
KnowledgeBuilder

All Articles in All Categories

Contents

<i>Directory Indexes</i>	1
<i>Guard Signups</i>	1
<i>Installing SSL's</i>	2
<i>PHP versions - finding out what your site is using and how to switch versions</i>	4
<i>Redirect URL</i>	4
<i>Reverse DNS and email</i>	6
<i>Spam Setting Options</i>	6
Common Reseller Questions	7
<i>Advanced (ish) SPF</i>	7
<i>AntiSpam Protection</i>	8
<i>Basic SPF</i>	11
<i>Customer wants mail to go to their Exchange Server</i>	12
<i>Directory Indexes</i>	13
<i>Guard Signups</i>	14
<i>HORDE - Unable to Retrieve Email Quota</i>	15
<i>How can I protect a folder on my site?</i>	15
<i>How do I add a domain without creating a Control Panel login?</i>	16
<i>How do I create a Control Panel for my customers?</i>	16
<i>How to setup WorldPay to tell the control panel it has received a payment</i>	16
<i>How To View Billing Statements</i>	17
<i>New Instant Alias not working</i>	17
<i>Quick guide on how to set-up your Reseller Account</i>	18
<i>Redirect URL</i>	18
<i>What is the difference between Disk Quota and Summary Disk Quota?</i>	20
<i>What is the path to Perl/Sendmail?</i>	20
Control Panel Branding	20
<i>Brand your CP with your own images/logos</i>	20
<i>How to change your Reseller URL</i>	20
<i>How to create a custom CP log-in form</i>	21
<i>How To View Billing Statements</i>	21
Email	22
<i>Reverse DNS and email</i>	22
<i>Spam Setting Options</i>	22
Using the support system	22
<i>Setting ticket priorities and expected response times</i>	22
<i>Support procedure for resellers</i>	24

Directory Indexes

Scenario:

When the client wants to set up their own index pages enabling clients to tell their visitors' browsers which page to load as they hit their domain. Usually, it's /index.html by default, but you can set any other custom welcome page.

Example: If a visitor goes to your site <http://www.example.com>, the first page to open will be <http://www.example.com/index.html>. However, if you set /welcome.html as the directory index, the page to open will be <http://www.example.com/welcome.html>.

Solution:

To set your custom directory indexes, do the following:

Select Quick Access in the Account menu.
Click the Web Options icon on the page that shows.
Click the Edit icon next to the domain you need.
On the Web Service page, scroll down to find the Directory Indexes option and turn it on.
Agree with the charges.
In the box that appears, enter the names for files that will be treated as indexes. Put file names in the descending order of priority and separate them with spaces (e.g. index.html cgi.bin about.html).

Skip this step if you are using a Windows-based plan.
At the top of the Web Service page, click the Apply link for the Server configuration to change. The changes will take effect within 15 minutes.
To edit the list you have made, click the Edit icon next to the Directory Indexes option: with spaces (e.g. index.html cgi.bin about.html).

If you are using a Unix-based plan, click the Apply link at the top of the Web Service page.

*your custom index pages won't add to the defaults; they will replace them. Therefore, make sure to enter the full list of indexes you would like to have in your configuration.

Guard Signups

Scenario:

End user's signing up to a plan without the knowledge of the reseller.

Solution:

This tends to happen when end users signup to plans via the signup link (Which can be found within the reseller's website).

Methods to Guard Signups:

The reseller can:

Stop anybody else from signing up to the plan.
Moderate users to a plan.
Set up billing for that plan.

1. Stopping anybody else from signing up to the plan:

- A) Info >> Quick Access >> Plans
- B) Switch Off under Signup Access.

2. Defining Billing:

- A) Info >> Quick Access >> Plans
- B) Under Action – Click on the hammer (Edit) to the desired plan.
- C) At the bottom of the screen under settings – you can set prices to the resources that would be used under the plan.

3. Define Moderation.

Get to the Signup Guard interface:

- A) Info >> Quick Access
- B) Under Settings >> Signup Guard
- C) Moderate Everything (Will ask for you to verify the person that signed up to the plan)

Installing SSL's

Installing SSL's
Use the Key and Certificate You Already Have

To enable SSL, do the following:

Select Domain info in the Domain Settings menu.
Click the Edit icon in the Web Service field.
Enable SSL for the domain in the list.
On the page that appears, choose the Import SSL certificate option in the SSL Support section.
Enter the SSL Server Private Key and SSL Certificate in the boxes that appear:

In the Site Name field, choose whether you want to secure with or without the www prefix. Only one option will work correctly. For instance, if you choose to secure http://www.domain.com, your visitors will get security warnings when they go to http://domain.com.
Click Submit. Now your site is secured.

Create a Temporary Certificate

The only difference between temporary and permanent certificates is that temporary certificates are generated by your control panel, not trusted Certificate Authorities. Thus, when visitors enter your site, they will get the "unknown certification authority" warning window.

To generate a new temporary SSL private key and certificate, do the following:

Select Domain info in the Domain Settings menu.
Click the Edit icon in the Web Service field.
Enable SSL for the domain in the list.
In the SSL Support section click Import SSL certificate.
On the page that shows click Generate a temporary SSL certificate and certificate request.

On the page that appears, apply your details by clicking Submit:

These data will be used to generate the certificate. Don't make changes to the data if you are not sure about the purpose of these changes.

Follow instructions that appear at the top of the next page.

SSL Certificate Signing request includes the details that you submitted on the previous step. Use this request if you want to get a permanent SSL certificate from a trusted Certificate Authority, such as Comodo CA, Thawte or VeriSign (see below).

SSL Server Private Key is the secret key to decrypt messages from your visitors. It must be stored in a secure place where it is inaccessible to others. Don't lose this key, you will need it if you get a permanent certificate.

Temporary SSL Certificate validates your identity and confirms the public key to assure the visitors that they are communicating with your server, not any other party.

Click Submit Query.

Acquire a Permanent Certificate

To get a permanent certificate, do the following:

Generate a temporary SSL certificate (see above).

Copy the certificate signing request (CSR) and private key for later use.

Go to Comodo CA or any other Certificate Authority and choose to get a new certificate. When requested, enter the signing request that you have saved.

Important: When obtaining SSL certificate, make sure it is generated for Apache regardless of whether you intend to install it on windows or Unix box.

After the permanent SSL Certificate has been generated, save it to a secure location.

Select Domain info in the Domain Settings menu.

Go to the Web Service page and click the Edit icon in the SSL field.

Enter the certificate into the upper box of the form that opens ("Install Certificate based on previously generated Certificate request"):

Enter your certificate:

Certificate Authority File (for Comodo - intermediate CA certificate).

Certificate Chain File (for Unix accounts only, Windows doesn't support Chain Certificates).

Click Install.

Now you can use the certificate jointly with the private key you have saved.

Use Your Provider's SSL Certificate (Shared SSL)

If your provider offers a Shared SSL certificate, you can use it instead of purchasing a certificate of your own. Unlike a regular SSL certificate, it costs less, doesn't require a dedicated IP, and belongs to an equally trusted Certificate Authority. The disadvantage of shared SSL is that it can be used only with third level domains.

Shared SSL requires that your site runs on a shared IP.

To secure your site with Shared SSL, do the following:

Select Domain info in the Domain Settings menu.

Click the Edit icon in the Web Service field.

Enable Shared SSL for the domain in the list.

Agree to charges, if any.

If you are using a second level domain (example.com), you will be asked to create a third level domain alias (e.g. domainalias.example.com):

Now the site is available both at the non-secured second level domain name (e.g.

<http://example.com>) and at the secured third level domain alias (e.g. <https://example.victor.psoft>).

Note that Shared SSL certificates work only within one domain level, i.e. for user1.example.com and not for www.user1.example.com. In the example above, the certificate will not work for www.example.victor.psoft, and your visitors will get the warning: "The name on the security

certificate does not match the name of the site".

NOTE: When designing your pages set any internal links to images or frames as `<img src= or simply <img src=. If you use the`

PHP versions - finding out what your site is using and how to switch versions

PHP versions - finding out what your site is using and how to switch versions

The major versions of PHP currently in use on our systems are 4 & 5. Minor versions (eg: 4.4.4) are updated periodically as the packages become available from our control panel vendor.

Currently, a Linux server is either set to use version 4 or version 5. To find out what version your site is using, you can create a phpinfo page which reports the version.

EXAMPLE:

(Save as info.php)

After creating this file and uploading it, browse to the URL were you placed the file, and you should see a PHP info page with the version number reported at the top.

Want to switch versions?

If you would like to use a different major version (eg: your site is using 4, and you'd like 5), then please just send a ticket to support detailing the account name you'd like to switch versions for.

NOTE: This request will cause the support team to re-locate the specified account to a different server. The account may contain multiple sites - all of them will be moved to the new server, so ALL of the them will use the chosen version of PHP. Sites within the same CP account will all use the same version of PHP.

Please also note that account moves take 24 hours to finalise (DNS changes) and if you have any sites with a dedicated SSL, then the move should be carefully planned (SSL has to be removed while the account moves and added again once the move is complete).

If you have any questions about the process, please just email support.

Redirect URL

Scenario:

If the reseller wants to redirect to another website.

Solution:

There are may ways to do this. These are:

- A) Through the CP.
- B) Through the code.

A) Through the CP:

Use this feature to redirect your visitors from one web page to another or even to a different website.

To create a redirect in a Unix-based account, do the following:

- Select Quick Access in the Account menu.
- Click the Web Options icon.

Click the Edit icon next to the domain you need.
On the Web Service page, scroll down to find the icon next to it.
Agree with the charges.
On the page that appears, create the redirect rule.

Redirect option and click the Add

Unix-based accounts

Entering `http://www.examples.com/products` into the Redirect from field and
`http://www.examples.com?param1=yes` in the to field, will take all the
`http://www.examples.com/products` visitors to the
`http://www.examples.com?param1=yes` page.

If you leave the Redirect from field empty, visitors will be redirected from any location in the site. In the to field, you can enter URLs with parameters, as illustrated in the screenshot above.

Leave Redirect status as is unless you want to change the default:

Permanent returns a permanent redirect status (301) indicating that the resource has moved permanently.

Temporary returns a temporary redirect status (302). This is the default and indicates to the client that the resource has moved temporarily.

See other returns a "See Other" status (303) indicating that the resource has been replaced.

Gone will cause a visitor's browser display "The requested resource is no longer available on this server and there is no forwarding address. Please remove all references to this resource." message when trying to go to the 'to' URL..

Windows-based accounts

In Windows plans, redirect works in a slightly different manner:

The exact URL entered above redirects requests for any files in the indicated directory to one file. For example, to redirect all requests for `products.html` file to the following URL: `'www.example.net'`, enter `www.example.net/products.html` in the To field and select this option.

You can redirect requests to URLs with parameters, for example `www.examples.net/?param1=yes`

*Note: you can redirect requests for files and directories both to your own site and to any other external URL.

A directory below this one redirects a parent directory to a child directory.

- For example, to redirect your `'examples.net/products'` directory to a subdirectory named `'news'`, enter `'example.net/products/news'` in the 'to' text box and select this option. Without this option, the Web server will continually map the parent to itself.

A permanent redirection for this resource sends the following message to the client: `'301 Permanent Redirect'`.

Redirects are considered temporary, and the client browser receives the following message: `'302 Temporary Redirect'`. Some browsers can use the `'301 Permanent`

Redirect' message as the signal to permanently change a URL, such as a bookmark.

B) Through the Code:

You can create a meta redirect by:

Above shows two parameters to set:

Content: The number of seconds to wait before the redirect takes place.

URL: The URL to redirect to.

Therefore:

Well redirect to my www.domain.com after 5 seconds. For immediate effect set the value to 0.

*Note that META tags must be withing tags.

*In order to redirect via a META tag - you can set directory indexes to open up the page that contains the META redirect as priority.

Reverse DNS and email

(Taken from AOL)

Reverse DNS is a way of associating an IP address with its domain name.

The reverse DNS identifier is contained in the PTR portion of the IP Zone File.

The IP Zone File contains all the different ways that your IP and domain name can be associated; each association serves a different need.

Altaire does require that all connecting Mail Transfer Agents have established reverse DNS, regardless of whether it matches the domain.

Reverse DNS must be in the form of a fully-qualified domain name. Reverse DNS containing in-addr.arpa are not acceptable, as these are merely placeholders for a valid PTR record. Reverse DNS consisting of IP addresses are also not acceptable, as they do not correctly establish the relationship between domain and IP address.

Reverse DNS that may be similar to dynamic IP space (containing pool, dhcp, dyn, etc.) may be treated as suspect. Therefore should be changed to reflect a fully-qualified domain name with standard MTA reverse DNS.

Spam Setting Options

Users can choose from two options "Spam check level" and "MaxScore level" to determine the level that mails would be marked as spam.

Only one can be defined for each configuration and not both at the same time.

Common Reseller Questions

Information on how to solve common issues that resellers have.

Advanced (ish) SPF

SPF - Sender Policy Framework - Advanced (well a little more advanced than basic!)

So we have set-up SPF for a 'default' domain example, now we want to move on to a situation where you are not using the default scenario (such as using exchange to send mail).

The basics are the same, the only difference is that you have to create the txt record manually!

Within the CP for the domain you want to add this for go to Domain Settings/Domain Info then click on DNS configuration (if you have more than one domain in this CP you will need to click on the relevant domain first).

Once the screen has loaded scroll to the bottom and click on Add DNS TXT Record (custom DNS records need to be enabled on the Plan for this to be available).

Once clicked it will load a new page with 3 available text fields to fill in. You can leave the first field (Name) and ignore the second (TTL) its the third (Data) that we are interested in :o)

You need to start all SPF records with v=spf1 then it becomes personal choice!

For this example we are going to say that I am going to be sending my emails from my website (example.com), occasionally by using webmail/SMTP (mail.example.com) and out via my exchange server which has an IP address of 1.2.3.4 which I have already set-up within the CP as exchange.example.com (see <http://www.logacall.com/index.php?action=kb&article=1> for how to do this) and I want to stop any body else from sending mail.

So my TXT record would be:

```
v=spf1 a:a:exchange.example.com mx -all
```

Which broken down becomes:

a - the A records for my domain (the address of where the website is for the form to send mail)

a:exchange.example.com - the A record for my exchange server

mx - the MX records for my domain (the IP address for the mail servers so I can use webmail or SMTP to send mail)

-all - stops everyone else

You can also use this if you are using your ISP's mail server to send out mail, in this case your TXT record would be something like:

```
v=spf1 a:a:mail.isp.com mx -all
```

Which as you can see has the A record for your ISP added as allowed to send mail.

In some instances you may also need to add an IP address instead of a domain name, this is also very easy you just use ip4: so to add the IP 1.2.3.4 to our SPF record it would then look like this:

```
v=spf1 a:a:exchange.example.com ip4:1.2.3.4 mx -all
```

So now we can send mail from all our A records as well as our exchange server and the IP 1.2.3.4 AND all our MX records! Sorted!

AntiSpam Protection

AntiSpam Protection

AntiSpam allows to trace, filter out and delete spam messages coming to your mailbox. The system doesn't delete messages recognized as spam. It only marks them as spam and delivers them in a regular way, which is why these messages also count against your summary traffic.

You can manage antispam protection:

- on the account level
- on the mail domain level
- on the mail resource level

To manage antispam for the entire account:

1. Select Account settings in the Account menu. The following page will show:
2. Click to add antispam resource for all mailboxes or for all mail resources (box, forward, alias, responder) in this account.
3. You can delete all antispams in this account by clicking the Trash icon.

To manage antispam at the level of maildomains:

1. Go to the Mail Info menu and select the mail domain from the drop-down box.
2. Click Go and you will see the mail service details of the chosen mail domain:
3. On the page you will be taken to, add antispam either for all mailboxes of this mail domain or for all mail resources (box, forward, alias, responder).
If necessary, you can delete all antispams under this mail domain by clicking the Trash icon.
4. Clicking the antispam icon will let you configure antispam settings for mail resources.
5. Click the Submit button at the bottom of the form.
6. On the page you will be taken to, add antispam either for all mailboxes of this mail domain or for all mail resources (box, forward, alias, responder).
If necessary, you can delete all antispams under this mail domain by clicking the Trash icon.
7. Clicking the antispam icon will let you configure antispam settings for mail resources.
8. Click the Submit button at the bottom of the form.

To configure antispam protection for a mail resource:

1. Click the e-mail address in the E-mail list on the Mail Controls page.
2. Check the AntiSpam box.
3. Click the Submit button at the bottom of the form.
4. On the Mail Controls page click the Antispam icon in the Resources included column:
5. Fill up the Antispam preferences page

Spam check level determines how aggressively spam will be filtered. Antispam filters analyze each email message as it passes through the gateway email server and score it between 1 and 14. The larger the number the more likely it is considered to be spam:

- * Very Aggressive: guarantees almost anything delivered to your mailbox will be legitimate. However you will lose a lot of email (processes messages that score over 2)
- * Aggressive: guarantees anything delivered to you will be legitimate. Still a fair chance of false positives (processes messages that score over 4)
- * Normal: might block some mailing lists messages (processes messages that score over 7)
- * Relaxed: accepts semi-legitimate bulk mail (processes messages that score over 10)
- * Permissive: accepts almost everything (processes messages that score over 14)

The default value is usually 3, but this can be changed by the hosting system administrator.

Spam processing:

Mark as spam: this will tag the email as spam, i.e. add the word SPAM to the subject line of the email and then forward the email on to the client as an attachment with details.

Remove: this will delete the spam email so when the client performs a send/recieve, they will never see the email.

Move To: this allows you to specify a mailbox spam email goes to. The client will never see this email unless they access the specified mailbox.

MaxScore level (in 2.4.3 RC 1), if not Undefined, overrides the Spam check level with an alternative score range from 20 to 500:

- * Very Aggressive - 20
- * Aggressive - 40
- * Strict - 60
- * Moderate - 80
- * Neutral - 100
- * Soft - 150
- * Permissive - 200
- * Loose - 300
- * Very Loose - 500

If a spam mail is detected on this level, it is deleted irrespective of your choice for Spam processing.

White List - sender e-mail addresses to accept

Black List - sender e-mail addresses to reject

Note: White and Black Lists have priority over the spam check level.

* you can use masks using '*' and '?'. For example: *@domain.com, ?abc@domain.com, *.domain.com

* e-mail addresses or masks should be separated by ',' or ';' or 'ENTER' or 'TAB' or 'SPACE'.

6. Click the Submit button at the bottom of the form.

Basic SPF

SPF - Sender Policy Framework.

SPF is a relatively new way of reducing the amount of spoofed mail being sent around the world. It works by adding a DNS TXT record to the domain identifying the users allowed to send mail from that domain. If the recipients mail server has SPF enabled then it checks the record and the sending server and then processes the mail according to the rules specified in the set-up.

As more and more ISP's/Mail providers are using this (including Altaire) as a way to stop spoofed mail coming into mail boxes I have written this easy (hopefully) to follow set-up guide:

To start with the following will only work if the nameservers for the domain are pointing to our servers (your hosted Name Servers) if not then you will need to modify these instructions for your own use.

For most of you using the default set-up for domains/mail then all you will need to do is switch SPF on within your plans and/or on for the individual domains this will cover you for using our servers for

sending out mail (SMTP = mail.domain.ext) as it allows automatically the A and MX records to send mail. Once switched on within the domain you will be given the following options:

SPF mechanism prefix:

Fail
Softfail
Pass
Neutral

Fail

This is the most common usage for SPF, if set here this will allow you to send mail from the A and MX records for the domain mail.domain.com and from a form on the website for example) and will FAIL all other attempts to send mail (a good thing!)

Softfail

Same as fail except that mail will still get sent but will be marked as not matching the SPF record if the mail has not been sent via the A or MX records.

Pass

Checks the mail for a record but allows anyone to send mail using your mail address (very bad)

Neutral

Doesn't care who sends or from where couldn't say either way!

We would obviously recommend that you use FAIL as this will help prevent the bad guys from spoofing your mail address.

Once submitted you will notice under DNS configuration for that domain that a TXT record has been created that will look something like:

```
v=spf1 a mx -all
```

This means that you are using spf version 1 and that the A and MX records for the domain are allowed to send but everyone else is not.

Simple :o)

Now if you are not using the 'default' settings (you are using an exchange server for example for mail) then you will need to create your SPF record manually! I will explain this in the KB article Advanced SPF <http://www.logacall.co.uk/index.php?action=kb&article=19>

Customer wants mail to go to their Exchange Server

Scenario:

Customer no longer wants mail to go to the shared mail servers but would like it redirected directly to his exchange server.

Solution:

Firstly you need the static IP address of your customers Exchange server, once you have this login to that customers CP.

Once logged in go to Domain Settings / Domain Info - If applicable select the domain you want to edit then select DNS configuration.

In the DNS config screen click on the link "Add DNS A record" (if this option is not available then you will need to edit the plan the user is on and enable "Custom DNS Record").

On the screen that is loaded enter a relevant name (exchange is always good to use!) and in the Data field add the customers IP address then press submit.

Once submitted you will return to the DNS config page where you will see the A record that you have just added, from here click on the "Add DNS MX record" link

On the screen that is loaded leave the name field blank, in the first Data field add a priority* and in

the second, larger, Data field add the name of the previously created A record (so if you called the record exchange then you will put exchange.domain.com) then submit.

Once submitted you will return to the DNS config page where you will see the MX record that you have just added, once this has been done then your customer will start to receive mail direct to there mail server.

*priority is a number set to determine where mail goes to and in what order, lowest number first. Default for our mail servers is 10. If your customers require a backup so that if they have a problem with there exchange server then mail is picked up by our servers then we would reccomend that you set the priority of the nw record to 5 this way if a failure occurs mail will still be collected, the customer will need to use a POP3 downloader on there exchange server to pickup the missed mail. If the customer doesnot require any failover then you can remove the default MX records and set the priority to the default of 10.

*You can’t add MX records directly by referencing an IP address as MX records can’t contain IP addresses within their DNS entries. In order to add the custom mail record we would need to add an A record to the DNS. From this A record we would then reference the MX record.

Example:

Prerequisites:

A) Our custom mail server is on the IP address: 123.456.789.101 and this is our exchange server.

B) The domain name is mydomain.com

1) First add an A record:

Our A record would need to point to 123.456.789.101 with the alias. Therefore we will call the alias: exch.mydomain.com to point to 123.456.789.101.

DNS A records are added by clicking on the “Add DNS A Record” Link.

2) Then add the MX record:

Our MX record will be referenced as mydomain.com. Therefore we would add the MX record as: mydomain.com to point to exch.mydomain.com.

DNS MX records are added by clicking on the “Add DNS MX Record” Link.

DNS configuration Zone: mydomain.com

Name	TTL	Class	Type
Data			
mydomain.com	86400	Built in A records	
Address]		IN	A [IP
*mydomain.com	86400	IN	A [IP
Address]			
Restore default A records			
Custom A Record			
exch.mydomain.com	86400	IN	A
123.456.789.101			
Add DNS A Record			
Built in MX records			
mydomain.com	86400	IN	MX 10 mail.mydomain.com
Restore default MX records			
Custom MX records			
mydomain.com	86400	IN	MX 1
exch.mydomain.com			
Add DNS MX Record			

Built in CNAME records

Restore default CNAME records

Built in TXT records

Restore default TXT records

Directory Indexes

Scenario:

When the client wants to set up their own index pages enabling clients to tell their visitors' browsers which page to load as they hit their domain. Usually, it's /index.html by default, but you can set any other custom welcome page.

Example: If a visitor goes to your site <http://www.example.com>, the first page to open will be <http://www.example.com/index.html>. However, if you set /welcome.html as the directory index, the page to open will be <http://www.example.com/welcome.html>.

Solution:

To set your custom directory indexes, do the following:

Select Quick Access in the Account menu.
Click the Web Options icon on the page that shows.
Click the Edit icon next to the domain you need.
On the Web Service page, scroll down to find the Directory Indexes option and turn it on.
Agree with the charges.
In the box that appears, enter the names for files that will be treated as indexes.
Put file names in the descending order of priority and separate them with spaces (e.g. index.html cgi.bin about.html).

Skip this step if you are using a Windows-based plan.
At the top of the Web Service page, click the Apply link for the Server configuration to change. The changes will take effect within 15 minutes.
To edit the list you have made, click the Edit icon next to the Directory Indexes option: with spaces (e.g. index.html cgi.bin about.html).

If you are using a Unix-based plan, click the Apply link at the top of the Web Service page.

*your custom index pages won't add to the defaults; they will replace them. Therefore, make sure to enter the full list of indexes you would like to have in your configuration.

Guard Signups

Scenario:

End user's signing up to a plan without the knowledge of the reseller.

Solution:

This tends to happen when end users signup to plans via the signup link (Which can be found within the reseller's website).

Methods to Guard Signups:

The reseller can:

- Stop anybody else from signing up to the plan.
- Moderate users to a plan.
- Set up billing for that plan.

1. Stopping anybody else from signing up to the plan:

- A) Info >> Quick Access >> Plans
- B) Switch Off under Signup Access.

2. Defining Billing:

- A) Info >> Quick Access >> Plans
- B) Under Action – Click on the hammer (Edit) to the desired plan.
- C) At the bottom of the screen under settings – you can set prices to the resources that would be used under the plan.

3. Define Moderation.

Get to the Signup Guard interface:

- A) Info >> Quick Access
- B) Under Settings >> Signup Guard
- C) Moderate Everything (Will ask for you to verify the person that signed up to the plan)

HORDE - Unable to Retrieve Email Quota

Scenario

When logging into Horde and you get the message: "Unable to Retrieve Quota" and you can't view any emails.

Solution.

This error is caused by Email headers not being generated properly from by a sender (Normal caused by spam) . To fix this problem:

- 1) In the Horde inbox, click on Options.
- 2) Click on Display Options (Under Other Options in the User Options page).
- 3) Change "Default sorting criteria:" to arrival time.

How can I protect a folder on my site?

Scenario:

You want a folder protected so that you have to log in to view the contents.

Solution:

You can protect a folder by doing the following:

- Login to Webshell (File Manager) from within the CP
- Click the protect button at the bottom of the screen.
- From this pop-up box, browse to the folder you want to protect (by clicking folder names) and select it by clicking the folder icon on the left hand side (next to the folder you want), this should start the protect wizard within the pop-up box.
- Follow the wizard to protect that folder.

To remove the protection

- Login to Webshell (File Manager) from within the CP
- Make sure the Webshell is set to show hidden files
- remove/delete the password control file from the protected folder (usually called .htaccess or such other name you have chosen at creation time)

To Remove the Protection:

- 1) In webshell over in the right hand corner you'll see "SETTINGS" click the box and check the "SHOW HIDDEN FILES" and then click apply to enable this.
- 2) To removed the protection you need to go to the location of the folder you have protected. To do

this click on the domain name that the folder is in and keep clicking until you reach that location. You should see a file in that folder called .htaccess. Put a check mark in the box to the right of that and select "delete" at the top of the webshell program. This will remove the protection from that location.

NOTE: Please remember to reset the hidden files so they do not display by going to SETTINGS > Uncheck hidden files and apply the settings.

How do I add a domain without creating a Control Panel login?

Scenario:

You want to add a customers domain but you don't want them to have any control over it.

Solution:

Within your hosting domain CP go to Domain Settings/Domain Info then click the "Add new domain" link then add the domain in the relevant field. Once submitted you will now have that domain under this CP. You can now add mail boxes for that domain and upload the site via ftp.

NOTE: If you wish the user to manage their own domain (FTP create email addresses etc) then they will need to have their own CP login.

How do I create a Control Panel for my customers?

Scenario:

You have a customer that wants to be hosted by you and wants to be able to manage his domain(s) himself, upload his own site and create his own mailboxes etc.

Solution:

You need to create a user plan and then sign the customer up to it. This will give the customer a CP of his own which you can then bill automatically and he can log-in to and manage his own domain(s). For more information on plan creation please see the KB article

How to setup WorldPay to tell the control panel it has received a payment

Scenario:

Customers are paying via worldpay but the control panel isn't notified of the payment being made

Solution:

Log into your WorldPay account and in your account setup you will see a 'callback' URL box.

Enter: `http://[YOURBRANDEDCPURL]/psoft/servlet/psoft.hsphere.WorldPay.payment` into this box replacing [YOURBRANDEDCPURL] with the URL you use for your customers eg:

`http://cp.altaire.co.uk/psoft/servlet/psoft.hsphere.WorldPay.payment`

Now when the CP emails invoices to your clients with WorldPay links for payment, WorldPay will send this data back to the CP.

Accounts will automatically be updated with payment information which can then trigger automatic account creation (new signups), monthly payments (to save having to check for WP payments before suspending users) etc.

If you use this feature in conjunction with the CP chasing bad debtors for you, you will have a fully automated hosting business!

For those of you who don't know, the CP can chase bad debtors sending several warnings (which you can customise), and then threaten/or actually suspend the debtors web sites until they make payment. Once suspended the user can only log into their CP to view/pay invoices and once paid, the CP automatically resumes the web site. You can turn on/off auto suspend if you wish and if they simply will not pay you can also automate account deletion. The client is kept informed of all

actions by email.

For further details click 'settings/managing debtors' in your reseller control panel.

How To View Billing Statements

To see your charges by billing profiles for one account, select Billing Statement in the Billing menu. Balance shows how much money you have on your balance. A negative balance shows how much you owe for the services used. This is usually appropriate for users who pay by check and for credit card users whose credit cards failed to be charged.

Credit restricts your ability to buy new resources in case your credit card fails to be charged or you have run out of your 'check' money.

Description: the name of your current account.

Amount: the amount accrued for the billing period. This amount consists of accruals for all resources, including the setup, recurrent and usage fee. However, it does not include or depend on factual charges, nor is it related to debits and credits to the account. For example, if you were accrued £10 setup fee, the Amount will show £10.00, even if your credit card has been immediately credited by this amount.

From: the beginning of the payment period.

To: the end of the payment period. In the example illustrated above, Opened means that the billing period has not finished.

A new bill is created for every new payment interval. The initial setup fee is put in a separate bill. To view details of any bill in the invoice, click its Description in the first column

Total shows the amount due for factual services offered. It does not include most of the items highlighted by yellow, such as items that were immediately charged off the credit card, credits or debits to the account balance by the administrator, etc.

*To get a printable version of your bill, click the Printer icon in the bill header which will open it in a separate window suitable for immediate printout (version 2.08 and higher).

New Instant Alias not working

Scenario:

You've just added a site, and want to check the content using the site instant alias. When you go to the instant alias, you get the default web utilities page.

This has recently happened to a couple of resellers, so here's what to do if it happens to you! You need to be logged into your administrative account to start.

Solution:

Firstly, this normally happens when we have added a new server, for which the you (the reseller) has not yet submitted an alias (so that a DNS record is created for the server, eg: web77.yourreselleraccount.com). This can be added by going to Enterprise Manager->Server aliases. On this screen, you'll see all the servers available to your account, and you may see that some have not been submitted (still show the dropdown). Submit here to add all outstanding servers (you may get errors for older servers, ignore these).

The process above should also create a server Instant alias for each server you have (format is *.N.yourreselleraccount.com, eg: *.98.yourreselleraccount.com). This is a wildcard DNS record, meaning any host on this instant alias will resolve to the particular server (so, your individual site Instant Alias, eg: d404394.98.yourreselleraccount.com - found in web options section of end user CP).

To test whether the site Instant Alias is setup, ping the server your site is on (eg: web77.yourreselleraccount.com) and note the IP address. Then ping your instant alias (d404394.98.yourreselleraccount.com) - this should return the same IP. If it does not, you can force the system to update the server instant aliases:

To do this, go to Enterprise Manager->DNS Manager, then click 'edit' on the right next to your branded domain. At the top of the page you will see an area titled 'Instant aliases for DNS zone...'. Click 'edit' on the right to edit the server Instant Aliases. On this page you'll see all the server instant aliases that have been created. It's likely that your alias (eg: 98) is not listed, and instead the server (eg: web77) will be listed at the bottom. Click the option at the bottom 'Add records to all listed logical servers' - this will create aliases for all outstanding servers.

Once this returns, you should see an entry for your server (eg: *.98...). Wait a few minutes for DNS to update then check DNS (on a site like www.dnsstuff.com) for your instant alias (eg: d404394.98.yourreselleraccount.com) - use the check DNS A record option on [dnsstuff](http://dnsstuff.com). The IP returned should now match the IP you got when pinging the server (eg: web77....).

So that's it? Well, not quite - you may have to wait for DNS to propagate to the DNS servers you are using before you can see the site using the instant alias (that's why [dnsstuff](http://dnsstuff.com) is used to check the current DNS records). This may take several hours or overnight

Quick guide on how to set-up your Reseller Account

Redirect URL

Scenario:

If the reseller wants to redirect to another website.

Solution:

There are many ways to do this. These are:

- A) Through the CP.
- B) Through the code.

A) Through the CP:

Use this feature to redirect your visitors from one web page to another or even to a different website.

To create a redirect in a Unix-based account, do the following:

- Select Quick Access in the Account menu.
- Click the Web Options icon.
- Click the Edit icon next to the domain you need.
- On the Web Service page, scroll down to find the Redirect option and click the Add icon next to it.
- Agree with the charges.
- On the page that appears, create the redirect rule.

Unix-based accounts

Entering <http://www.examples.com/products> into the Redirect from field and <http://www.examples.com?param1=yes> in the to field, will take all the visitors to the <http://www.examples.com/products> page.

If you leave the Redirect from field empty, visitors will be redirected from any location

in the site. In the to field, you can enter URLs with parameters, as illustrated in the screenshot above.

Leave Redirect status as is unless you want to change the default:

Permanent returns a permanent redirect status (301) indicating that the resource has moved permanently.

Temporary returns a temporary redirect status (302). This is the default and indicates to the client that the resource has moved temporarily.

See other returns a "See Other" status (303) indicating that the resource has been replaced.

Gone will cause a visitor's browser display "The requested resource is no longer available on this server and there is no forwarding address. Please remove all references to this resource." message when trying to go to the 'to' URL..

Windows-based accounts

In Windows plans, redirect works in a slightly different manner:

The exact URL entered above redirects requests for any files in the indicated directory to one file. For example, to redirect all requests for products.html file to the following URL: 'www.example.net', enter www.example.net/products.html in the To field and select this option.

You can redirect requests to URLs with parameters, for example www.examples.net/?param1=yes

*Note: you can redirect requests for files and directories both to your own site and to any other external URL.

A directory below this one redirects a parent directory to a child directory.

- For example, to redirect your 'examples.net/products' directory to a subdirectory named 'news', enter 'example.net/products/news' in the 'to' text box and select this option. Without this option, the Web server will continually map the parent to itself.

A permanent redirection for this resource sends the following message to the client: '301 Permanent Redirect'.

Redirects are considered temporary, and the client browser receives the following message: '302 Temporary Redirect'. Some browsers can use the '301 Permanent Redirect' message as the signal to permanently change a URL, such as a bookmark.

B) Through the Code:

You can create a meta redirect by:

Above shows two parameters to set:

Content: The number of seconds to wait before the redirect takes place.
URL: The URL to redirect to.

Therefore:

Well redirect to my www.domain.com after 5 seconds. For immediate effect set the value to 0.

*Note that META tags must be withing tags.

*In order to redirect via a META tag - you can set directory indexes to open up the page that contains the META redirect as priority.

What is the difference between Disk Quota and Summary Disk Quota?

Disk Quota controls the amount of disk space the account is given (for storing website content). There are separate quotas for disk, email and database resources. Alternatively, Summary Disk Quota can be set, which allocates a total amount for all resources together (disk, email and databases).

What is the path to Perl/Sendmail?

Perl path is: /usr/bin/perl

Sendmail path is: /usr/sbin/sendmail

Control Panel Branding

Information on how to Brand your Control Panel interface

Brand your CP with your own images/logos

Scenario:

You wish to add your own logos/colours/images to the CP

Solution:

Login to your Admin Account, go to Look and Feel / Corporate Logo - here you can add links to your company logo/signup image logo and login image logo from here you can also add HTML code that will display in the top banner, ideal for messages to your customers.

If you wish to customise all the images and banners you can (within reason), to do this you first need to download the images directory (in the dowload section) and then upload to a directory within your domain and unzip, the folder MUST be called IMAGES (in caps) for it to work correctly! Then within your Admin Account go to Look and Feel / Design Settings then click the Change button next to Base Image directory or URL, in the screen that loads put in the URL to the directory ABOVE the unzipped image directory (for example if you uploaded to <http://www.yourdomain.com/hsphere/IMAGES> then put the URL <http://www.yourdomain.com/hsphere/> then make changes to the relevant images **WARNING** when making changes to images ensure that you make all replacement images the same size and name as the ones you are changing otherwise you will have a LOT of problems! If you make a mistake or your images do not show then clear the URL field and submit then you will be using the shared images again.

How to change your Reseller URL

Scenario:

Customers see "altaire" in the CP URL

Solution:

Login to your Top Level reseller account (<http://www.altaire.com/login>)
From the info menu click "Change URL"
You will see a URL similar to: r95.res.altaire.co.uk
Replace this with cp.yourdomain.ext (this domain MUST be the domain you have set-up as your reseller domain, the one you use for your DNS etc)
Click 'Change'

Your customers can now login at the branded URL cp.yourdomain.ext

How to create a custom CP log-in form

Scenario:

You wish to have a login form to the CP from your own homepage

Solution:

Insert the following code into any web page of your site:

Log into your hosting account:

Username:

Password:

Replace REPLACE_WITH_CP_LOGIN with your control panel URL for example
<http://cp.altaire.co.uk/psoft/servlet/psoft.hsphere.CP>

How To View Billing Statements

To see your charges by billing profiles for one account, select Billing Statement in the Billing menu. Balance shows how much money you have on your balance. A negative balance shows how much you owe for the services used. This is usually appropriate for users who pay by check and for credit card users whose credit cards failed to be charged.

Credit restricts your ability to buy new resources in case your credit card fails to be charged or you have run out of your 'check' money.

Description: the name of your current account.

Amount: the amount accrued for the billing period. This amount consists of accruals for all resources, including the setup, recurrent and usage fee. However, it does not include or depend on factual charges, nor is it related to debits and credits to the account. For example, if you were accrued £10 setup fee, the Amount will show £10.00, even if your credit card has been immediately credited by this amount.

From: the beginning of the payment period.

To: the end of the payment period. In the example illustrated above, Opened means that the billing period has not finished.

A new bill is created for every new payment interval. The initial setup fee is put in a separate bill. To view details of any bill in the invoice, click its Description in the first column

Total shows the amount due for factual services offered. It does not include most of the items highlighted by yellow, such as items that were immediately charged off the credit card, credits or debits to the account balance by the administrator, etc.

*To get a printable version of your bill, click the Printer icon in the bill header which will open it in a separate window suitable for immediate printout (version 2.08 and higher).

Email

Email settings, bounce messages etc

Reverse DNS and email

(Taken from AOL)

Reverse DNS is a way of associating an IP address with its domain name.

The reverse DNS identifier is contained in the PTR portion of the IP Zone File.

The IP Zone File contains all the different ways that your IP and domain name can be associated; each association serves a different need.

Altaire does require that all connecting Mail Transfer Agents have established reverse DNS, regardless of whether it matches the domain.

Reverse DNS must be in the form of a fully-qualified domain name. Reverse DNS containing in-addr.arpa are not acceptable, as these are merely placeholders for a valid PTR record. Reverse DNS consisting of IP addresses are also not acceptable, as they do not correctly establish the relationship between domain and IP address.

Reverse DNS that may be similar to dynamic IP space (containing pool, dhcp, dyn, etc.) may be treated as suspect. Therefore should be changed to reflect a fully-qualified domain name with standard MTA reverse DNS.

Spam Setting Options

Users can choose from two options "Spam check level" and "MaxScore level" to determine the level that mails would be marked as spam.

Only one can be defined for each configuration and not both at the same time.

Using the support system

Logging tickets☐

Setting priorities☐

Expected response times☐

Accessing knowledge base☐

Setting ticket priorities and expected response times

Setting ticket priorities and expected response times

****Please refer to the article on support procedure before creating tickets, this will help us help you****

We currently operate 4 priority levels for support tickets:

- Low
- Normal
- Urgent
- Business cannot continue

When submitting a ticket online using the support system, you may set a priority. When you submit a ticket using email you cannot set a priority.

The support team will assign a priority or change a priority once they have viewed the ticket. Please review this document before assigning priorities to your tickets and be sensible. Please avoid diluting the process by assigning urgent or higher categories to trivial issues.

Response times are targets for our team to work to as a minimum, you will often receive a reply more quickly. This structure helps us to prioritise tickets so that each request is given the appropriate visibility.

Below we will describe each priority, so that you can understand when to use them.

:LOW: TARGET RESPONSE TIME* - 5 working days

This category is for queries you have regarding configuration or functionality changes where you need our advice.

Examples: CP configuration questions/DNS configuration questions/Domain registration questions

:NORMAL: TARGET RESPONSE TIME* - 2 working days

This category should be used for common queries where you require us to take action.

Examples: CP resource creation errors/Configuration issues/Unexpected results/Cannot FTP

:URGENT: TARGET RESPONSE TIME* - 1 working day

This category is reserved for issues which are severely affecting you or your customers now, that require action from us to resolve.

Examples: A single element of the customers resources are not functioning - such as no email or website/Expired domain

:BUSINESS CANNOT CONTINUE: TARGET RESPONSE TIME* - 1 hour

This category is strictly reserved for issues that prevent you or your customers from continuing to operate.

NOTE: If you are logging a ticket with this priority outside support hours, please wait for your ticket number, then call the support line on 0871 6661166. Supply your ticket number and explain your ticket is urgent and an engineer will be contacted to investigate.

Examples: E-commerce site down

*SUPPORT HOURS: 9am - 5.30pm Monday to Friday excluding Public holidays.

Support procedure for resellers

Support procedure for resellers

This document sets out the procedure you should go through when using Altaire support services.

Support process:

Before contacting Altaire support, you must determine where the problem lies, when it occurs and your own priority for the request. Below are some guidelines for getting support from Altaire.

Pre-requisites:

To get support from Altaire you must have an active reseller account or support agreement.

You need to have an active account on support.altaire.com (requires registration).

You should have read at least the getting started guide, ideally the PDF manual.

You should be able to understand the basic concepts of websites, email and domain registration.

Who is responsible?

Altaire is responsible for:

- You/your customers website hosting (the platform provided for the website) - excluding domain registration UNLESS Altaire is the registrar
- You/your customers databases (providing they are installed on the system)
- You/your customers email (where the email is hosted on Altaire servers)
- You/your customers DNS (where the DNS servers specified for a domain belong to Altaire)

Altaire is not responsible for:

- Domain registrations where Altaire is not the registrar
- DNS records where Altaire DNS servers are not used
- Configuring any control panel settings which are available within your login
- Email sending where Altaires servers are not used
- Connection issues outside Altaires network
- Your broadband connection
- Your website functionality
- Custom configurations where no specific support contract is in place
- 3rd party software including Easyapps (provided for your use as is)
- Operating system/applications on dedicated systems where no support contract is in place
- Teaching you the basics - FTP/email etc

If Altaire is or could be responsible for all or part of the issue, prepare notes detailing the issue, these should include:

- A basic description of the issue and how it is affecting you/your customer
- When it occurred/frequency
- Conditions under which it happens
- Error messages received (bounce reports/error codes)
- Why you think it is an issue with part of the Altaire service (Tests you have performed)
- Any other investigation you have carried out
- The priority of the issue

Please do not simply forward your customers email onto us - you should investigate first and gather the above information before raising the issue with us. This will help us to solve any problems on our systems quickly without having to gather basic information from you first.

We realise that some issues are very simple from your end, eg: "I cannot see my customers website", but these still require you to do as much as possible to verify that the problem is something we can help with. For example, if you are unable to see a customers website, make sure you test the basics:

-
- have you got an internet connection (can you see other websites)?
 - is your DNS resolution working (try browsing to website you have not used today)?
 - can other people see the website (it is possible that the Altaire security systems can block a specific IP)
 - have there been any changes to the website files/settings recently (is the right index page set?)

If the above steps are followed before raising a ticket, then we can give everyone a faster turn-around!

Once you are ready to submit a request:

- Check the knowledge base articles on support.altaire.com to see if the question you have has already been answered
- Check the forum at forum.altaire.com for posts that may be useful
- Login to your account or send an email to support@altaire.com
- You should receive a confirmation email with a ticket number
- All your replies regarding this issue should be to emails from the support system (this makes sure that your issue is tracked properly and all the relevant emails are related to a single ticket number.

Please raise a new ticket for each issue you have - don't raise multiple issues in a single ticket please.

If you haven't supplied all the information the support team need, they will ask for it!