://www.cpanel.com> go to the same place, as [cpanel.com](http://www.cpanel.com) is a parked domain for [cpanel.net](http://www.cpanel.net).

PEAR (PHP Extension and Application Repository): A repository of PHP code. cPanel allows you to search for and install PEAR packages consisting of PHP programs which can perform useful functions for your website.

Perl: Known for its ability to process text, Perl is a useful language for web applications. Perl applications are commonly found as .pl, .pm, and .cgi files and may require Perl modules. Perl modules can be installed within cPanel.

Perl Module: A piece of software written in the Perl language. Modules are common pieces of software that are reused often. For example, rather than writing a set of functions to display calendars, you can simply use a calendar module.

PHP: A computer scripting language in which many web-based applications are written. PHP applications are commonly found with the filename extensions .php, .php4, or .php5. Some PHP applications require PEAR packages, which can be installed in cPanel through the PHP PEAR Packages feature.

PHP Package: A piece of software written in the PHP language.

phpMyAdmin: A graphical application that allows you to manipulate and manage MySQL databases over the Internet. Full documentation for phpMyAdmin can be found at its creators' website: <http://www.phpmyadmin.net>.

POP3 (Post Office Protocol version 3): Along with IMAP, one of the two most widely used email transfer methods. POP3 simply copies every message in your email account to your local computer. No information is sent back to your email account about message replies, forwarding, etc. If you use multiple computers to check your email, it is advised that you use IMAP instead of POP3

POSIX (Portable Operating System Interface): A standardized collection of commands for the Unix operating system.

Private Key: A string of characters that a computer uses to encode or decode encrypted messages it receives. Encryption schemes use a matching pair of keys (one public, one private) to create a secret code so that anyone looking at messages sent from or received by your computer will be unable to determine the contents of those messages without access to the private key. A private key is integral to protecting your confidential information and should be safeguarded appropriately.

Proxy: In computing, a computer or program that serves as an intermediary between two other entities. For instance, a proxy server receives a request from a client, finds the requested resource, and returns it to the client. You can use the cPanel Proxy to access to your cPanel interface when normal access is blocked (for example, from behind a firewall).

Public Key: A string of characters that a computer uses to encode or decode encrypted messages it receives. A public key is provided to anyone you wish to send sensitive information to. Typically, a public key will be placed on a server so you can access that server with encryption.

public_ftp: The subdirectory, located inside your home directory, that holds files available for public download. This is the default directory users will access when they connect to your site via anonymous FTP.

public_html: The subdirectory, located inside your home directory, that holds the files that make up your website. The www directory is a link to public_html. Any files and folders inside of public_html are visible over the Internet, unless you specifically protect them with password protection or using a .htaccess file.

Redirect: A feature that allows you to send visitors who try to access one URL to another URL. cPanel allows you to set up either temporary or permanent redirects. Redirects are useful when you change the URL of a page on your website. You can put up a redirect at the old URL to make sure your visitors are automatically sent to the new URL.

Referer: A web page which links to your site; also called an “HTTP referer.” This spelling is the industry standard term, though it is based on a misspelling of “referrer.”

Root: Specific to Unix and Unix-based systems, a computer account, used by a system administrator, which carries full privileges for configuring a computer system. Also called “superuser.”

RSA: An algorithm for generating public and private keys when sending encrypted data between a local machine and a remote machine. The name of this method is not an abbreviation; it is named after its three inventors.

SCP (Secure Copy Protocol): A method of transferring encrypted files from one computer to another. This method prevents data from being intercepted and read.

Shell: Software that allows you to interact with a computer. Many Unix shells allow you to type commands, and are often referred to as CLIs, or command line interfaces.

Shortcut: A link to an application which allows you to access it from a convenient location, like your computer’s desktop.

Spam: Chiefly, unsolicited email sent in bulk, usually by an automated system. As spam is considered a costly nuisance to the recipient, cPanel includes features like SpamAssassin and BoxTrapper that can cut down on the amount of spam received.

SpamAssassin: An application which can filter suspected spam before you receive it. SpamAssassin can be configured to filter spam more or less aggressively, according to your needs. Learn more about SpamAssassin at its website: <http://spamassassin.apache.org/>.

SPF (Sender Policy Framework): A feature that allows a recipient server to verify that an email message has really been sent from the domain specified in the *From:* field. Enabling SPF can prevent your server from receiving replies to spam that has forged your domain name as part of the sender’s address. SPF only works if both the sending and receiving mail servers have SPF enabled.

Spoofing: In email, this term is used to describe the forgery of a domain name as the sender in the header of an email. Enabling SPF makes it more difficult for spammers to spoof your domain.

SSH (Secure Shell Handler): A network protocol that allows a user to log into a remote machine user account securely. cPanel can create keys for authenticating your identity during SSH login, and provides a Java applet for accessing SSH through your web browser.

SSL Certificate: An electronic document (using the filename extension .crt) which binds a public key to an identity consisting of an email address, company, and location. This electronic document is a key piece in an authentication process.

SSL (Secure Sockets Layer)/TLS (Transport Layer Security): TLS is simply the more recent version of SSL. Both are cryptographic schemes that allow for secure interaction between a web browser and a web server. All sensitive data (credit card numbers, login information, etc) that is transmitted over the internet should be protected by SSL/TLS. You can install an SSL certificate on your web site to allow your site to be protected by SSL/TLS.

Subdomain: A subsection of your website that exists as a subdirectory in your home folder. If your domain were example.com, then the subdomain URL would appear as subdomain.example.com.

Tar: Originally derived from "Tape Archive," a program that collates files for transfer or distribution. Files processed by this program are usually compressed, commonly called "tarballs," and use the filename extension .tar. Due to the compression commonly used, .tar often precedes the .gz file extension.

Tarball: A file collated by the tar program, and usually compressed.

Telnet: A network protocol that allows a user to log into a remote machine user account remotely. Telnet is similar to SSH, but less secure. Telnet should not be used to connect to your web site except for testing purposes. Login information is sent through Telnet as plain text and can be easily intercepted.

Thumbnail: A version of an image file that is reduced in size, allowing for easy viewing of multiple images. cPanel includes a Thumbnailer tool as part of its Image Manager section.

Thumbnailer: A cPanel tool that automatically sizes down all the images in a directory. The new thumbnails are stored in a subdirectory named */Thumbnails, where * is meant to represent the parent directory containing the original images.

URI (Universal Resource Identifier): On the web, a URI is a string of characters that identifies a website. URI is often used synonymously with the terms “URL” and “web address,” although there are technical differences among the three.

URL (Universal Resource Locator): On the web, a URL is a string of characters that identifies the location of a website. Since IP addresses are difficult to remember, URLs are used instead. For example, it is much easier to remember to go to <http://www.example.com> than <http://208.77.188.166>. URL is often used synonymously with the terms “URI” and “web address,” although there are technical differences among the 3.

User: A person who uses a computer to accomplish some purpose.

Visitor: A person who views your website.

Web Browser: An application used to view and interact with sites and pages on the World Wide Web. Examples include Firefox®, Internet Explorer®, and Safari®.

Web Disk: A feature of cPanel that lets you manipulate your web files by dragging and dropping, just as you do on your local computer’s operating system.

Web Root: The top-most directory of your website (namely, `public_html` or `www`), inside which all of the files and subdirectories for your website reside.

Web Server: A program, such as Apache, which receives requests from clients (web browsers), retrieves the requested web pages, and “serves” them to the clients.

Webalizer, The: A program that displays various statistics for your website using tables and graphs. Full documentation for The Webalizer can be found at its creators’ website:
<http://www.webalizer.com>.

Webmail: Any application which allows you to access your email through a web browser. The main advantage to webmail is the ability to access your email account from any computer connected to the Internet without having to install or configure a specific mail program.