Technical information

Technical details and documentation about web hosting.

- Nameservers, DNS and CloudFlare
- Which control panel do you offer? Do you offer cPanel?
- How can I manage my website? How can I access the control panel (cPanel)?
- Do you make backups of client websites? Where do you store backups? How do I restore a backup? How long do you keep backups?
- Do you support Node.js®? Which versions of Node do you support?
- Can I use Git? Do you support version control systems?
- Can I use an SSL certificate? Can I use HTTPS? Do you support Let's Encrypt?
- Which PHP versions are supported? Which PHP extensions are installed?
- How can I change PHP settings? How can I increase the file upload limit or memory limit of PHP?
- Common issues related to Wordpress (incl. Elementor)
- Unable to connect e-mail account to Gmail with POP3. Connection timed out or connection refused in Gmail.
- How to add an additional website / domain to my hosting plan?
- My IP was blocked from accessing my website or the hosting control panel!
- Addon domains and Cloudflare - Error "This domain points to an IP address that does not use the DNS servers associated with this server"

Nameservers, DNS and CloudFlare

Nameservers respond to DNS queries for your domain, essentially telling the browser where to find your website. For web hosting, Cloudey operates 2 nameservers, one located in Germany and the other in Finland, to provide especially low latency in both Western and Eastern Europe.

If you are using your own domain for hosting (you selected "I will use my own domain" at checkout) or you would like to add an addon domain to your account, you will need to update the nameservers for your domain at the domain registrar. The domain registrar is usually where you bought the domain from.

> If you are using CloudFlare or another third party DNS provider, skip to **Using CloudFlare**. You *should not* change your nameservers in this case.

> To see an overview of the current active DNS records for your domain, use **DNSy**.

Updating the nameservers

To change the nameservers for your domain, log in to your *registrar's* control panel. The process for changing nameservers differs slightly for every registrar, but generally you should look for "Nameservers" or "DNS servers". You may need to select "I want to use my own nameservers" or a similar option.

Cloudey's nameservers are:

ns1.cloudey.net
ns2.cloudey.net

Some registrars require specifying the nameserver IPs:

ns1.cloudey.net: **159.69.29.198**
ns2.cloudey.net: **95.216.151.238**

Once you have made the necessary changes and applied them, the changes need to propagate across the world's DNS servers. **This process may take anywhere from 30 minutes to 24 hours**, depending on the registrar. If your site does not resolve correctly after updating the nameservers, it's very likely due to DNS propagation not being complete. In that case, all you can do is sit back and wait for the changes to take effect.

Once the changes have taken effect, you might see a 403 error (if you haven't added any content to your website) or your website (if you have) when visiting the domain. Don't worry about the 403 error - once you add content to your website, it will disappear! You can access your hosting control panel (cPanel) by navigating to yourdomain.com/cpanel or cpanel.yourdomain.com.

Congratulations! You are now in business!

> If you run into any issues while updating your nameservers, feel free to open a support ticket! We can't help with registrar-specific issues, but we can usually point you in the right direction.

Using CloudFlare

CloudFlare is one of the largest DNS and CDN providers in the world, offering services such as DNS, CDN, DDoS protection, edge workers, domain registration, and others. They have a compelling set of features available for free, so we recommend checking them out.

If your domain's DNS provider is CloudFlare, the process of pointing your domain towards our servers is slightly different. Since you cannot and should not change your nameservers, you will need to manually add the necessary DNS records at CloudFlare.

First, take note of the server IP your hosting account has been provisioned to. This is specified in the welcome e-mail you receive after placing your order, titled "Your Hosting Account Information for Cloudey". If you haven't received it, make sure it didn't end up in your spam folder. The server IP is listed in the e-mail under the heading **Server Information**. If you are not sure where to find the IP, please open a support ticket, and we'll help you out!

To create the records, go to CloudFlare's control panel and open the DNS tab for your domain.

You need to create the following records:

Type	Name	Record / Domain name	TTL
A	@	*server IP from welcome e-mail*	Automatic
CNAME	www	@	Automatic
MX	@	**Priority:** 0 **Destination:** @	Automatic
TXT	@	v=spf1 +a +mx +ip4:*server IP from welcome e-mail* +include:relay.mailchannels.net ~all	Automatic
CNAME	mail	@	Automatic
CNAME	ftp	@	Automatic
CNAME	cpanel	@	Automatic
CNAME	webmail	@	Automatic
CNAME	autoconfig	@	Automatic
CNAME	autodiscover	@	Automatic
CNAME	webdisk	@	Automatic

Replace *server IP from welcome e-mail* with the IP you discovered in the previous steps.

> In Cloudflare, @ signifies the root domain (e.g. example.com). This shorthand may not be supported by other DNS providers. In that case, simply use the domain name (e.g. example.com) in place of @.

Make sure to **turn off CloudFlare HTTP proxy** (change the orange cloud to grey cloud) for the records: mail, ftp, cpanel, autoconfig, autodiscover and webdisk. CloudFlare's HTTP proxy interferes with the functioning of these services.

> **To improve e-mail deliverability**, it is also strongly recommended to create DKIM records. These are unique for each domain. You can look up the value of this record from the hosting control panel (cPanel), under the Domains section: Zone Editor -> Manage (next to your domain). Find the TXT record "default._domainkey.YOURDOMAIN.COM", and create an identical one in CloudFlare with the same value as the one in Zone Editor.

> If you are encountering issues with the provisioning of SSL certificates, make sure CloudFlare's SSL setting is set to **off** for your domain or disable CloudFlare's HTTP proxy (change the orange cloud to grey cloud) for the record that is having issues with SSL.

After that's done, the changes should take effect almost immediately, but may take up to an hour in some cases.

Once the changes have taken effect, you will see a blank directory listing (if you haven't added any content to your website) or your website (if you have) when visiting the domain. You can access your hosting control panel (cPanel) by navigating to yourdomain.com/cpanel or cpanel.yourdomain.com.

Congratulations! You did it!

> **IMPORTANT:** If you create subdomains for your domain in cPanel, you need to manually add them in CloudFlare as CNAME records pointing to your root domain, similar to the *www* record. Otherwise, the subdomains will not resolve.

> If you run into any issues while setting up CloudFlare, feel free to open a support ticket! We can't help with CloudFlare-specific issues, but we can usually point you in the right direction.

Using a 3rd party DNS provider (Google DNS, Route53, etc.)

We cannot provide specific instructions for every single third party DNS provider, for obvious reasons. In general, you will need to create exactly the same records as specified in the section for using CloudFlare. **You may need to substitute the @ in the records for your top-level domain name (e.g. example.com)**, as not all DNS providers offer this shorthand. If you run into any issues setting up a 3rd party DNS provider, we recommend contacting them directly, as they can offer more specific advice about their systems.

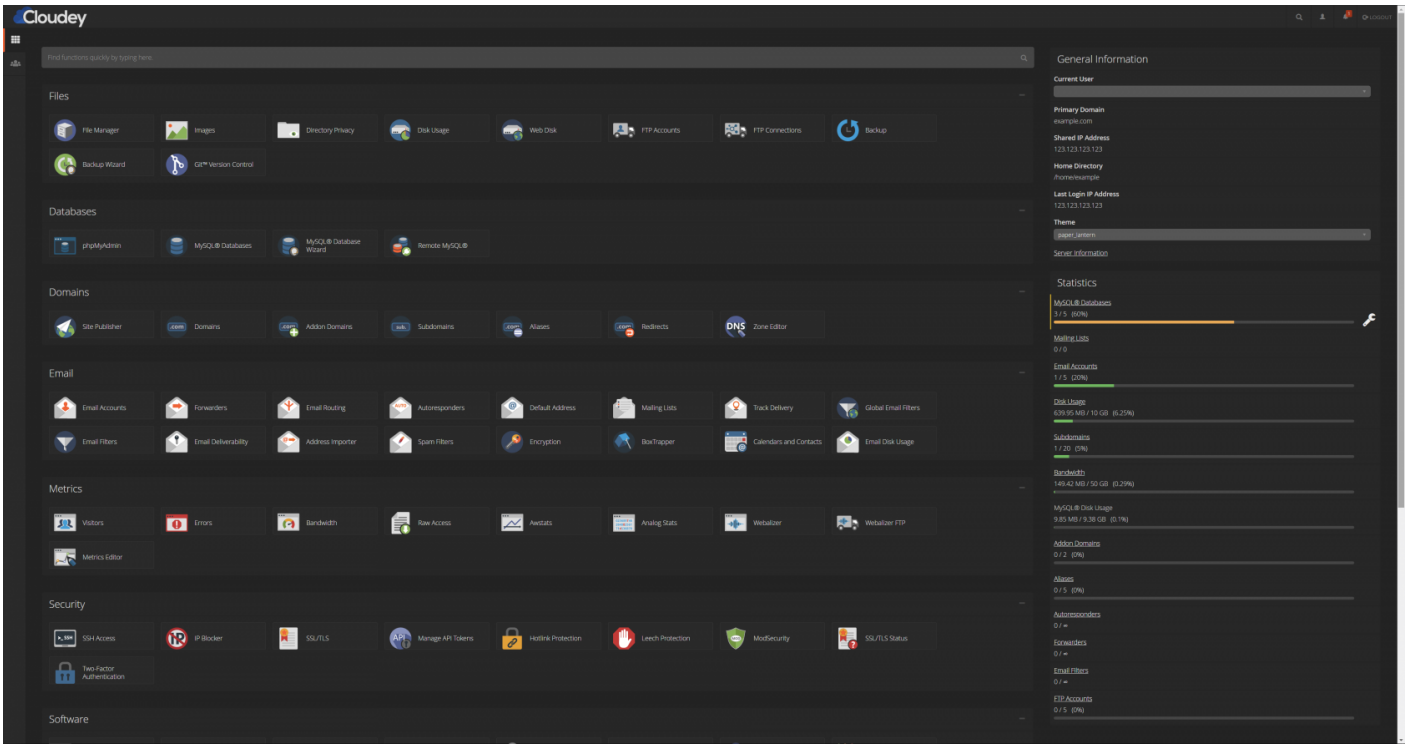
Check your DNS records

You can check your domain DNS records using our free DNS lookup tool DNSy.

Which control panel do you offer? Do you offer cPanel?

All our regular web hosting plans come with **cPanel**, the long-term industry standard web hosting control panel, which is easy to use and generally very well known.

By default, we use the standard dark theme for cPanel, with no other alterations. You can optionally use a light theme by changing it in within the control panel options.



How can I manage my website? How can I access the control panel (cPanel)?

You can access cPanel (the hosting control panel) by entering *yourdomain.com/cpanel* in your address bar, replacing *yourdomain.com* with the domain you are hosting with us. If this doesn't work, you can also access the hosting control panel by logging into our Client Portal, navigating to your service and clicking on *Login to cPanel* in the left sidebar.

In order to log in to cPanel, you need to know your hosting account username and password. **This is not the same as the e-mail and password used to log into the Client Portal**. The username and initial password were sent to you in the welcome e-mail after submitting the order, titled "Your Hosting Account Information". If you did not receive this e-mail, get in touch with us by opening a support ticket in the Client Portal.

Do you make backups of client websites? Where do you store backups? How do I restore a backup? How long do you keep backups?

Frequency and scope

We make **daily** individual backups of all accounts on our shared hosting plans. A backup includes all files, databases, e-mails, and configuration of an account. An account backup can be used to restore the entire cPanel account on our hosting service or any other hosting provider that uses cPanel. These are the backups we will focus on in this article. We also make daily backups of all system configuration of our cPanel servers, which include account data, server configuration, DNS entries, etc. which we can use to recover system configuration in the event of data loss.
As a last resort, daily backups are made of all shared hosting servers in the form of system snapshots, which we can use to quickly restore a server in its entirety, possibly on different hardware or even a different datacenter, should the entire server fail and the more granual backups prove ineffective or corrupted.

Restoring backups

In the event of a disaster, hardware of software failure, or other infrastructure problems which fall under our responsibility, we will try to restore your account as soon as possible and to the nearest available point of time. This process is automatic and does not incur any fees to you.

To restore a backup in other cases, on your own initiative or if the issue does not fall under our responsibility, you may submit a support ticket via the Client Portal.
Restoring a backup manually incurs a service fee:

- **5€** for a backup made within the **last 3 days**
- **25€ + 0.10€ per GB** for a backup made **4 or more days ago**
- **Free** for websites with any **managed** service level (Lite, Pro or Premium)

After receiving your request, we will restore your account to the specified time as soon as possible. The service fee will be invoiced to you within 14 days.

Storage and redundancy

To make *absolutely* sure we have reliable backups available in a disaster recovery scenario, we have taken extensive measures to avoid a single point of failure in terms of backup storage. The account-level backups are stored in a different geographic region from the main servers, and are periodically tested for integrity and reliability.

Retention time

We store account-level backups for 30 days. After that, all data is permanently purged and cannot be recovered. We do not keep 30 days of daily backups due to the non-viable storage requirements. To provide up to 30 days of backup availability, we store the last 3 daily backups, 2 weekly backups taken every monday, and 1 monthly backup taken on the 1st of each month.

Disclaimer

We make backups of your data as a final fail-safe measure against data loss. You should**always** keep your own backups and take other appropriate measures to protect your data. Even though we take very extensive measures to prevent this, we are not responsible for data loss due to corrupted or otherwise irrecoverable backups, unless otherwise specified in a service contract.

Do you support Node.js®? Which versions of Node do you support?

We support running and managing Javascript applications using Node.js® on all web hosting plans. To get started, simply click *Setup Node.js App* in your cPanel.

The following versions are currently supported:

- 11
- 12

New versions are added as they become available in the upstream repositories.

To make deploying and updating your Node application easier, we recommend using Git.

Can I use Git? Do you support version control systems?

We provide full integration for version control via Git through cPanel. You can set up cloning from external repositories in cPanel by clicking on *Git™ Version Control*.

Other version control systems are not currently supported.

Can I use an SSL certificate? Can I use HTTPS? Do you support Let's Encrypt?

All our web hosting plans include **free HTTPS for all domains and subdomains** on the account. This means you do not need to bring or purchase your own SSL certificate, a certificate will be issued automatically and at no extra cost. However, **you *can* use your own certificate** if you so prefer, eg. for Extended Validation.

How to setup HTTPS for your domain

Once your account has been set up and DNS for your domain has finished propagating, a certificate will be automatically issued and installed within 24 hours. You can follow this process and see currently active HTTPS hosts under *SSL/TLS Status* in cPanel.

Once the certificate has been issued, you can visit your site using the https:// protocol, and you will see a green padlock in the address bar indicating a secure connection. If you see a warning about mixed content or an insecure connection, please follow the troubleshooting steps listed further below.

Redirecting HTTP connections to HTTPS

Once you have verified that HTTPS connections to your site are working without issues, it is recommended to redirect all HTTP URLs to HTTPS, in order to provide better security by default.

The exact procedure for doing this depends on the software you are running. For many content management systems, such as Wordpress, there are plugins available which automatically configure the redirection. Make sure to also change the application URL in Wordpress (or other CMS) settings to avoid mixed content warnings.
If you are hosting a regular PHP or static application, you may need to make some simple changes to the *.htaccess* file in your web directory, for which there are plenty of tutorials available online.
When hosting a Node.js application, you may need to include the redirection logic in your application code.

> If you are not comfortable with setting up and configuring HTTPS or other aspects on your site, we offer managed hands-on support at a competitive hourly rate. Configuring HTTPS and automatic redirection usually requires no more than 20 minutes of support time.

Using your own SSL/TLS certificate

You may opt to use your own SSL/TLS certificate, purchased from a third-party vendor. Private keys, certificate signing requests (CSRs), and certificates can be managed in cPanel under *SSL/TLS*.

Let's Encrypt

Let's Encrypt is a well-known certificate authority (CA) which issues free domain validation (DV) SSL/TLS certificates. Instead of using Let's Encrypt, we issue certificates using AutoSSL powered by Comodo, which provides virtually the same service, but is integrated into cPanel.

Therefore, while we do not technically support Let's Encrypt, we still offer free certificates using an alternative provider.

Troubleshooting and common problems

My site is working fine over HTTP but accessing via HTTPS gives an error about an invalid certificate

This usually occurs when the certificate has not been issued yet, or if AutoSSL has been disabled for the domain. Check *SSL/TLS Status* in cPanel for any errors or notices. If the issue remains unsolved after 24 hours, open a support ticket in our client portal.

I am seeing errors or warnings about mixed content

This means some resources (images, videos, fonts) on your site are not using HTTPS. Make sure that all URLs on your site, including those which refer to pictures and other resources start with https://. If you are using Wordpress, make sure your application URL in Wordpress settings has been changed to include https:// at the beginning.
Also make sure all external resources used on your site are included using an HTTPS URL.

There is a comprehensive guide made by Google for finding and solving mixed content on your website.

If you are still encountering issues, or you are unsure how to proceed, consider our managed hands-on support to have us analyse any application-specific issues and resolve them for you.

When accessing my site over HTTPS, some images/fonts/videos are missing

This is usually due to mixed content being blocked. See above for possible causes.

I have questions or problems regarding HTTPS or using SSL/TLS certificates

If you have any questions regarding HTTPS or SSL/TLS certificates, feel free to open a support ticket in our client portal, and we will be happy to help you!

Which PHP versions are supported? Which PHP extensions are installed?

PHP versions

All shared hosting plans support the following PHP versions:

- **PHP 7.4** *Available until 1 Jan 2023*
- **PHP 8.0** *Available until 1 Jan 2024* - **Default**
- **PHP 8.1** *Recommended*

Support for end-of-life PHP releases will be removed 1 month after reaching end-of-life.
It is strongly recommended to always use the latest PHP version available. Newer versions contain important updates and security improvements, and also significantly help with site performance.

PHP extensions

The following PHP extensions are installed and enabled on the newest PHP version:

php-bcmath
php-bz2
php-calendar
php-cli
php-common
php-curl
php-dba
php-devel
php-enchant
php-exif
php-fileinfo
php-fpm
php-ftp
php-gd
php-gettext
php-gmp
php-iconv
php-imap
php-intl
php-ldap
php-litespeed
php-mbstring

php-mysqlnd
php-odbc
php-opcache
php-pdo
php-pgsql
php-posix
php-process
php-pspell
php-snmp
php-soap
php-sockets
php-sodium
php-tidy
php-xml
php-zip

Other details

The PHP runtime used is suphp with FPM.

How can I change PHP settings? How can I increase the file upload limit or memory limit of PHP?

Changing PHP settings

You can find various PHP settings in cPanel under MultiPHP INI Manager, located under the Software section. PHP settings can be set per webroot, ie per domain or subdomain. The MultiPHP INI Manager allows you to change settings such as memory limit, file upload limit, error display, etc.

Increase or decrease the file upload size limit

The default limit for file uploads is 64 MB. If you need to upload larger files, follow these steps:

1. Open cPanel (`yourdomain.com/cpanel`)
2. Navigate to **MultiPHP INI Manager** under the Software section
3. Choose the appropriate domain from the dropdown, or select Home Directory to apply settings globally
4. Find the row **upload_max_filesize** and change the value as needed. Use **M** to indicate megabytes, or G to indicate gigabytes. (e.g. 100M = 100 MB)
5. Find the row **post_max_size** and change it to the value of ***upload_max_filesize* + 4M**. For example, if you set the maximum upload filesize to 100M, set post_max_size to 104M. **post_max_size should always be higher than upload_max_filesize**, otherwise uploads may fail.
6. Press **Apply**

Increase or decrease the memory limit

If you are using memory-intensive applications, such as Wordpress with Elementor or other resource-heavy plugins, you may find that some pages fail to load or load slowly. To fix this, increase the PHP memory limit. By default, the memory limit is set to 128MB, which should be sufficient for nearly all use cases, but in rare cases you may need to increase it.

To change the memory limit, do as follows:

1. Open cPanel (`yourdomain.com/cpanel`)
2. Navigate to **MultiPHP INI Manager** under the Software section
3. Choose the appropriate domain from the dropdown, or select Home Directory to apply settings globally
4. Find the row **memory_limit** and change it to an appropriate value, e.g. 256M. Use **M** to indicate megabytes, or G to indicate gigabytes. (e.g. 100M = 100 MB)
5. Press **Apply**

Note that you cannot allocate more memory to PHP than the limits set by your hosting plan. Setting the memory limit to an arbitrarily large number will not improve the performance of your site, nor will it allow PHP to use memory up to the limit. If you find your site needing more memory than allowed by your plan, you might need to upgrade to a higher plan.

Common issues related to Wordpress (incl. Elementor)

Listed below are some common issues that sometimes occur when using Wordpress with Elementor or other resource-intensive plugins.

My Wordpress site is slow

If your Wordpress website seems slow, try the following steps:

In a vast majority of cases, slowness of Wordpress websites is caused by having too many and/or poorly optimised plugins installed on the site. Before looking at any other causes, make sure you only have plugins installed on your site which the site actually requires to function. Try disabling plugins one-by-one to see if any single one causes a significant change in performance.

In certain cases, especially on resource-heavy sites, you may need to increase the PHP memory limit, as described here: How can I change PHP settings? How can I increase the file upload limit or memory limit of PHP?

Try analysing your site performance with a performance audit, such as Google Lighthouse. Such tools give useful tips on how to improve performance, and also include Wordpress-specific hints.

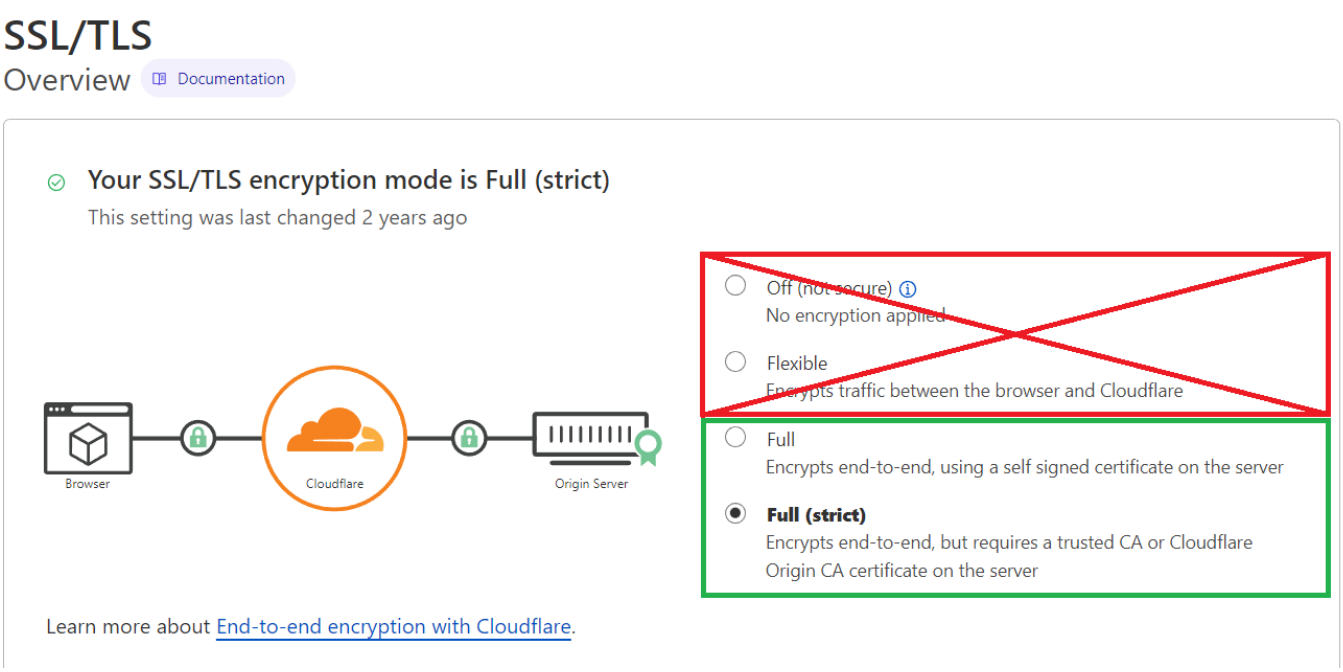
If you have a high-traffic site and you experience slowness during peak traffic, look into caching solutions for Wordpress, such as WP Super Cache or W3 Total Cache. If you still experience slow loading speeds, consider upgrading to a higher plan with more resources.

Too many redirects / redirect loop when accessing admin dashboard

If your site is using Cloudflare and the Wordpress admin dashboard is inaccessible due to a redirect loop ("Too many redirects" error in the browser), the problem is likely caused by the SSL/TLS mode in Cloudflare.

Follow these steps:

1. Navigate to the management page for your domain **at Cloudflare**
2. Click on **SSL/TLS** in the left sidebar.
3. Switch the SSL/TLS encryption mode is to **Full** or **Full (Strict)**, and *not* Flexible or Off. (See screenshot below)
4. After 5 minutes, the Wordpress admin dashboard should be accessible again.



In Flexible mode, Cloudflare connects to your site on our servers using an unencrypted connection, ie. over HTTP, even when the visitor uses HTTPS. Wordpress is usually configured to redirect from HTTP to HTTPS for security reasons, and has no idea that the visitor is already using HTTPS (since the request goes through Cloudflare which turns it into HTTP). As such, Wordpress tries to continuously redirect the visitor to HTTPS, causing a redirect loop. Setting the SSL/TLS mode to Full or Full (strict) makes Cloudflare connect over HTTPS, resolving the issue and improving security.

Elementor fails to load, shows a loading spinner or is slow

This concerns the following symptoms:

1. Opening a page for editing with Elementor (or other site builder) results in a loading spinner and/or the page not loading
2. Editing a page with Elementor is very slow

Try the following solutions in this order:

1. Update Elementor **and** Elementor Pro (if applicable). Elementor Pro is updated separately from Elementor and the update often appears only after Elementor has been updated. Using an incompatible version of Elementor Pro often results in Elementor not loading.
2. If updating did not help, increase the PHP memory limit, as described here: How can I change PHP settings? How can I increase the file upload limit or memory limit of PHP?
3. If increasing the memory limit did not help, disable ModSecurity. Navigate to cPanel and find ModSecurity under the Security section. Switch the toggle for your domain to *Off*. **If this does not resolve your issue, it is recommended to turn ModSecurity back on to improve security on your site.**

403 Access Denied error on certain pages

If you find yourself hitting 403 on certain pages, try switching off ModSecurity:
Navigate to cPanel and find ModSecurity under the Security section. Switch the toggle for your domain to *Off*. **If this does not resolve your issue, it is recommended to turn ModSecurity back on to improve security on your site.**

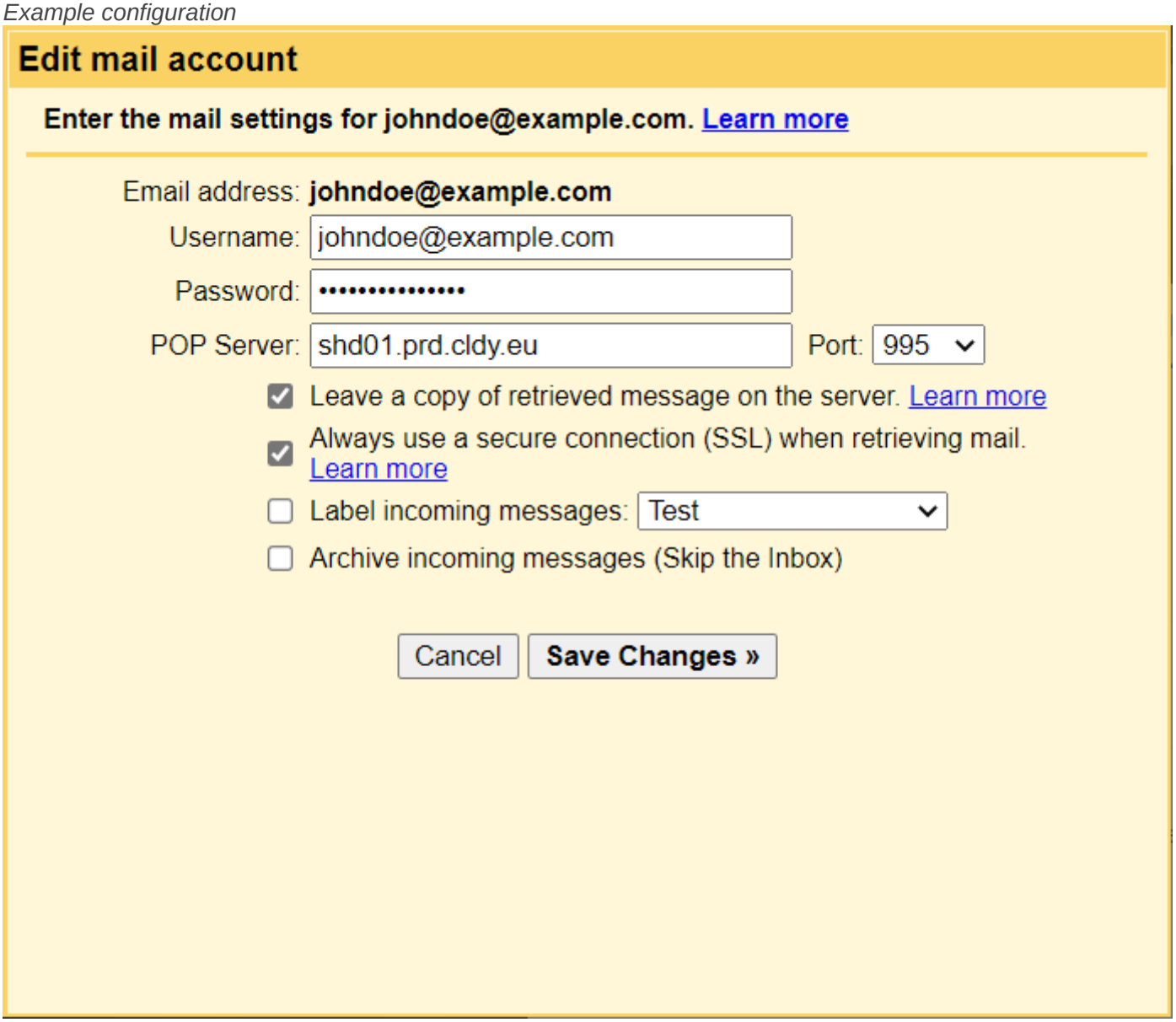
Unable to connect e-mail account to Gmail with POP3. Connection timed out or connection refused in Gmail.

It can be covenient to connect your email account hosted with us to your Gmail account in order to have all your emails in the same place. However, in some cases using the provided details in the control panel (cPanel) does not work in Gmail while still working fine with other email clients.

If you are seeing error messages such as "Connection timed out" or "Connection refused" when connecting your account to Gmail, use the following connection details instead of the ones provided in cPanel:

Setting	Value
Username	*Email account address* (e.g. firstname@domain.com)
Password	*Email account password*
POP Server	*Hosting server name* e.g. **shd01.prd.cldy.eu** (not mail.yourdomain.com)
Port	**995**
Always use a secure connection	**Yes**

Example configuration



Most issues are caused by Gmail having problems with the server being entered as *mail.yourdomain.com* instead of the server name. This is something we cannot fix on our side and is up to Gmail to resolve in the future.

If you are still having trouble connecting your account to Gmail or other email client, get in touch with us by opening a ticket in the client portal!

How to add an additional website / domain to my hosting plan?

All hosting plans support hosting multiple websites / domains on the same plan. The Rain, Thunder, and Tornado plan support 3, 5, and 10 websites respectively, including the main domain.

Adding an additional website

To add an additional website to your hosting account, follow these steps:

1. **Make sure your domain points to Cloudey.** This can be achieved by either changing the nameservers of your domain to Cloudey nameservers (ns1.cloudey.net and ns2.cloudey.net) or by creating an A record that points to the IP of your hosting server. The A record should be the same as the one for your main domain. For more information regarding nameservers and DNS, see here. You can check the nameservers and DNS records of your domain using our simple tool.
2. Open the hosting control panel (cPanel) and navigate to **Domains** under the identically named *Domains* section.
3. Click the button **Create A New Domain** on the top right of the page.
4. Enter your new domain as instructed in the form.
5. **Uncheck** the checkbox to share document root with the main domain. Otherwise, you **will not** be able to use the domain for a separate website from your main domain.
6. Click **Submit**.

If everything went well, you should now see a new folder for the new website in the home directory of your account (use the File manager in the hosting control panel to manage your website's files). You can proceed with uploading files or installing software for your new site.

An SSL certificate will be provisioned automatically for your new domain, but it may take a few moments. Read more about HTTPS and SSL certificates

Using Cloudflare

Are you using Cloudflare instead of Cloudey's nameservers for your domain? In this case, the procedure above may not work for you. **Open a ticket** with us instead to add the domain to your account.

Troubleshooting

The most common error when trying to add a new website to your account looks like this:

> (XID j3rjtd) This domain points to an IP address that does not use the DNS servers associated with this server. Transfer the domain to this server's nameservers at the domain's registrar or update your system to recognize the current DNS servers. To do this, use WHM's Configure Remote Service IPs interface.

This means that the DNS settings of the domain you are trying to add are not correct, and the domain is not pointed to Cloudey. To fix this, follow the instructions in step 1 above. Keep in mind that DNS changes can take anywhere from a few minutes to a couple of hours to take effect. If you recently changed the domain's DNS settings and see this error, try again later.

If the problem persists, get in touch with our support, and we will add the domain manually.
Are you using Cloudflare and seeing the error above? Open a ticket with us to add the domain to your account.

My IP was blocked from accessing my website or the hosting control panel!

There are various reason why an IP can end up temporarily or permanently blocked from accessing the server. In most cases, this helps prevent our servers and your website against malicious attackers and botnets, but in rare cases, it can end up blocking legitimate users.

Getting unblocked

In some cases, you will be presented with a captcha which lets you unblock your IP quickly and easily without further issues.

In other cases, you may need to contact our support to unblock your IP. Make sure to include your IP in the support ticket!

IP being blocked repeatedly

Sometimes you may find your IP blocked almost immediately after unblocking yourself. In a vast majority of cases, this is due to a misconfigured email client on your device or on your network, which makes repeated failed login attempts to your email account hosted with us, causing the IP to be blocked as a suspected attacker.

This can happen if you recently changed your email account password, or if you have entered the wrong password to an email client. Check the email clients and apps on **all of your devices** and make sure they are using the correct credentials. After you have corrected your email details, get in touch with us, and we will unblock your IP.

Is your IP still getting blocked, and you are convinced it is not due to a misconfigured email app? Get in touch, and we will figure out what is causing the issue!

Addon domains and Cloudflare - Error "This domain points to an IP address that does not use the DNS servers associated with this server"

Problem

When adding an additional domain to your hosting account (*addon domain*), a verification of the domain's nameservers is performed. To successfully add the domain, its nameservers must be set to ns1.cloudey.net and ns2.cloudey.net. This is done to prevent adding domains which belong to a third party.

However, this check fails for domains using Cloudflare, since the nameservers of the domain will not match ours. When trying to add a domain which is set up with Cloudflare, you will see the error message "This domain points to an IP address that does not use the DNS servers associated with this server".

Solution

To add a domain which uses Cloudflare (or other 3rd party DNS provider) instead of Cloudey's nameservers, please **open a ticket** containing the domain you would like to add to your account. We will fulfil your request as soon as possible!

Keep in mind that you will need to manually add any DNS records, including for subdomains, when using Cloudflare. You can find the essential DNS records for e-mail and other services here: Nameservers, DNS, and Cloudflare