Comodo
cWatch Web Security

Software Version 5.8

Quick Start Guide

Guide Version 5.8.010820

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo cWatch Web Security - Quick Start Guide

- cWatch Web Security is a cloud-based security intelligence service that continuously monitors and protects websites against millions of attacks and threats.
- In addition to **website protection**, cWatch includes content delivery network (CDN) and backup services.

This document explains how you can purchase licenses, add websites for protection, and use the cWatch interface.

Purchase Website Licenses

If you haven't done so already, please choose a cWatch plan at **https://cwatch.comodo.com/plans.php**.

Available license types are:

- Basic
- Pro
- Premium

General notes

- You can purchase licenses from the cWatch website at **https://cwatch.comodo.com/plans.php**. You can also purchase them from within the cWatch console after creating an account.
- Licenses are charged per-website. Sub-domains are not covered if you buy a license for a primary domain. For example, you would need to buy separate licenses for domain.com and mail.domain.com.

- You can add multiple license types to your account if you want to implement different protection levels on different sites.
- You can associate websites with licenses in the cWatch interface. See **Add Websites** for more details.
- You can only purchase backup licenses after you have purchased a cWatch license. See '**Purchase a Backup License**' if you need help with this.

The following table shows the features and services with each license:

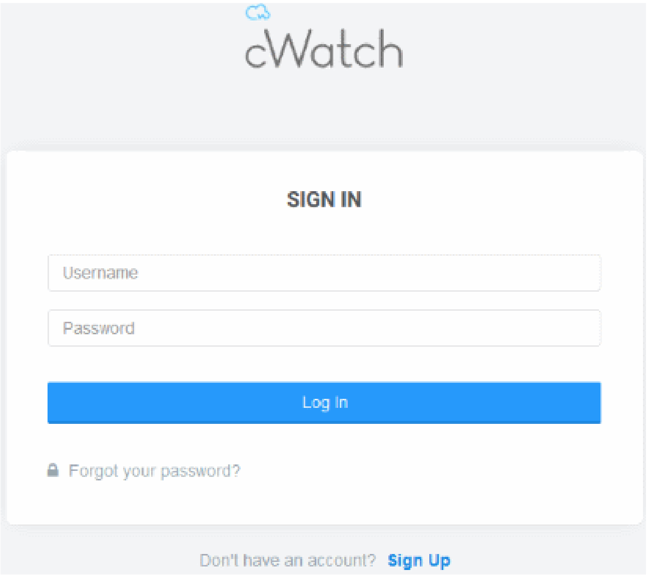
Feature/Service	Premium	Pro	Basic
Malware removal by experts Hack repair and restore Vulnerability repair and restore Traffic hijack recovery SEO/Search poisoning recovery	Unlimited	Unlimited	One time
Automatic Malware Removal	✓	✓	✗
Spam & Website Filtering	✓	✓	✗
Malware Scan	Every 6 hours	Every 12 hours	Every 24 hours
Vulnerability (OWASP) Detection	Every 6 hours	Every 12 hours	Every 24 hours
Security Information and Event Management (SIEM)	✓	✓	✗
24/7 Cyber-Security Operations Center (CSOC)	✓	✓	✗
Dedicated analyst	✓	✓	✗
Web Application Firewall (WAF)			
Custom WAF rules	✓	✗	✗
Bot Protection	✓	✓	✗
Scraping Protection	✓	✓	✗
Content Delivery Network (CDN)			
Layer 7 DDoS Protection	✓	✓	✓
Layer 3, 4, 5 & 6 DDoS Protection	✓	✓	✓
Trust Seal	✓	✓	✓

After completing a purchase:

- **New users -** A Comodo account will be created for you at **https://accounts.comodo.com**. We will send you an email containing your subscription ID and an account activation link.
- **Existing users -** We will send you a confirmation mail containing your license key.
- Please save your license key in a safe location.
- Next, login to cWatch at **https://login.cwatch.comodo.com/login**

Login to cWatch

You can login into cWatch at **https://login.cwatch.comodo.com/login** using any browser:



cWatch

SIGN IN

Username

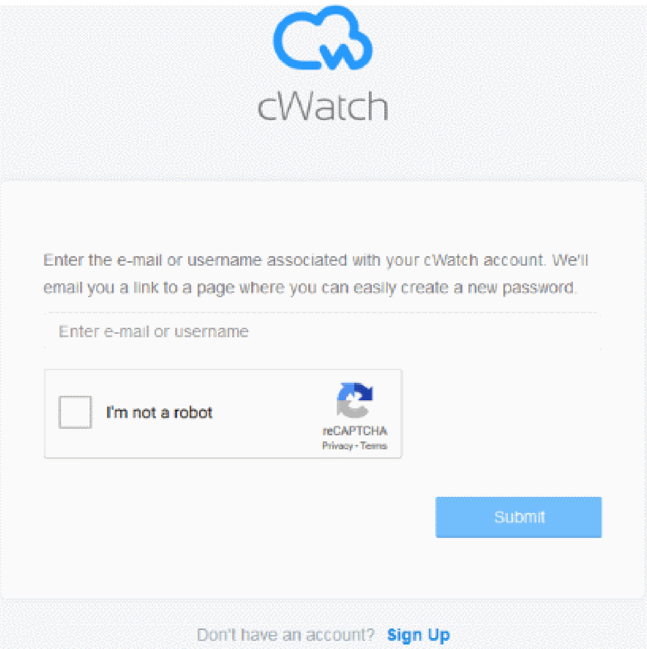
Password

First time Login:

- Get your username and password from the cWatch confirmation email.
- After logging in, please change your password immediately for security reasons.

Lost Passwords

- Click 'Forgot your password?' to reset your password.
- Enter your mail address, complete the Captcha, and click 'Submit' on the confirmation screen:



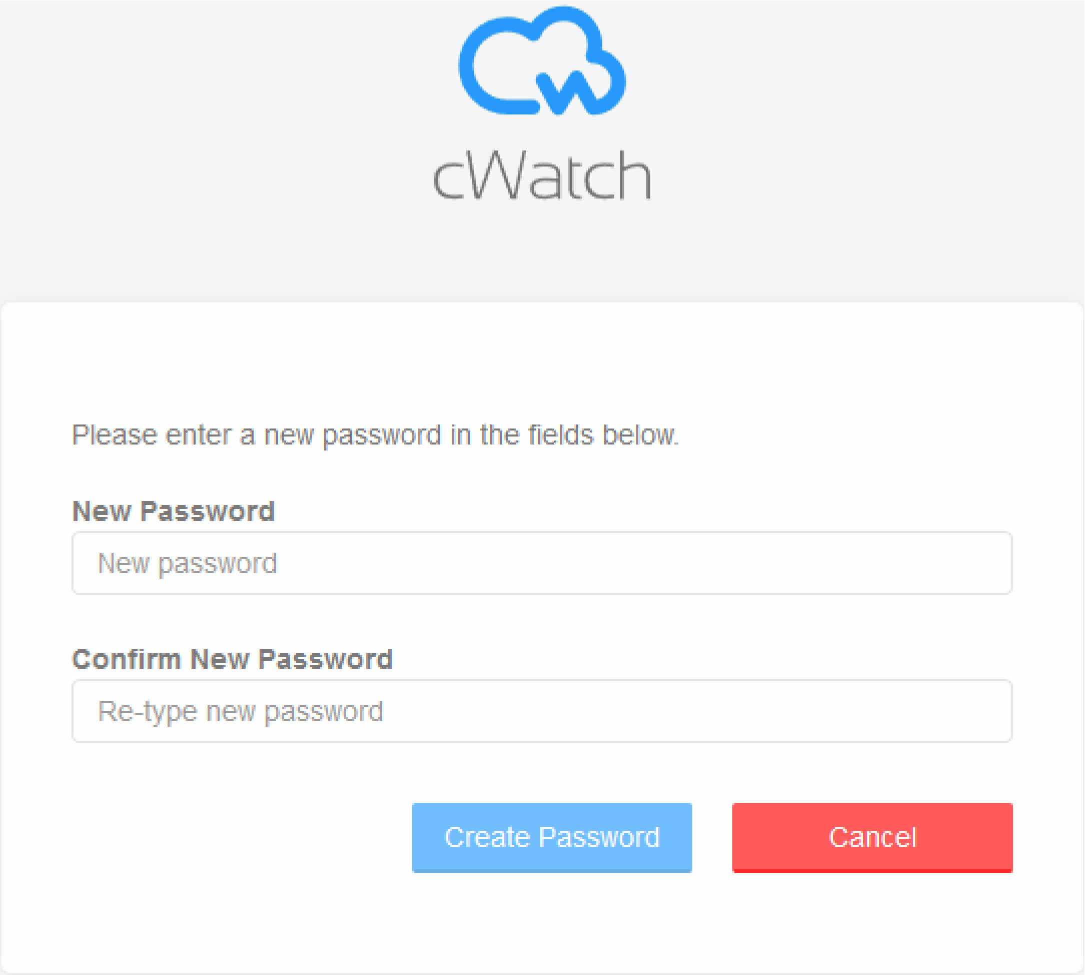
cWatch

Enter the e-mail or username associated with your cWatch account. We'll email you a link to a page where you can easily create a new password.

Enter e-mail or username

□ I'm not a robot

- You will receive a password reset mail.
- Click 'Reset Password' to open the password creation page.
- Enter a password and confirm it:



Please enter a new password in the fields below.

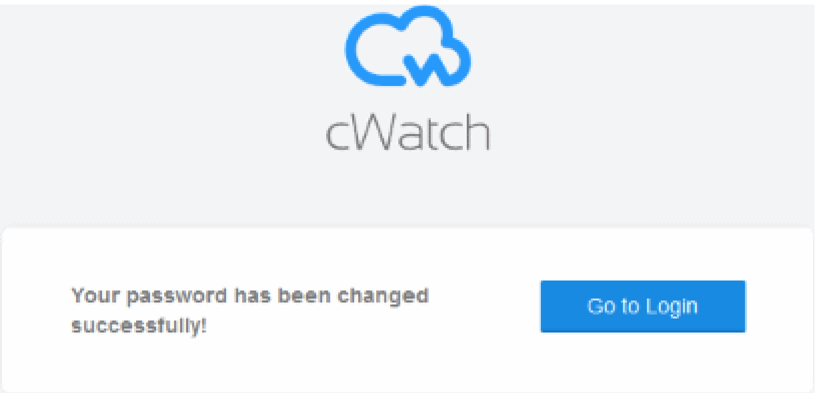
New Password

New password

Confirm New Password

Re-type new password

- Click 'Create Password'



Your password has been changed successfully!

- Click 'Go to Login' to access your account with your new password.

Add Websites

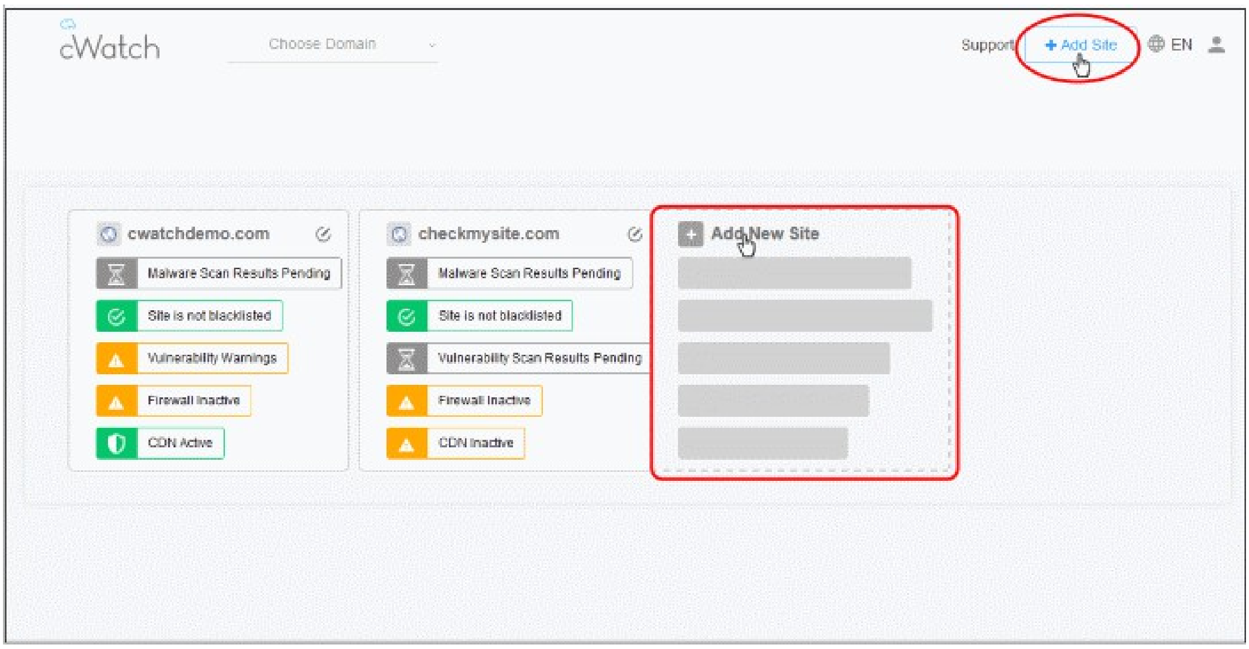
- Your first step is to add websites to cWatch so you can activate protection and use the content delivery network (CDN).
- The number of sites you can add depends on your license.
- Once added, you can configure malware scanning, threat monitoring, CDN, and backup settings for each site. See the next section, **Configure your Websites**, for more details.

Add a new domain

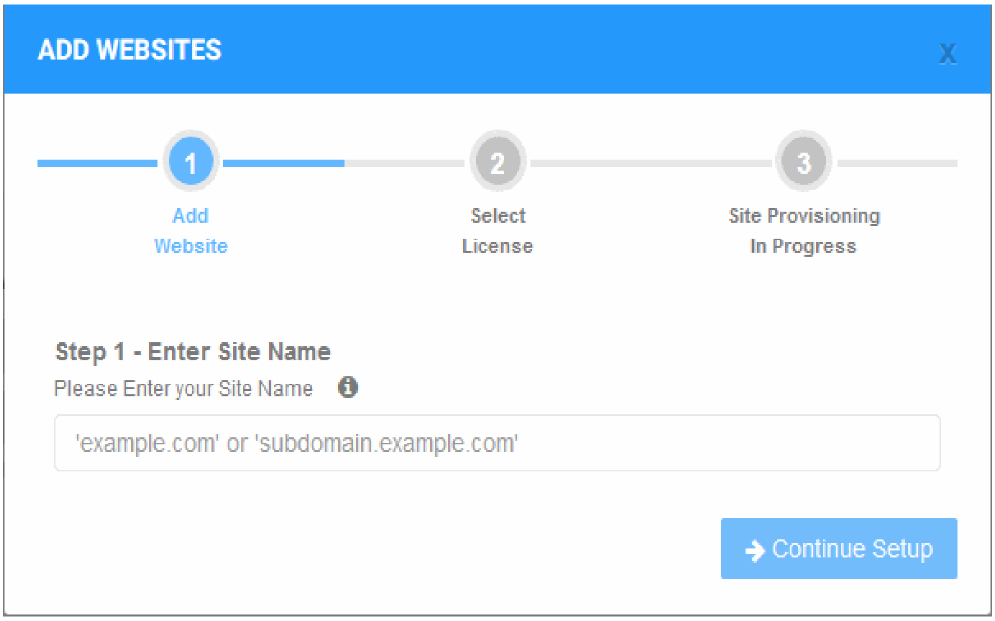
- Login to cWatch at **https://login.cwatch.comodo.com/login** with your Comodo account credentials.

The cWatch dashboard shows any existing sites as tiles. New users should only see the 'Add New Site' tile.

- Click the 'Add New Site' tile, or the 'Add Site' button at top-right:



First, enter the domain you want to add:


ADD WEBSITES

Step 1 - Enter Site Name

Please Enter your Site Name

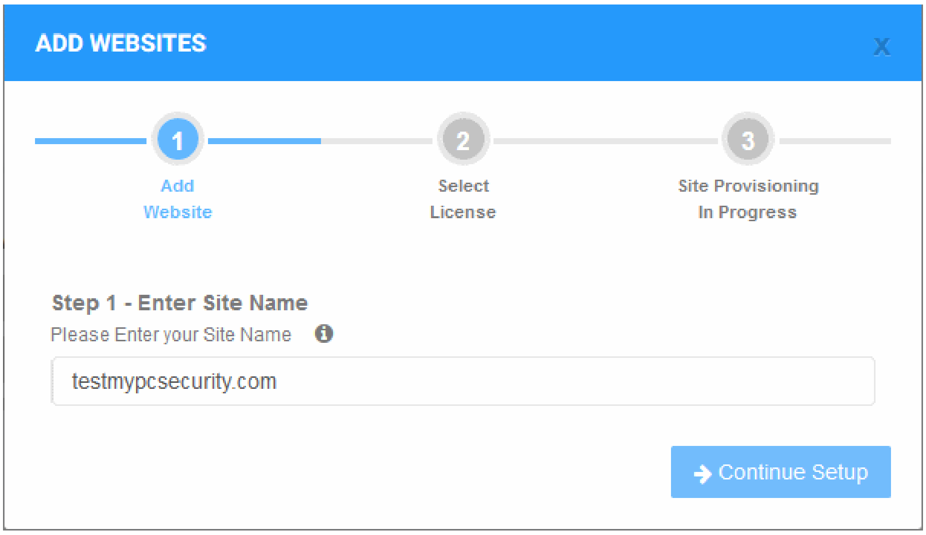
'example.com' or 'subdomain.example.com'

The wizard has three steps:

- Step 1 - Register your website
- Step 2 - Select License
- Step 3 - Finalization

Step 1 - Register your website

- Enter the domain name of the site you want to register. Do not include 'www.' at the start.



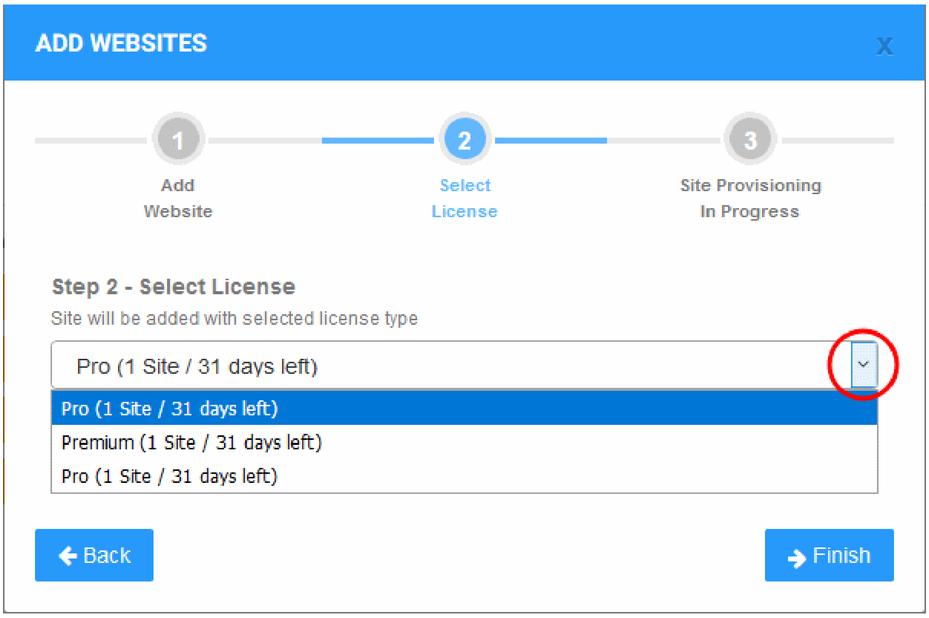
Step 1 - Enter Site Name
Please Enter your Site Name
testmypcsecurity.com

- Click 'Continue Setup' to move to the next step.

Step 2 - Select License

Next, choose the license you want to apply to the site.

- cWatch features vary according to license type.
- The drop-down lists all licenses that you have purchased.
- Choose the license you want to apply to the site then click ‘Finish’:

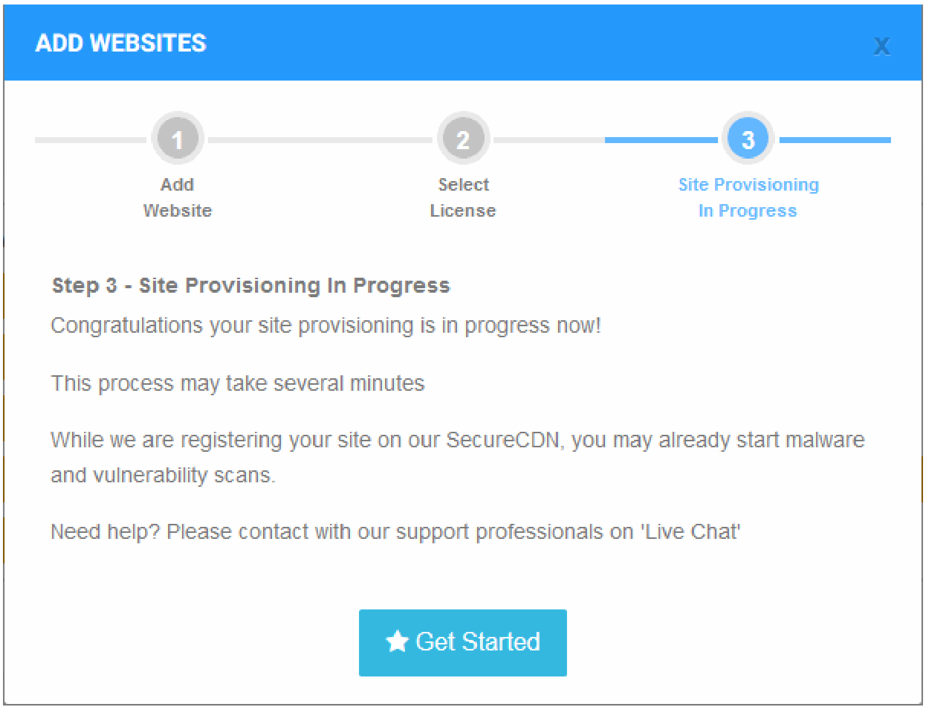


Step 2 - Select License
Site will be added with selected license type
Pro (1 Site / 31 days left)

Pro (1 Site / 31 days left)
Premium (1 Site / 31 days left)
Pro (1 Site / 31 days left)

Step 3 - Finalization

The final stage is automatic - cWatch will provision your site:



Step 3 - Site Provisioning In Progress

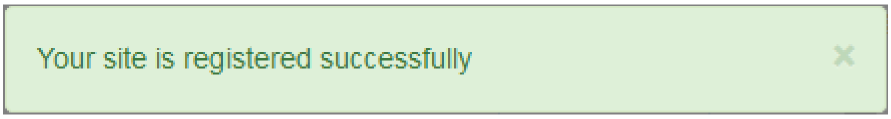
Congratulations your site provisioning is in progress now!

This process may take several minutes

While we are registering your site on our SecureCDN, you may already start malware and vulnerability scans.

Need help? Please contact with our support professionals on 'Live Chat'

You will see the following message when the process is complete:



Your site is registered successfully

The next sections cover how to enable protection and configure your sites.

- Click 'Get Started' to open the site's 'Overview' page
- The overview page lets you configure malware and vulnerability scans, firewall rules, CDN settings, and more.

Note:

- cWatch auto-generates a CNAME DNS record for the website you just added.
- You need to add this record to the DNS entry for your domain. This will activate the content delivery network (CDN) on the site.
- View the CNAME record:
  - Select a website in the drop-down at top-left of the dashboard
  - Select the 'DNS' tab (or click the hamburger button and select 'DNS')
  - The CNAME record is shown under 'DNS'
- Your web host may be able to help you add the CNAME. Guidance is also available at **https://support.google.com/a/topic/1615038?hl=en**.

Tip: You can skip this step for now and add the CNAME to DNS later. See **DNS Configuration** for help with this.

- A basic website scan will run on the site immediately after it has been added. This is a first-level check for threats and requires no configuration. Any discovered vulnerabilities are shown in the results at the end of the scan. See '**Website Scans**' for more information about this.

Configure your Websites

The next steps are to:

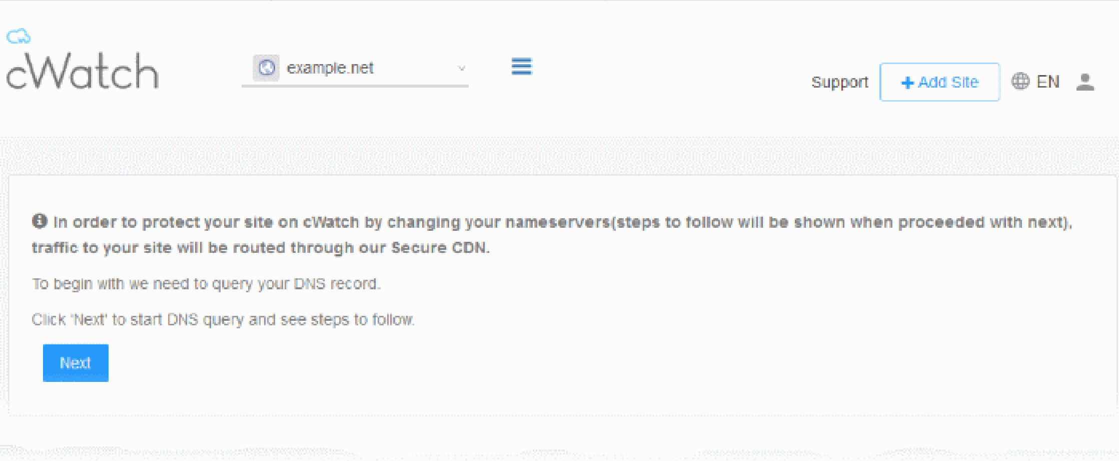
- **Configure DNS**. This lets you enable cWatch site monitoring, the content delivery network, and the web application firewall (WAF).
- **Configure your SSL certificate**. Doing so allows cWatch to inspect encrypted, https traffic.
- **Configure Malware Scans**. Schedule regular virus scans on your website. You can also run scans on-demand if you wish.
- **Configure the CDN**. This improves site performance by serving your website from the location closest to your visitor.
- **Configure the Web Application Firewall (WAF).** The firewall keeps your site online by automatically blocking a wide range of attacks, including DDOS attacks, SQL injection and cross-site scripting.
- **Configure the Trust Seal**. The trust seal is a website badge which tells visitors your site is protected by the leading name in online security. See **Add Trust Seal to Your Websites** for more details.
- **Configure Website Backup**. Back up your website and database. You can restore your website with a single click in the event of data loss.

DNS Configuration

- Select a website from the drop-down at top-left then choose 'DNS'
- You need to change your site's authoritative DNS server to Comodo DNS to enable cWatch protection, the content delivery network, and the Web Application Firewall (WAF).
  - The DNS page shows the authoritative name servers (NS) for your site. You can use these to configure DNS settings.
- After switching to Comodo DNS, you should use this page for DNS management instead of your web host's DNS management page. For example, you can add new 'CNAME' and 'A' records, change MX records, and more.

Configure DNS settings on your site

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'DNS' tab
  - Or click the hamburger button and select 'DNS'
- Click 'Next' to fetch your existing DNS records:

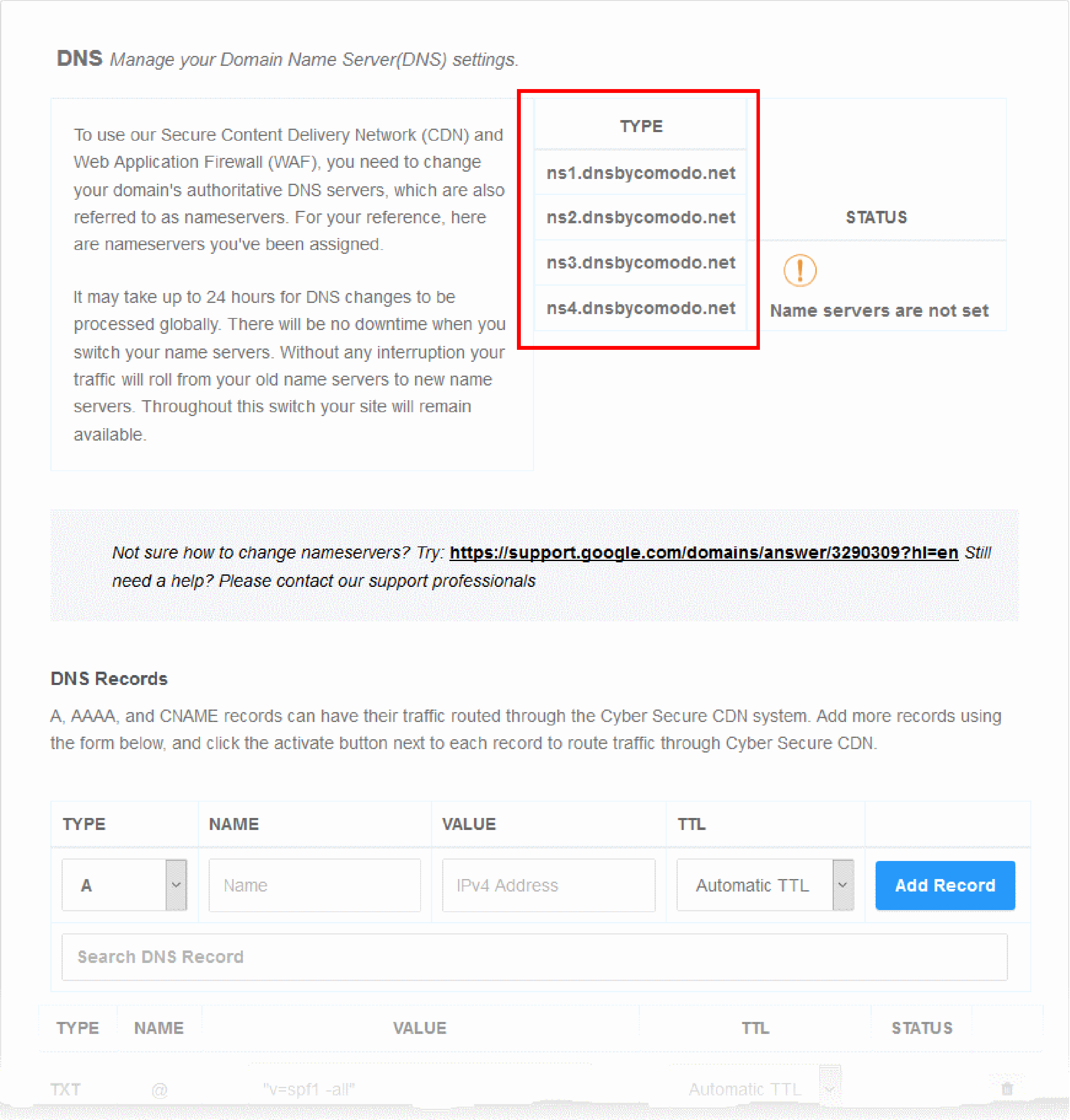


In order to protect your site on cWatch by changing your nameservers(steps to follow will be shown when proceeded with next), traffic to your site will be routed through our Secure CDN.

To begin with we need to query your DNS record.

Click 'Next' to start DNS query and see steps to follow.

- You need to go to your site's DNS management page and enter the new name servers.
- cWatch will show your site's name server (NS) details as follows:



DNS *Manage your Domain Name Server(DNS) settings.*

To use our Secure Content Delivery Network (CDN) and Web Application Firewall (WAF), you need to change your domain's authoritative DNS servers, which are also referred to as nameservers. For your reference, here are nameservers you've been assigned.

It may take up to 24 hours for DNS changes to be processed globally. There will be no downtime when you switch your name servers. Without any interruption your traffic will roll from your old name servers to new name servers. Throughout this switch your site will remain available.

TYPE	STATUS
ns1.dnsbycomodo.net ns2.dnsbycomodo.net ns3.dnsbycomodo.net ns4.dnsbycomodo.net	! Name servers are not set

Not sure how to change nameservers? Try: **https://support.google.com/domains/answer/3290309?hl=en** *Still need a help? Please contact our support professionals*

DNS Records

A, AAAA, and CNAME records can have their traffic routed through the Cyber Secure CDN system. Add more records using the form below, and click the activate button next to each record to route traffic through Cyber Secure CDN.

TYPE	NAME	VALUE	TTL	
A	Name	IPv4 Address	Automatic TTL	Add Record

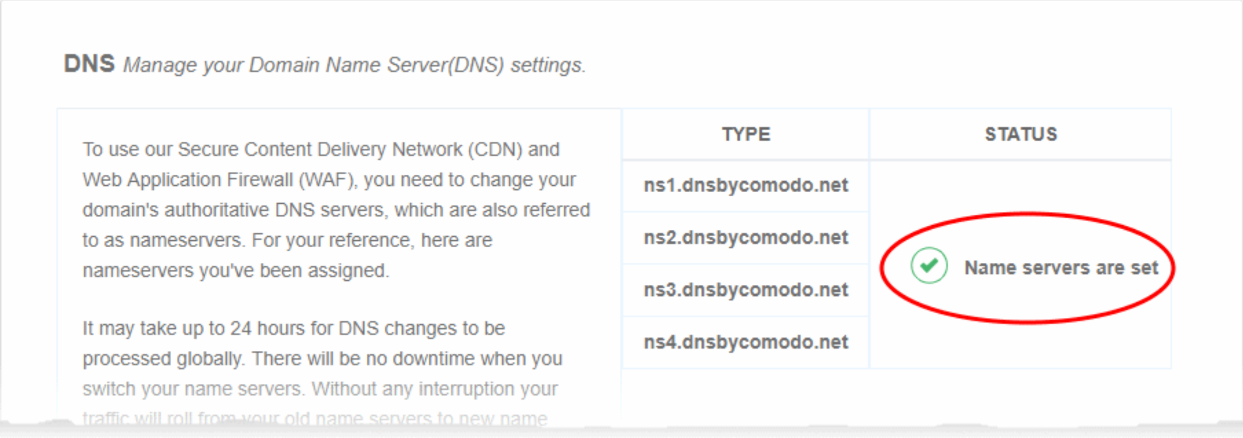
Search DNS Record

TYPE	NAME	VALUE	TTL	STATUS
TXT	@	"v=spf1 -all"	Automatic TTL	

- See **https://support.google.com/domains/answer/3290309?hl=en** if you need help to change nameservers.

You can view whether the change was successful in the cWatch interface:

- Select the target website from the menu at top-left
- Click the 'DNS' tab
  - or click the hamburger button and select 'DNS'
- Look in the 'Status' column:



DNS *Manage your Domain Name Server(DNS) settings.*

To use our Secure Content Delivery Network (CDN) and Web Application Firewall (WAF), you need to change your domain's authoritative DNS servers, which are also referred to as nameservers. For your reference, here are nameservers you've been assigned.

It may take up to 24 hours for DNS changes to be processed globally. There will be no downtime when you switch your name servers. Without any interruption your traffic will roll from your old name servers to new name

TYPE	STATUS
ns1.dnsbycomodo.net	✓ Name servers are set
ns2.dnsbycomodo.net	
ns3.dnsbycomodo.net	
ns4.dnsbycomodo.net	

- It may take up to 24 hours for the DNS changes to propagate
- There is no site downtime when you switch name servers. It is a seamless transition.

Note:

- You have to use the cWatch interface to manage your DNS records once you have changed to Comodo DNS. You can no longer do these changes in your web host's DNS management page.
- For example, changes to your MX records must be done in cWatch. See '**Manage DNS Records**' in the cWatch admin guide for more.

SSL Configuration

- Select a website from the drop-down at top-left
- Click the 'SSL' tab
- SSL certificates identify a website’s owner, and encrypt all data that passes between the site and a visitor's browser.

There are two ways to deploy a certificate:

1) Bring your own SSL certificate

- Upload your site’s existing certificate to the cWatch CDN edge servers. Recommended for most customers.
- This will secure the traffic between your site (the origin server) and the cWatch CDN.
- See **Upload your own SSL Certificate** to find out how to deploy your certificate

2) Get a free SSL certificate

- Deploy a free certificate from Comodo to the CDN Edge servers. Again, this will encrypt traffic between your site and the CDN.

You need to configure your site to use Comodo DNS in order to get the free certificate. There are two ways to do this:

a) Change your domain's authoritative DNS servers to Comodo DNS

OR

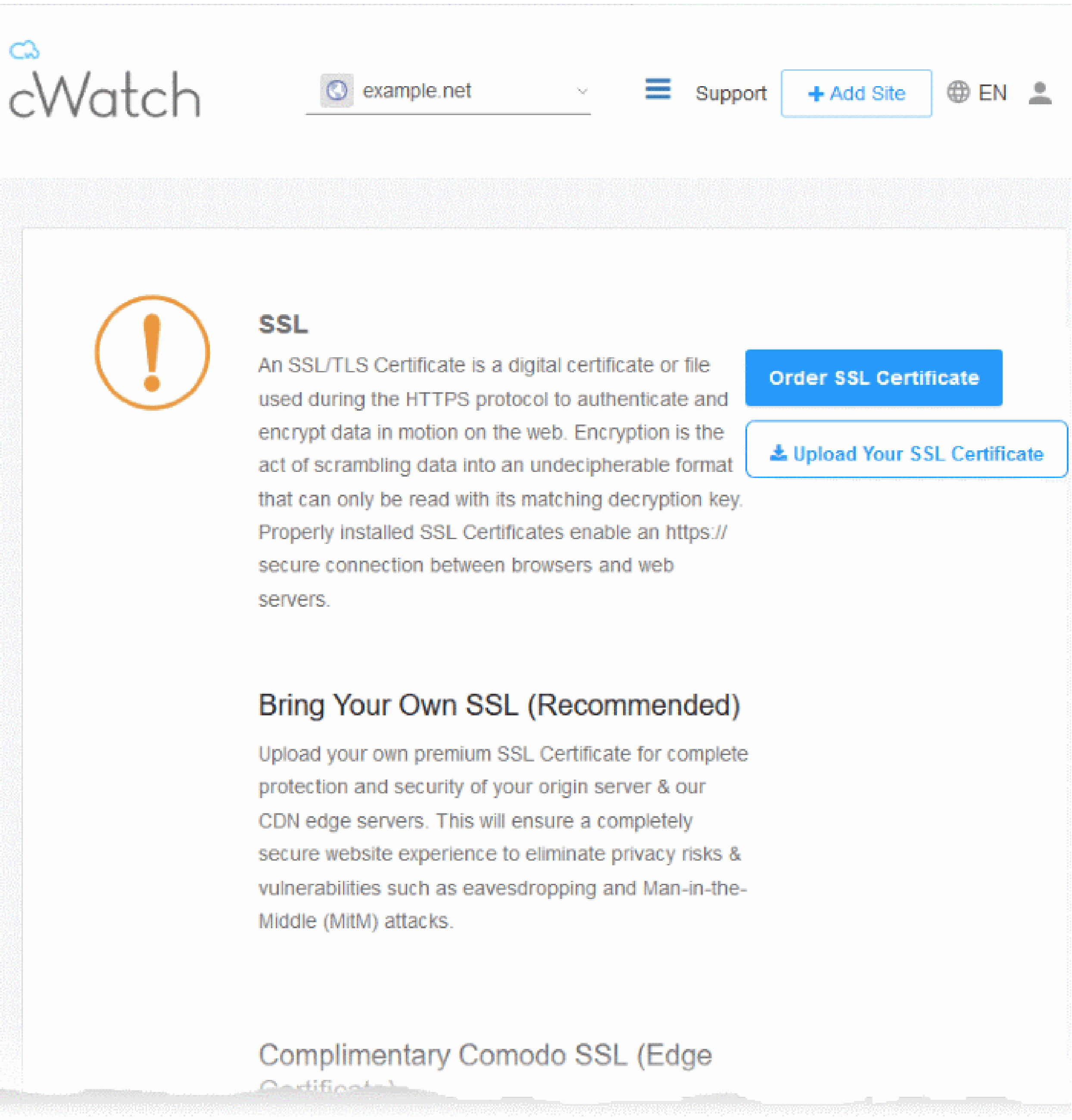
b) Enter DNS records explicitly

Help to configure DNS is available in **Activate CDN for a Website**.

See **Install Complimentary SSL Certificate** for help to deploy your free certificate.

Upload your own SSL Certificate

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'SSL' tab
  - Or click the hamburger button and select 'SSL'



SSL

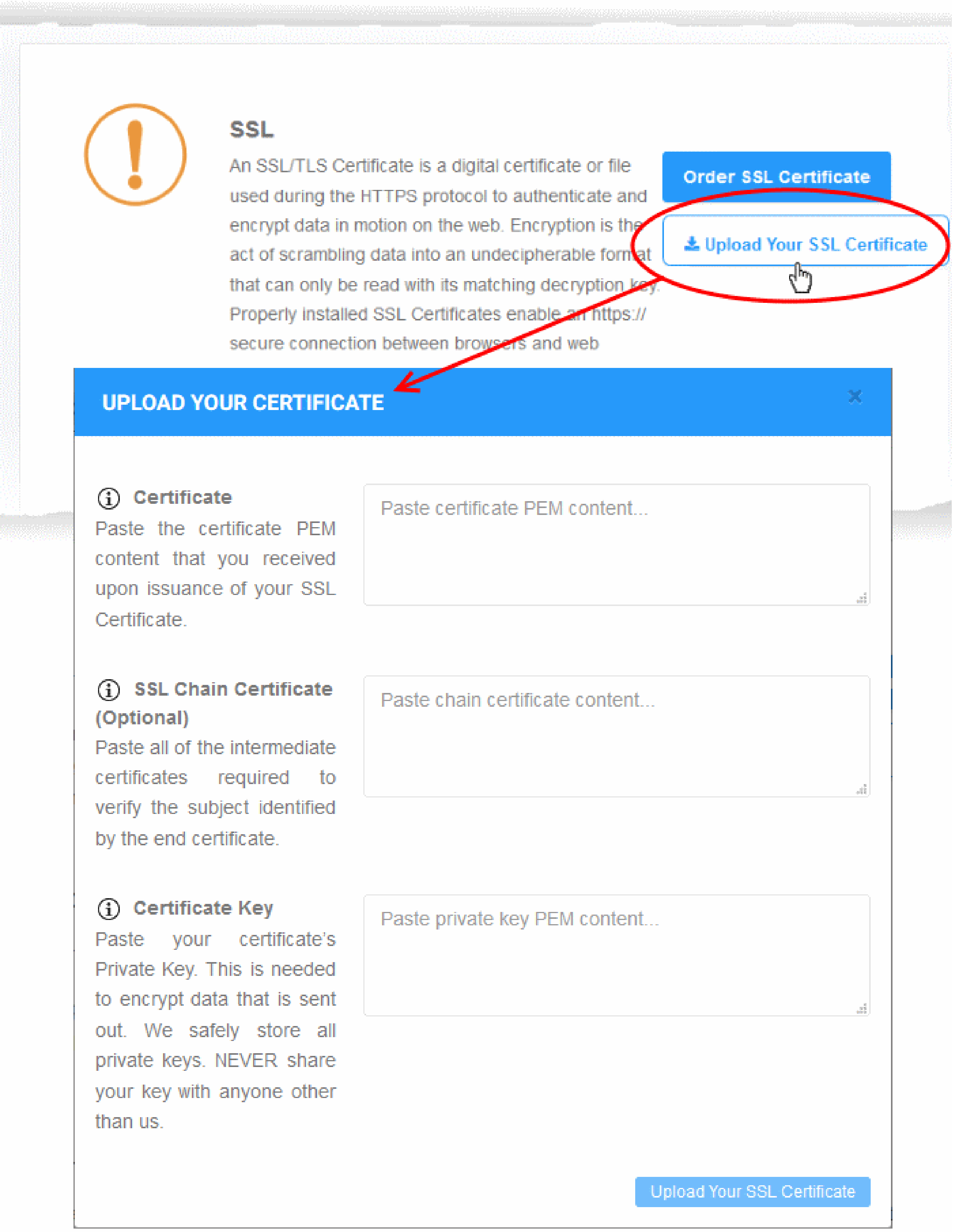
An SSL/TLS Certificate is a digital certificate or file used during the HTTPS protocol to authenticate and encrypt data in motion on the web. Encryption is the act of scrambling data into an undecipherable format that can only be read with its matching decryption key. Properly installed SSL Certificates enable an https:// secure connection between browsers and web servers.

Bring Your Own SSL (Recommended)

Upload your own premium SSL Certificate for complete protection and security of your origin server & our CDN edge servers. This will ensure a completely secure website experience to eliminate privacy risks & vulnerabilities such as eavesdropping and Man-in-the-Middle (MitM) attacks.

Complimentary Comodo SSL (Edge

- Click 'Order SSL Certificate' if you do not already have a certificate on your site
  - You will be taken to SSL purchase page to buy a new certificate
  - You can install the certificate on your web-server then upload it to cWatch.
- Click 'Upload Your SSL Certificate' to submit your existing certificate:



SSL

An SSL/TLS Certificate is a digital certificate or file used during the HTTPS protocol to authenticate and encrypt data in motion on the web. Encryption is the act of scrambling data into an undecipherable format that can only be read with its matching decryption key. Properly installed SSL Certificates enable an https:// secure connection between browsers and web

UPLOAD YOUR CERTIFICATE

Certificate
Paste the certificate PEM content that you received upon issuance of your SSL Certificate.

Paste certificate PEM content...

SSL Chain Certificate (Optional)
Paste all of the intermediate certificates required to verify the subject identified by the end certificate.

Paste chain certificate content...

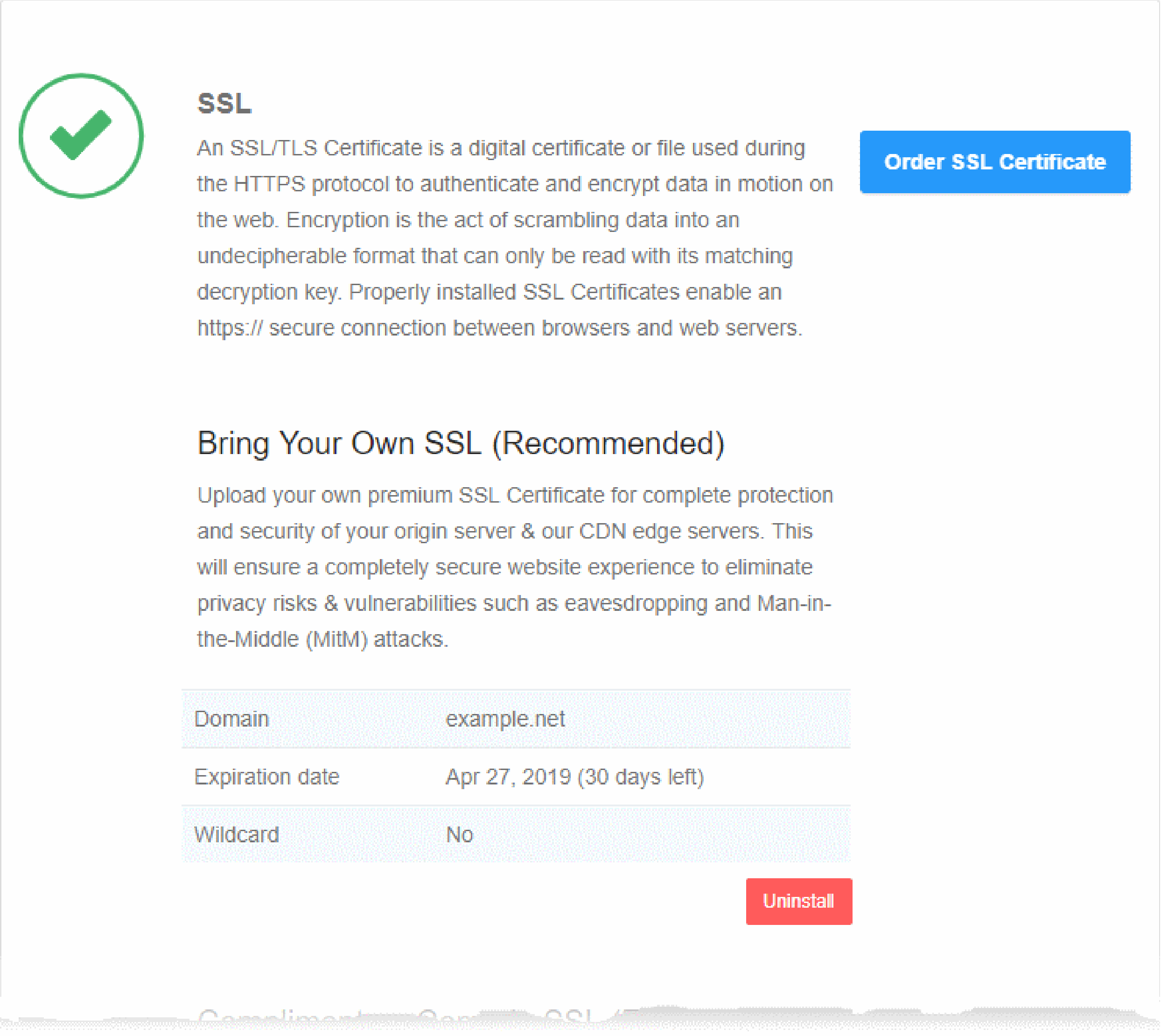
Certificate Key
Paste your certificate's Private Key. This is needed to encrypt data that is sent out. We safely store all private keys. NEVER share your key with anyone other than us.

Paste private key PEM content...

Upload Your Certificate - Form Parameters	
Parameter	**Description**
Certificate	Paste the content of your certificate. The content you are looking for is something like this: -----BEGIN CERTIFICATE----- MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGE wJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBAcTAkNOMQswCQYDVQQKEwJPTjELMAkGA 1UECxMC VU4xFDASBgNVBAMTC0hlcm9uZyBZYW5nMB4XDTA1MDcxNTIxMTk0N1oXD TA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAgTAlBOMQswCQYDV QQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTAlVOMRQwEgYDVQQDEwtIZXJvb mcgWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBe wKE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbMOoRcKK9vEcgMtcLFuQTWDl3RA gMBAAGj gbEwga4wHQYDVR0OBBYEFFXI70krXeQDxZgbaCQoR4jUDncEMH8GA1UdI wR4MHaA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMQswCQYDVQQGEwJDTjELM AkGA1UE CBMCUE4xCzAJBgNVBAcTAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECxMCV U4xFDAS BgNVBAMTC0hlcm9uZyBZYW5nggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIh vcNAQEE BQADQQA/ugzBrjjK9jcWnDVfGHlk3icNRq0oV7Ri32z/ +HQX67aRfgZu7KWdI+Ju Wm7DCfrPNGVwFWUQOmsPue9rZBgO -----END CERTIFICATE-----
SSL Chain Certificate	If your certificate contains an intermediate certificate then paste it here. If not, leave this field blank.
Certificate Key	Private key of your certificate

- Click 'Upload Your SSL Certificate'

The SSL certificate will be uploaded to the CDN edge servers.



SSL

An SSL/TLS Certificate is a digital certificate or file used during the HTTPS protocol to authenticate and encrypt data in motion on the web. Encryption is the act of scrambling data into an undecipherable format that can only be read with its matching decryption key. Properly installed SSL Certificates enable an https:// secure connection between browsers and web servers.

Bring Your Own SSL (Recommended)

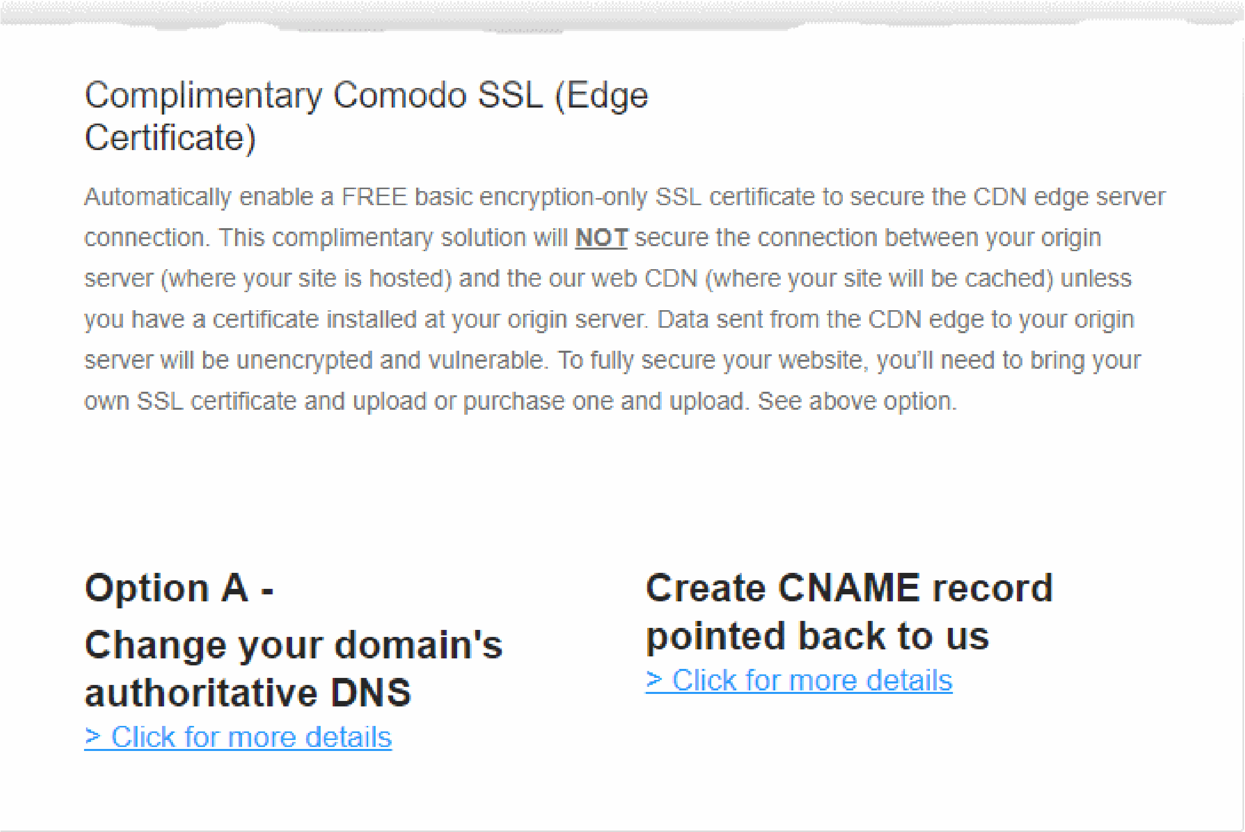
Upload your own premium SSL Certificate for complete protection and security of your origin server & our CDN edge servers. This will ensure a completely secure website experience to eliminate privacy risks & vulnerabilities such as eavesdropping and Man-in-the-Middle (MitM) attacks.

Domain	example.net
Expiration date	Apr 27, 2019 (30 days left)
Wildcard	No

Once uploaded, traffic between the CDN and your website visitors is encrypted. Since the certificate is already installed on your site, the communication between the origin and the CDN is also encrypted.

Install Complimentary SSL Certificate

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'SSL' tab
  - Or click the hamburger button and select 'SSL'
- Scroll down to 'Complimentary Comodo SSL (Edge Certificate)':



Complimentary Comodo SSL (Edge Certificate)

Automatically enable a FREE basic encryption-only SSL certificate to secure the CDN edge server connection. This complimentary solution will **NOT** secure the connection between your origin server (where your site is hosted) and the our web CDN (where your site will be cached) unless you have a certificate installed at your origin server. Data sent from the CDN edge to your origin server will be unencrypted and vulnerable. To fully secure your website, you'll need to bring your own SSL certificate and upload or purchase one and upload. See above option.

Option A -

Change your domain's authoritative DNS

> Click for more details

Create CNAME record pointed back to us

> Click for more details

You have two options to enable the free certificate:

- **Option A - Change your domain's authoritative DNS servers to Comodo** - Applies if you have already pointed your name servers to Comodo authoritative DNS.
- **Option B - Create a CNAME record which points to Comodo** - Applies if you have entered explicit DNS records to your domain's DNS settings

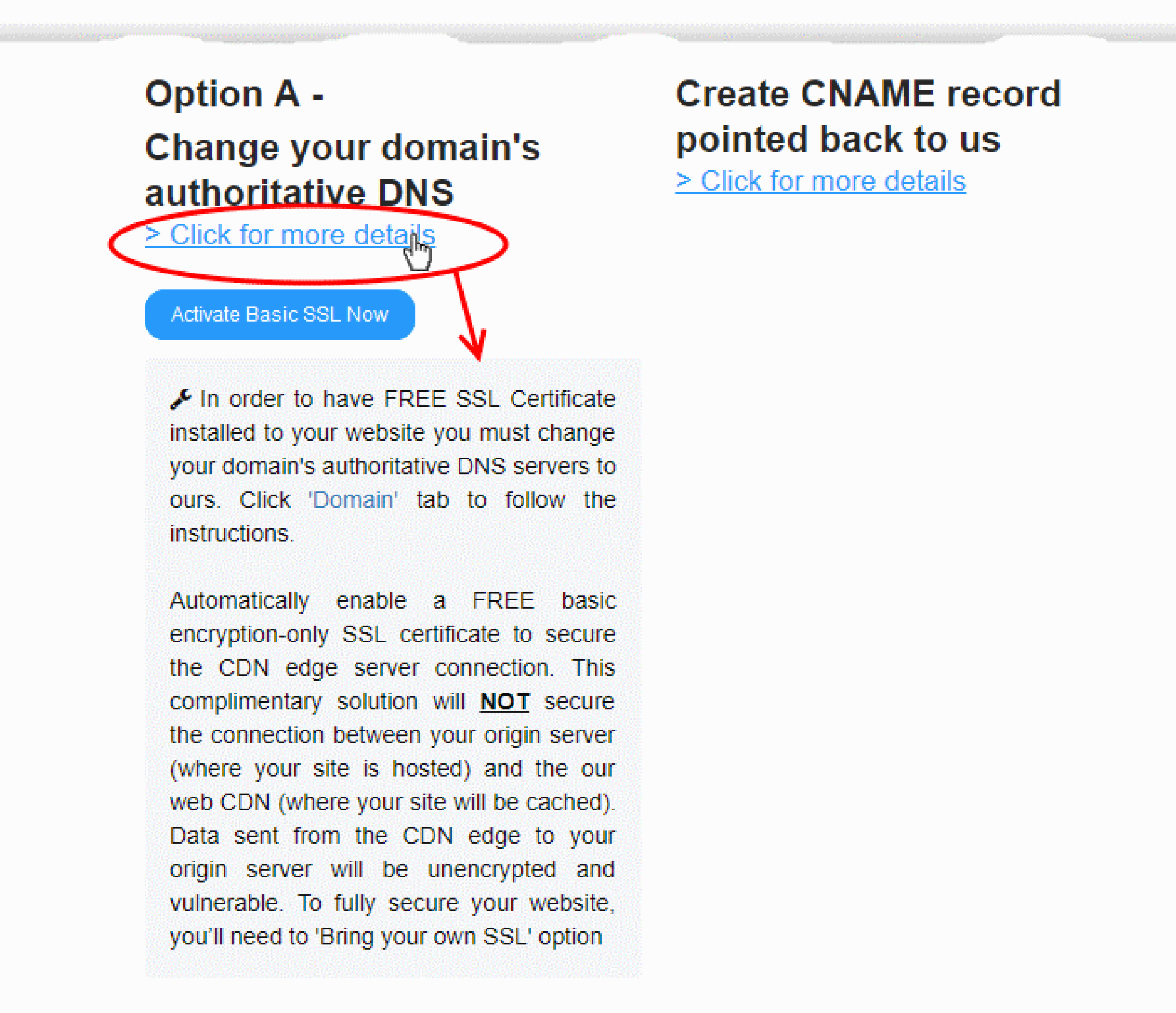
Option A - Change your domain's authoritative DNS servers to Comodo

Prerequisite - You have configured the site to use Comodo DNS by adding the name server (NS) records.

- The NS records are available in the 'DNS' and 'CDN' > 'Settings' > 'Activation' pages of the site.

See **DNS Configuration** for more details.

- Scroll to 'Option A - Change your domain's authoritative DNS servers to Comodo'
- Select 'Click here for more details'



Option A -

Change your domain's authoritative DNS

> Click for more details

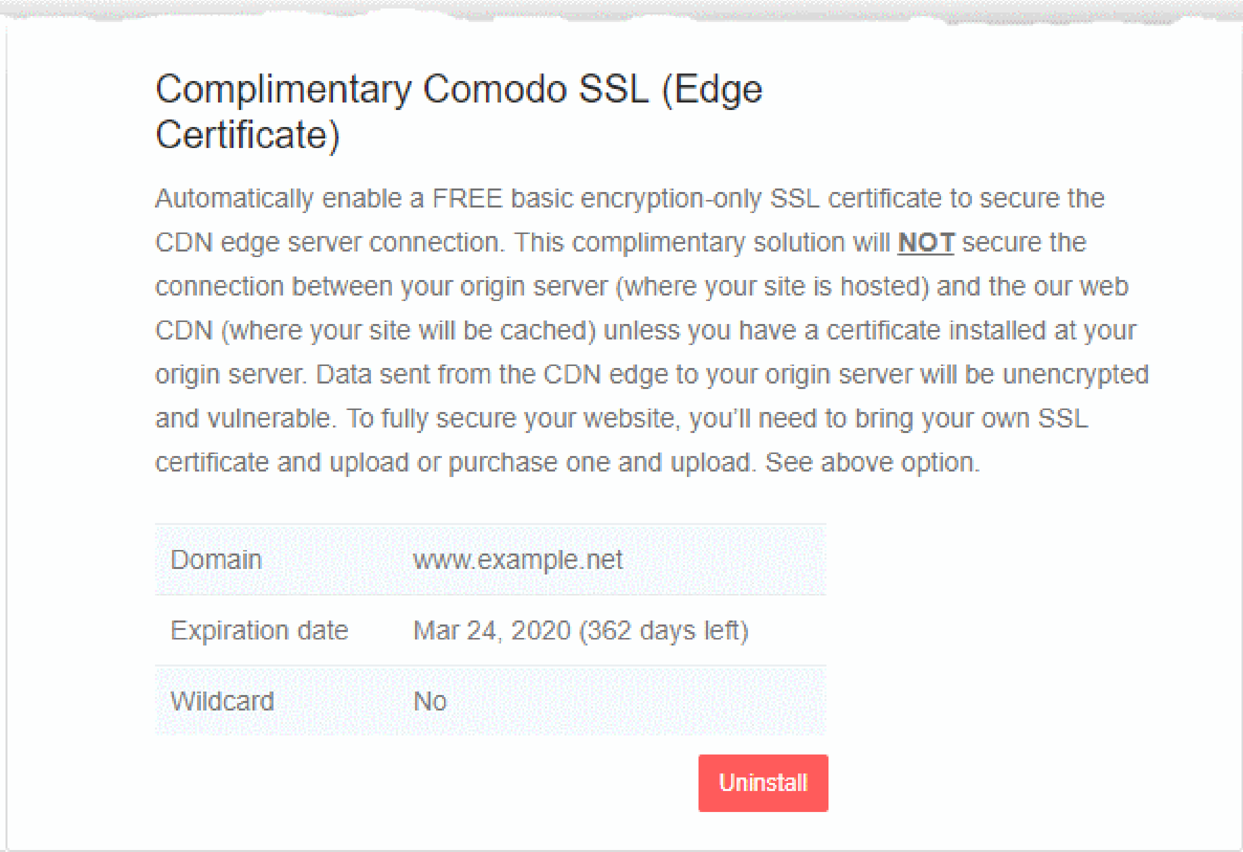
Create CNAME record pointed back to us

> Click for more details

🔧 In order to have FREE SSL Certificate installed to your website you must change your domain's authoritative DNS servers to ours. Click 'Domain' tab to follow the instructions.

Automatically enable a FREE basic encryption-only SSL certificate to secure the CDN edge server connection. This complimentary solution will **NOT** secure the connection between your origin server (where your site is hosted) and the our web CDN (where your site will be cached). Data sent from the CDN edge to your origin server will be unencrypted and vulnerable. To fully secure your website, you'll need to 'Bring your own SSL' option

- Click the 'Activate Basic SSL Now' button
- The process will take a few minutes to complete.
- Once activated, you can see the certificate in 'Settings' > 'SSL', listed under 'Complimentary Comodo SSL (Edge Certificate)'.



Complimentary Comodo SSL (Edge Certificate)

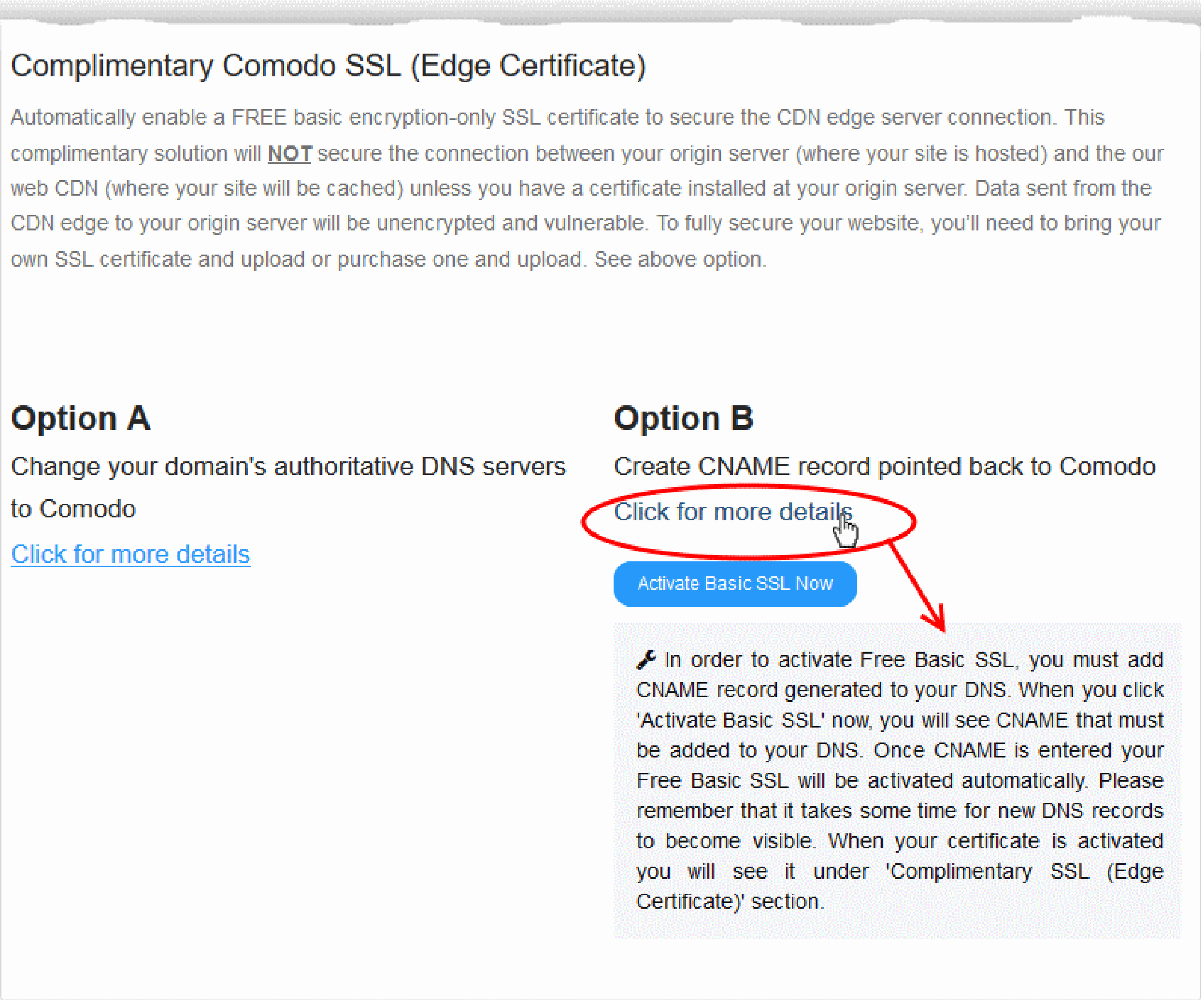
Automatically enable a FREE basic encryption-only SSL certificate to secure the CDN edge server connection. This complimentary solution will **NOT** secure the connection between your origin server (where your site is hosted) and the our web CDN (where your site will be cached) unless you have a certificate installed at your origin server. Data sent from the CDN edge to your origin server will be unencrypted and vulnerable. To fully secure your website, you'll need to bring your own SSL certificate and upload or purchase one and upload. See above option.

Domain	www.example.net
Expiration date	Mar 24, 2020 (362 days left)
Wildcard	No

- The certificate is valid for one year and is set for auto-renewal.
- Note - This certificate encrypts the connection between the CDN servers, which host a copy of your site, and your website visitors.
- It does not encrypt the traffic between your web-server and the CDN edge servers.
- You need to upload your own certificate to encrypt CDN <--> origin site traffic. See '**Upload your own SSL Certificate**' for more details.

Option B - Create a CNAME record which points to Comodo

- Scroll to 'Option B - Create CNAME record pointed back to Comodo'
- Select 'Click here for more details'
- Select 'Click here for more details' beside 'Option B - Create CNAME record pointed back to Comodo'



Complimentary Comodo SSL (Edge Certificate)

Automatically enable a FREE basic encryption-only SSL certificate to secure the CDN edge server connection. This complimentary solution will **NOT** secure the connection between your origin server (where your site is hosted) and the our web CDN (where your site will be cached) unless you have a certificate installed at your origin server. Data sent from the CDN edge to your origin server will be unencrypted and vulnerable. To fully secure your website, you'll need to bring your own SSL certificate and upload or purchase one and upload. See above option.

Option A

Change your domain's authoritative DNS servers to Comodo

Click for more details

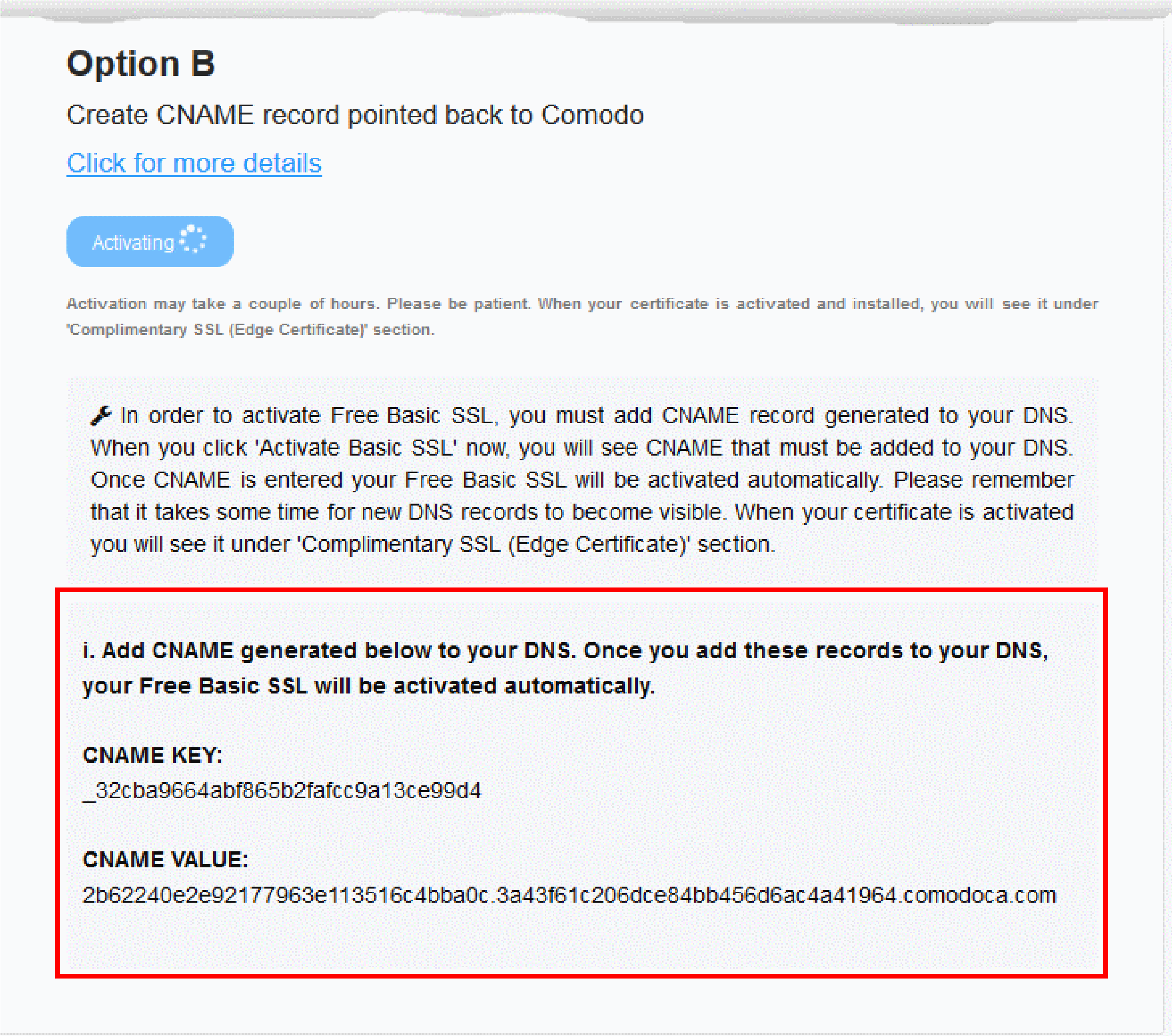
Option B

Create CNAME record pointed back to Comodo

Click for more details

In order to activate Free Basic SSL, you must add CNAME record generated to your DNS. When you click 'Activate Basic SSL' now, you will see CNAME that must be added to your DNS. Once CNAME is entered your Free Basic SSL will be activated automatically. Please remember that it takes some time for new DNS records to become visible. When your certificate is activated you will see it under 'Complimentary SSL (Edge Certificate)' section.

- Click the 'Activate Basic SSL Now' button:



Option B

Create CNAME record pointed back to Comodo

Click for more details

Activation may take a couple of hours. Please be patient. When your certificate is activated and installed, you will see it under 'Complimentary SSL (Edge Certificate)' section.

In order to activate Free Basic SSL, you must add CNAME record generated to your DNS. When you click 'Activate Basic SSL' now, you will see CNAME that must be added to your DNS. Once CNAME is entered your Free Basic SSL will be activated automatically. Please remember that it takes some time for new DNS records to become visible. When your certificate is activated you will see it under 'Complimentary SSL (Edge Certificate)' section.

i. Add CNAME generated below to your DNS. Once you add these records to your DNS, your Free Basic SSL will be activated automatically.

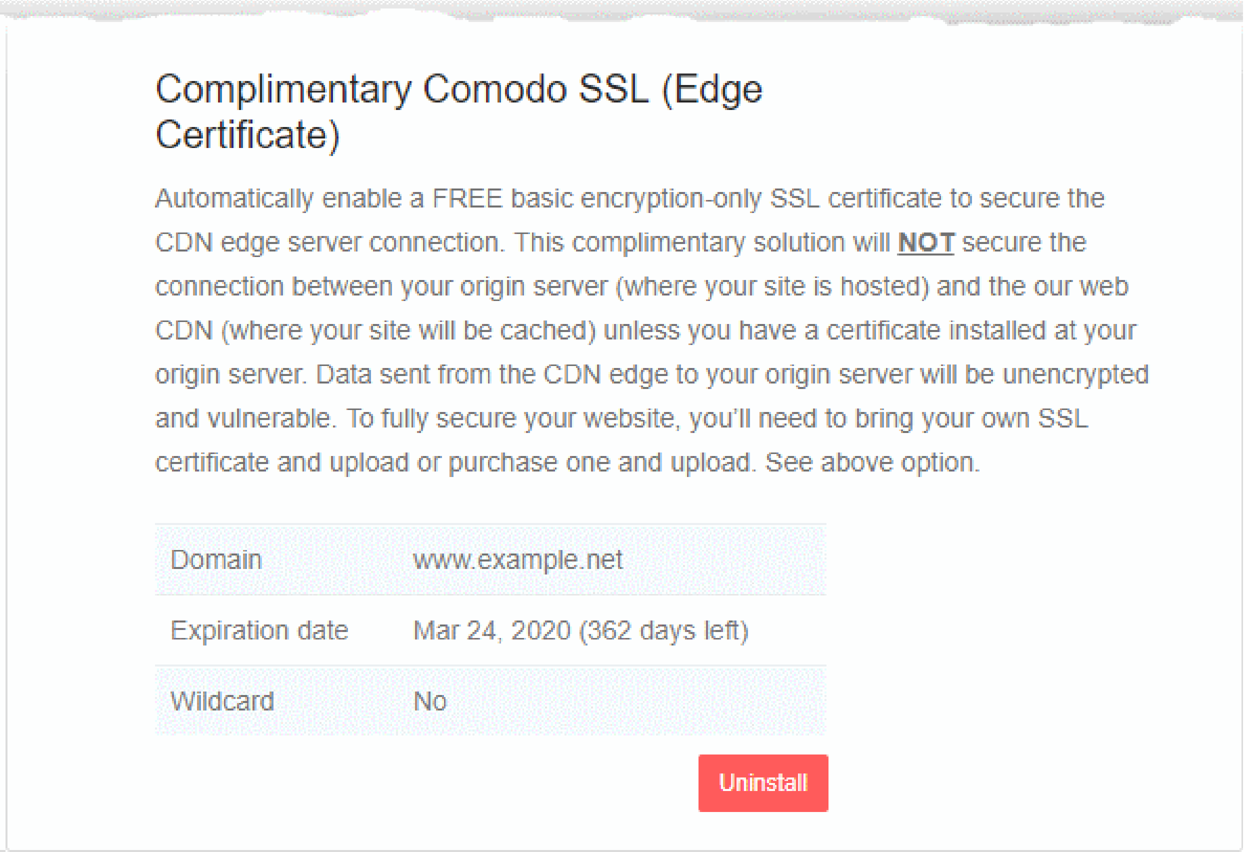
CNAME KEY:
_32cba9664abf865b2fafcc9a13ce99d4

CNAME VALUE:
2b62240e2e92177963e113516c4bba0c.3a43f61c206dce84bb456d6ac4a41964.comodoca.com

cWatch generates a CNAME record for domain control validation.

- Note down the 'CNAME KEY' and 'CNAME VALUE' records
- Go to your website's DNS management page and enter the 'CNAME KEY' and 'CNAME VALUE' records
- If you need more help regarding adding 'CNAME KEY' and 'CNAME VALUE' records, visit **https://support.google.com/a/topic/1615038?hl=en**
- After the CNAME records are added to your domain's DNS settings, the certificate will be activated and deployed to the edge servers. It may take up to two hours to complete.

Once activated, you can see the certificate listed under 'Complimentary Comodo SSL (Edge Certificate)'.



Complimentary Comodo SSL (Edge Certificate)

Automatically enable a FREE basic encryption-only SSL certificate to secure the CDN edge server connection. This complimentary solution will **NOT** secure the connection between your origin server (where your site is hosted) and the our web CDN (where your site will be cached) unless you have a certificate installed at your origin server. Data sent from the CDN edge to your origin server will be unencrypted and vulnerable. To fully secure your website, you'll need to bring your own SSL certificate and upload or purchase one and upload. See above option.

Domain	www.example.net
Expiration date	Mar 24, 2020 (362 days left)
Wildcard	No

- Note - This certificate encrypts the connection between the CDN servers, which host a copy of your site, and your website visitors.
- It does not encrypt the traffic between your web-server and the CDN servers.
- You need to upload your own certificate to encrypt CDN <--> origin site traffic. See 'Upload your own SSL Certificate' for more details. See '**Upload your own SSL Certificate**' for more details.

Configure Malware Scans

- Select the website name then click 'Scan' > ‘Server Side Scan’ > 'Overview'
- You need to upload the cWatch scanner file to your site to activate malware scans.
- Once done, cWatch will run scheduled scans on all files hosted on the website. You can also run manual scans if required.

You can upload the file automatically or manually:

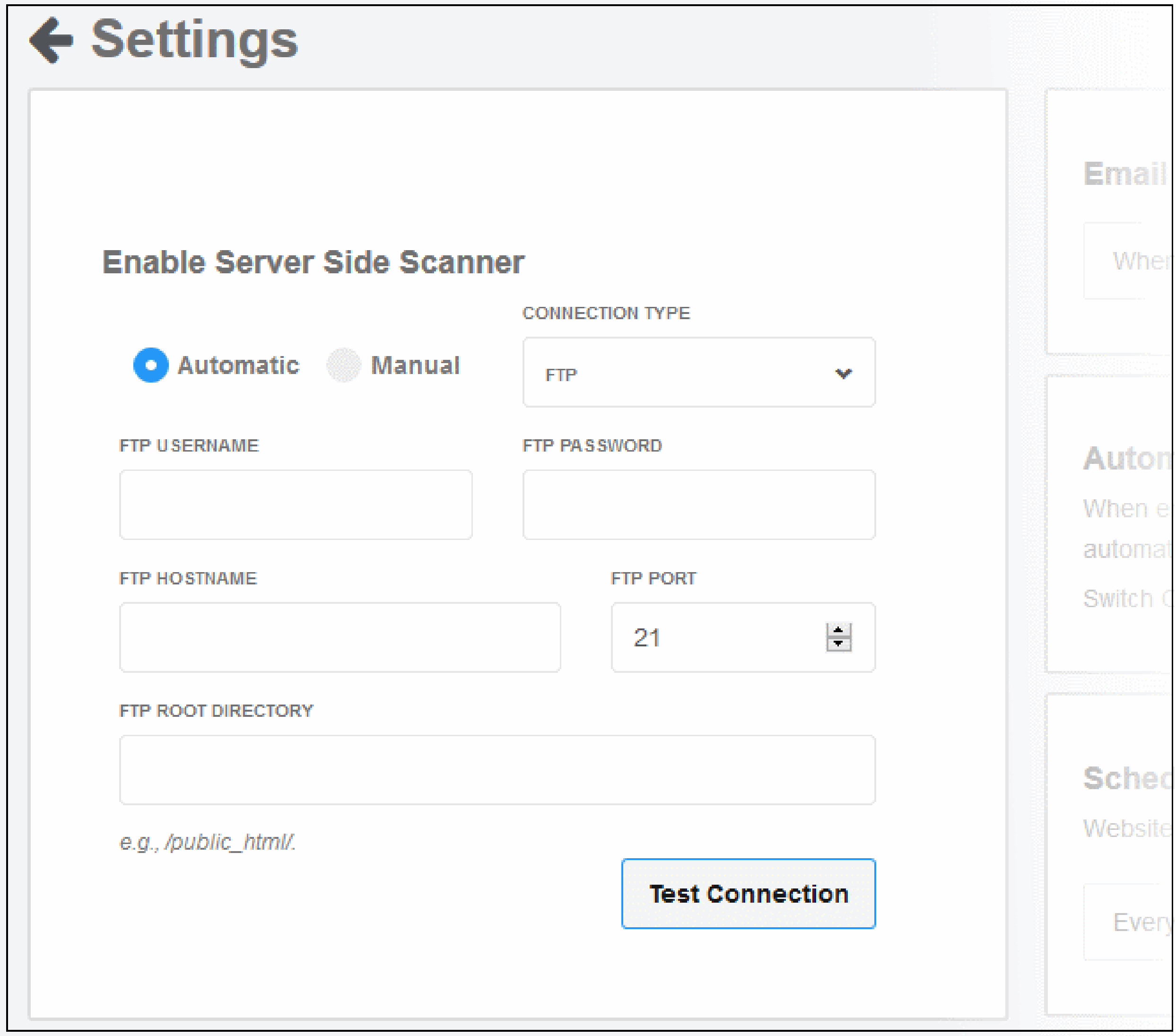
- **Automatically** – need to provide FTP details
- **Manually** – download the agent file then place it on your site

Automatic Configuration

You need to provide FTP details for your site to enable automatic configuration. cWatch will use the details to upload the scanner agent.

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Server Side Scan' > 'Overview'
- Click 'Enable Scanner'

- Select 'Automatic' in the server side scanner box:



Settings

Enable Server Side Scanner

● Automatic ○ Manual

CONNECTION TYPE: FTP

FTP USERNAME

FTP PASSWORD

FTP HOSTNAME

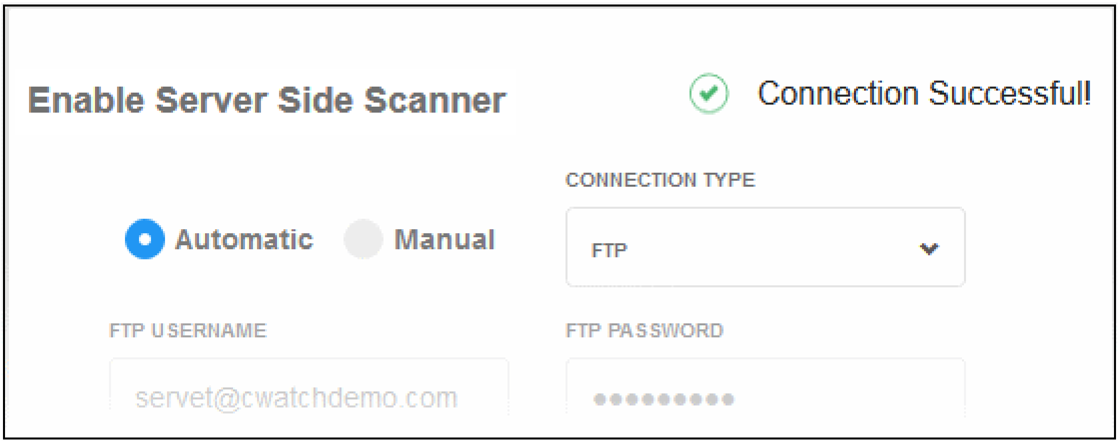
FTP PORT: 21

FTP ROOT DIRECTORY

e.g., /public_html/.

FTP / s/FTP Settings - Table of Parameters	
Parameter	**Description**
Connection Type	Select FTP or sFTP as required.
FTP Username / FTP Password	Enter the username and password of your FTP server
Hostname	IP or hostname of your web-server
Port	By default, FTP / sFTP connections use ports 21 and 22 respectively. Change this if your web-server uses different ports for FTP connections.
FTP Directory	The path of your web root folder. For example '/public_html/

- **Test Connection** - Click this after completing all fields. cWatch will check your settings and, if successful, show a confirmation message as follows:



Enable Server Side Scanner

✓ Connection Successful!

● Automatic ○ Manual

CONNECTION TYPE: FTP

FTP USERNAME: servet@cwatchdemo.com

FTP PASSWORD: ●●●●●●●●●●

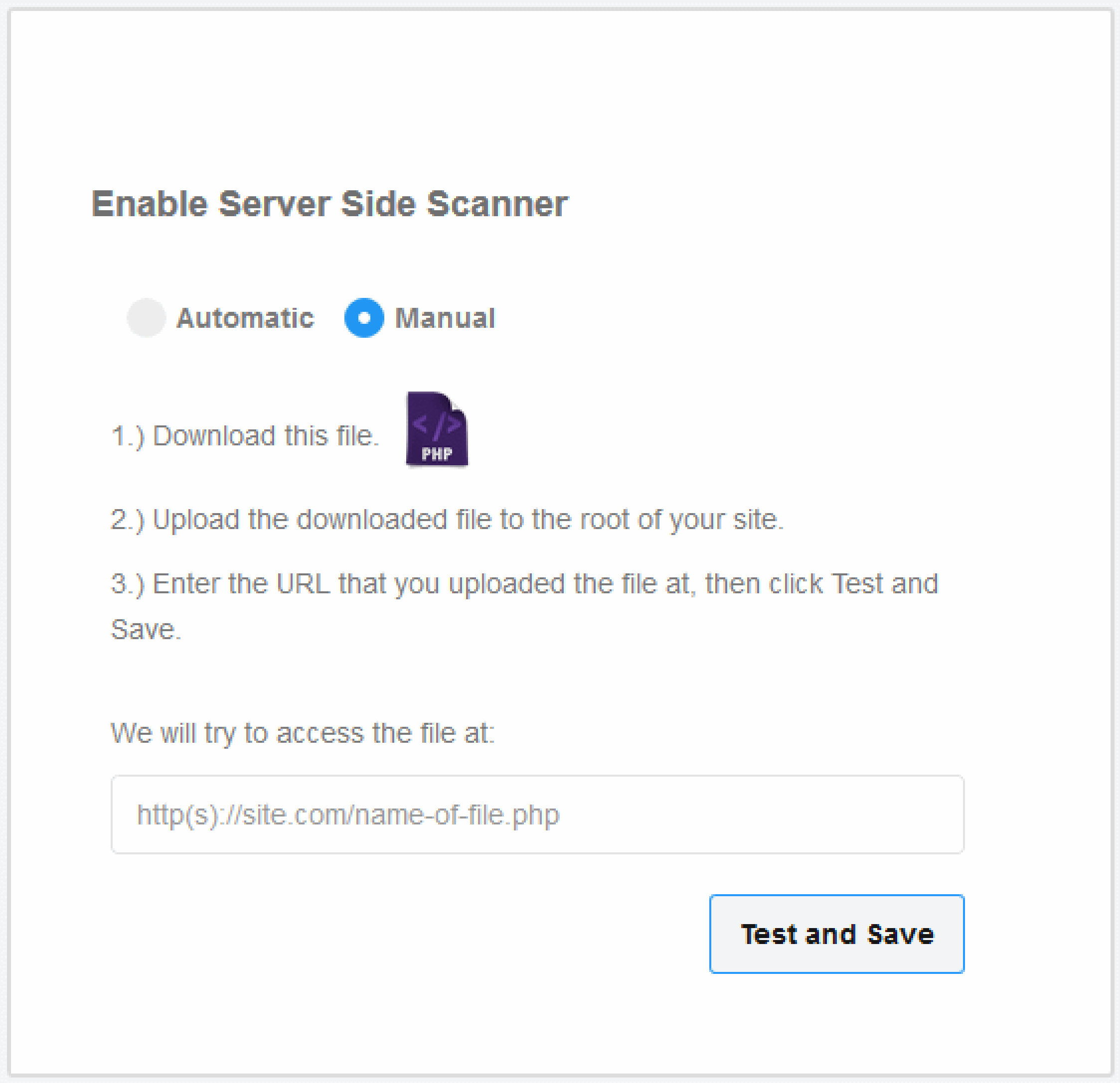
- Click 'Save'

cWatch will upload the agent to your site. You will see 'Server side scanner is enabled' if everything is successful.

Manual Configuration

Manual configuration means downloading the agent file then copying it to your site. You need to place the file in a publicly accessible location so we can authenticate it and start the scans.

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Server Side Scan' > 'Overview'
- Click 'Enable Scanner'
- Select ‘Manual’ in the server side scanner box:



Enable Server Side Scanner

○ Automatic ● Manual

1.) Download this file.

2.) Upload the downloaded file to the root of your site.

3.) Enter the URL that you uploaded the file at, then click Test and Save.

We will try to access the file at:

http(s)://site.com/name-of-file.php

- Download the PHP file in step 1
- Upload the file to the root folder of your website. The file should be publicly accessible.
- Enter the URL of the uploaded file in the text field.
- Click 'Test and Save' to run the check.
- The scans will start after successfully completing the check.

Configure CDN Settings

- The content delivery network (CDN) improves the performance and security of your websites.
- Make sure you have configured the DNS settings of your website to use the CDN. See **DNS Configuration** for more information.
- You can also configure DNS settings at 'CDN' > 'Settings' > 'Activation'. See **https://help.comodo.com/topic-285-1-848-13908-Activate-CDN-for-a-Website.html** if you want help with this.

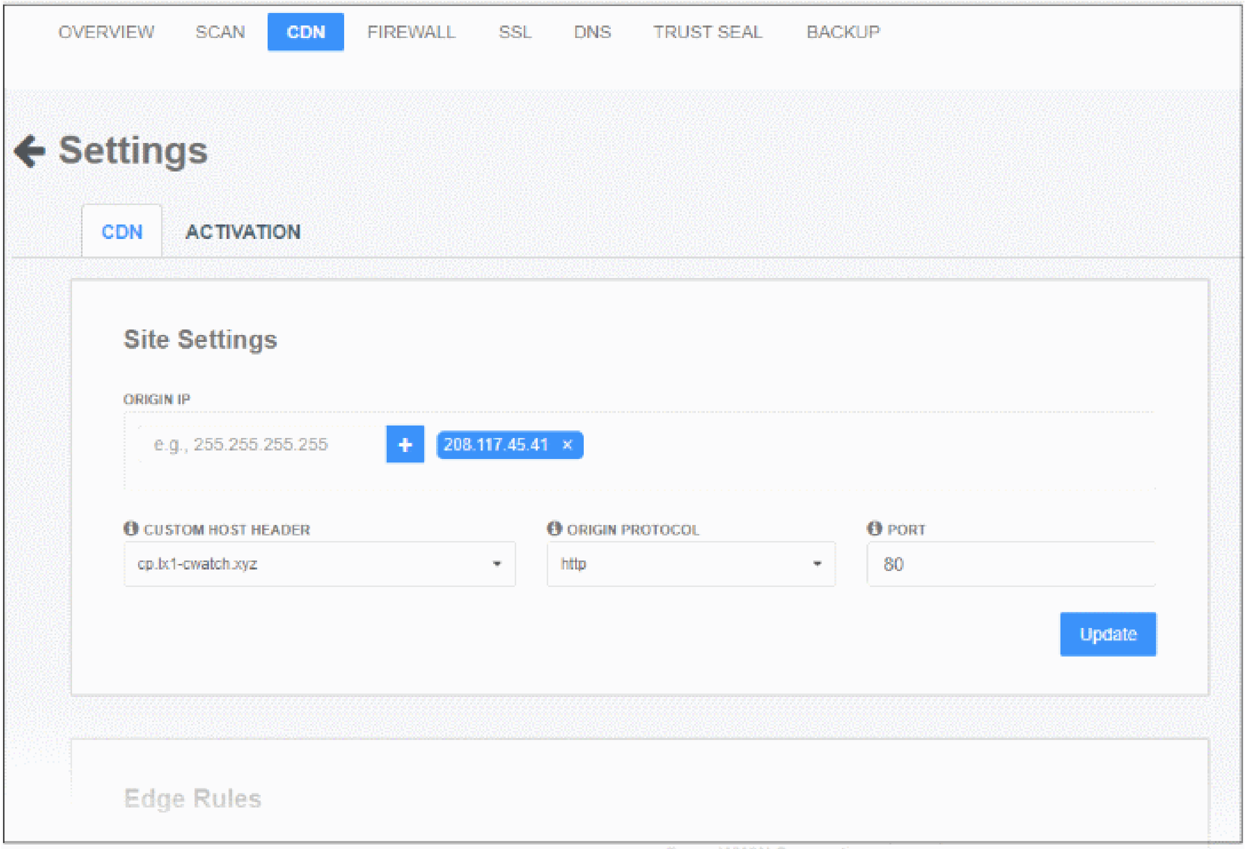
Once configured, the CDN service will:

- Accelerate performance by serving your website from the data center closest to your visitor’s location.
- Forward event logs to the Comodo CSOC team who will monitor your traffic for threats.
- Enable Comodo web application firewall (CWAF) protection for your domains. The CSOC team constantly

improves the firewall rules to provide cutting edge protection for our customers.

Configure CDN Settings

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click 'CDN' > 'Settings' > 'CDN'



Click the following links for help with each box on the settings screen:

- **Site Settings**
- **Edge Rules**
- **Cache Settings**
- **Purge Files**
- **Quick Configuration**

Site Settings

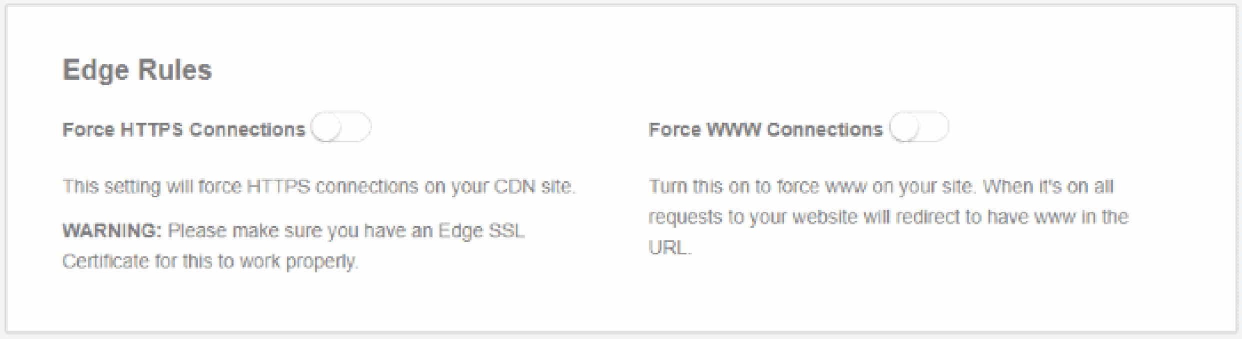
- **Origin IP** – The website's IP address. The CDN will collect the site's content from this IP.
  - Enter the site's IP then click the '+' button. You can add multiple origin addresses. The CDN will load balance from the list of origins.
- **Custom Host Header** – Enter the domain name of the origin website. For example, simply enter **www.yourwebsite.com**

  Background – If you don't complete the custom host header field, then the CDN will simply retrieve the default website at the origin IP. While this is OK if there is only one site hosted on the IP, it can be problematic if the IP hosts multiple sites. By specifying your domain, you tell the CDN exactly which website to collect.

- **Origin Protocol** - Select whether the site is hosted over HTTP or HTTPS. Choose the https or http version of your URL as appropriate.
- **Port** – The port number on the site that the CDN should connect to.

Click 'Update' to save your changes.

Edge Rules



Edge Rules

Force HTTPS Connections

This setting will force HTTPS connections on your CDN site.

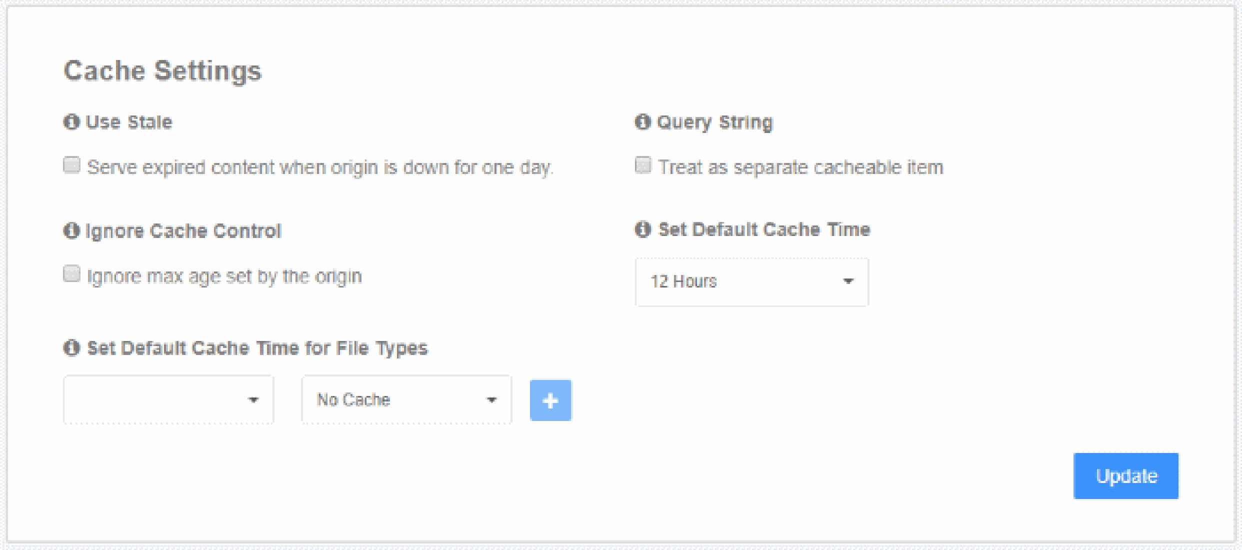
WARNING: Please make sure you have an Edge SSL Certificate for this to work properly.

Force WWW Connections

Turn this on to force www on your site. When it's on all requests to your website will redirect to have www in the URL.

- **Force HTTPS Connections** – Ensures your site is only ever served over a secure, HTTPS, connection. Any requests made over HTTP will be converted to HTTPS. Make sure that you have uploaded your SSL certificate to the CDN edge servers. See **SSL Configuration** for help to do this.
- **Force WWW Connections** – Resolves all requests for your domain to the www version. For example, requests for **https://your-website.com** will be redirected to **https://www.your-website.com**

Cache Settings



Cache Settings

Use Stale

□ Serve expired content when origin is down for one day.

Query String

□ Treat as separate cacheable item

Ignore Cache Control

□ Ignore max age set by the origin

Set Default Cache Time

12 Hours

Set Default Cache Time for File Types

No Cache

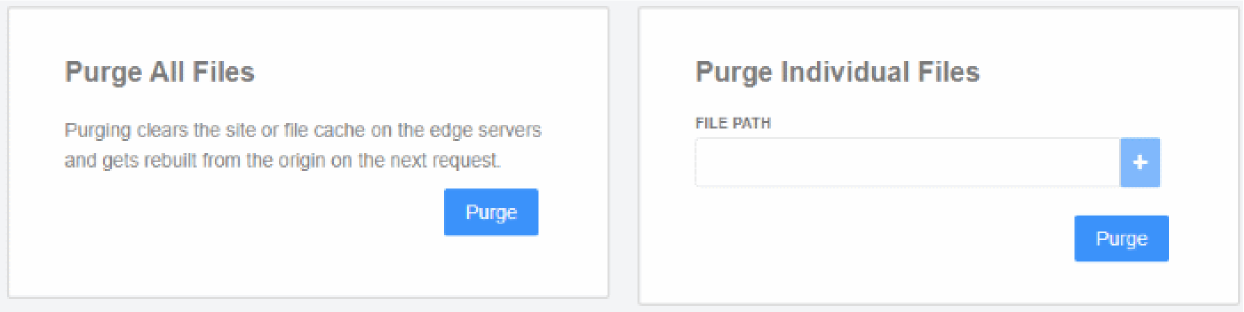
- **Use Stale** – Serve cached-but-expired content to visitors if your site is not reachable for 24 hours or more. This is useful to ensure you keep a web-presence if your server is hit by problems.
- **Query String** - Web-pages with a query string (e.g.'?q=something') will be cached as separate files. CDN updates the cached files whenever the original pages are updated.

- **Ignore Cache Control** – Enable this to invalidate cache settings on the origin. Selecting this option will automatically disable 'Use Stale' setting above.
- **Set Default Cache Time** - Define how long content fetched from your web servers should remain in the CDN cache. Cached content is used to accelerate site loading times for your visitors.

  The CDN will collect refreshed content from your site when this period expires.
- **Set Default Cache Time for File Types** – Define how long files should be cached before they are forced to request a new copy from your origin.
  - Select the file type from the first drop-down and set the cache time in the second. Click '+' to add the file type. Repeat to add more file types.

Click 'Update' to save your changes.

Purge Files



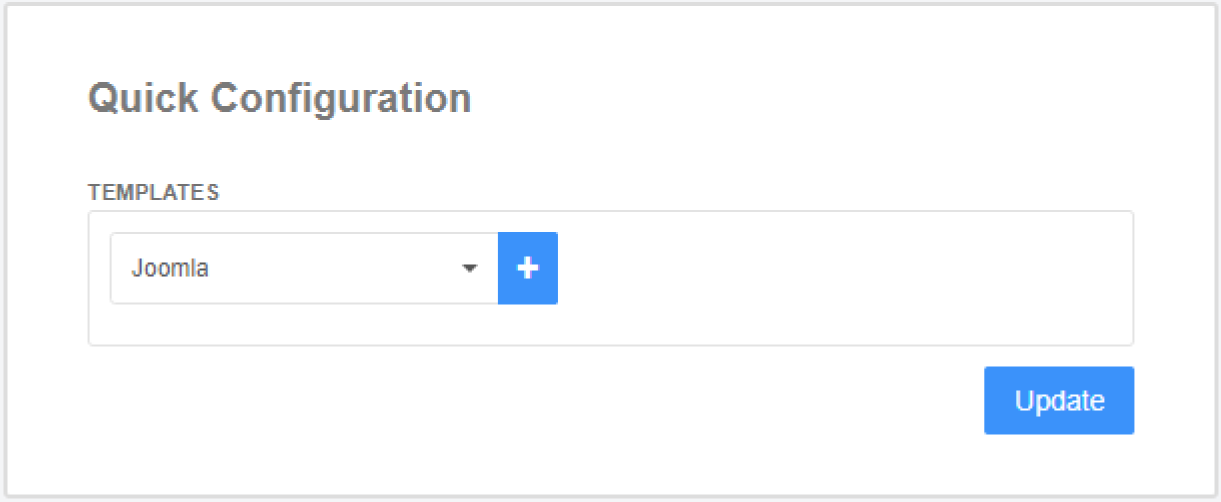
Purge All Files

Purging clears the site or file cache on the edge servers and gets rebuilt from the origin on the next request.

- **Purge All Files** - Manually remove all cached files so the CDN is forced to check your website the next time the files are requested.
- **Purge Individual Files** - Remove specific files from the cache so that the CDN is forced to check your website the next time these files are requested.
  - Enter the URI of the file in the box then click the blue '+' button
  - Repeat the process to add more files
  - Click 'Purge'

Quick Configuration

Tell cWatch the content management system (CMS) used to develop your site. Doing so helps accelerate CDN setup and performance. While cWatch supports all content management systems, quick configuration currently only supports Joomla and WordPress.


Quick Configuration

TEMPLATES

Joomla

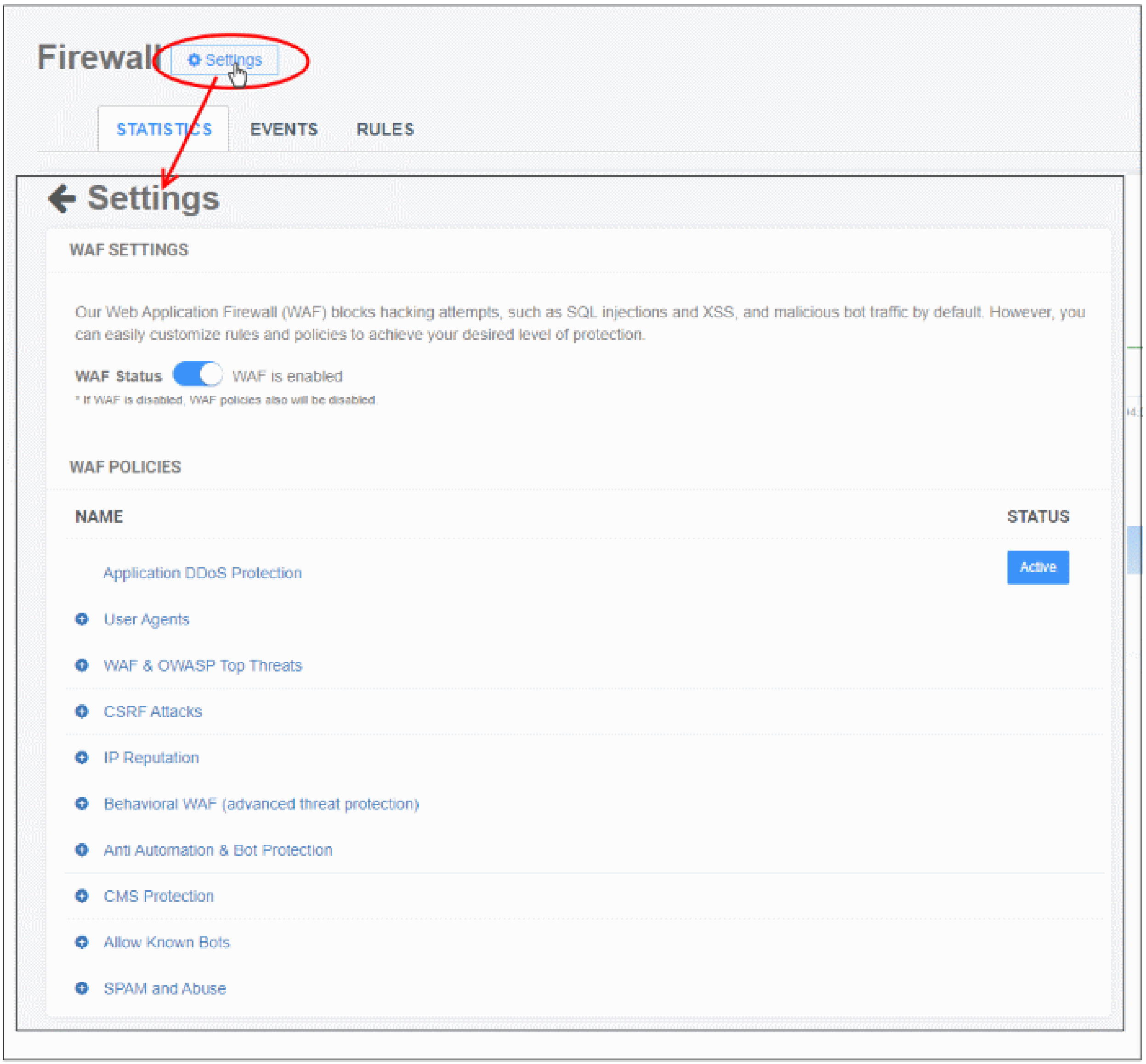
- Select a CMS type and click the '+' button. Repeat to add more types.
- Click 'Update' to save your settings.

Configure WAF Policies

- Select a website from the drop-down at top-left and choose 'Firewall'
- Click the 'Settings' button
- cWatch ships with built-in firewall policies to deal with a wide range of attacks, including SQL injections, bot traffic and more.
- Each policy contains a set of firewall rules to filter traffic and take preventative measures when required. These rules are non-editable.
- You can enable or disable individual rules as required.

Configure WAF settings

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Firewall' tab
- Click 'Settings' to open the 'WAF Settings' page



Settings

WAF SETTINGS

Our Web Application Firewall (WAF) blocks hacking attempts, such as SQL injections and XSS, and malicious bot traffic by default. However, you can easily customize rules and policies to achieve your desired level of protection.

WAF Status ● WAF is enabled

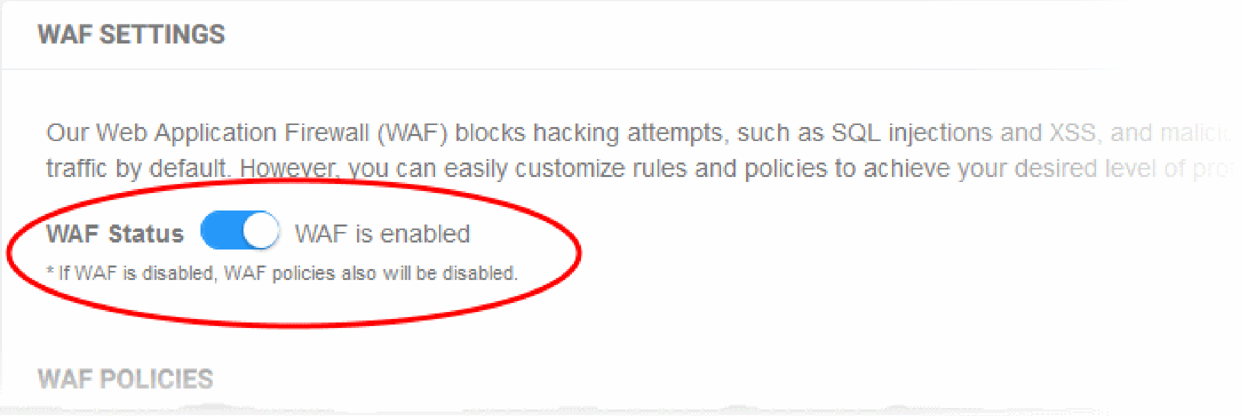
* If WAF is disabled, WAF policies also will be disabled.

WAF POLICIES

NAME	STATUS
Application DDoS Protection	Active
+ User Agents	
+ WAF & OWASP Top Threats	
+ CSRF Attacks	
+ IP Reputation	
+ Behavioral WAF (advanced threat protection)	
+ Anti Automation & Bot Protection	
+ CMS Protection	
+ Allow Known Bots	
+ SPAM and Abuse	

WAF Settings

- Use the switch beside 'WAF Status' to enable or disable the firewall:



WAF SETTINGS

Our Web Application Firewall (WAF) blocks hacking attempts, such as SQL injections and XSS, and malici traffic by default. However, you can easily customize rules and policies to achieve your desired level of pro

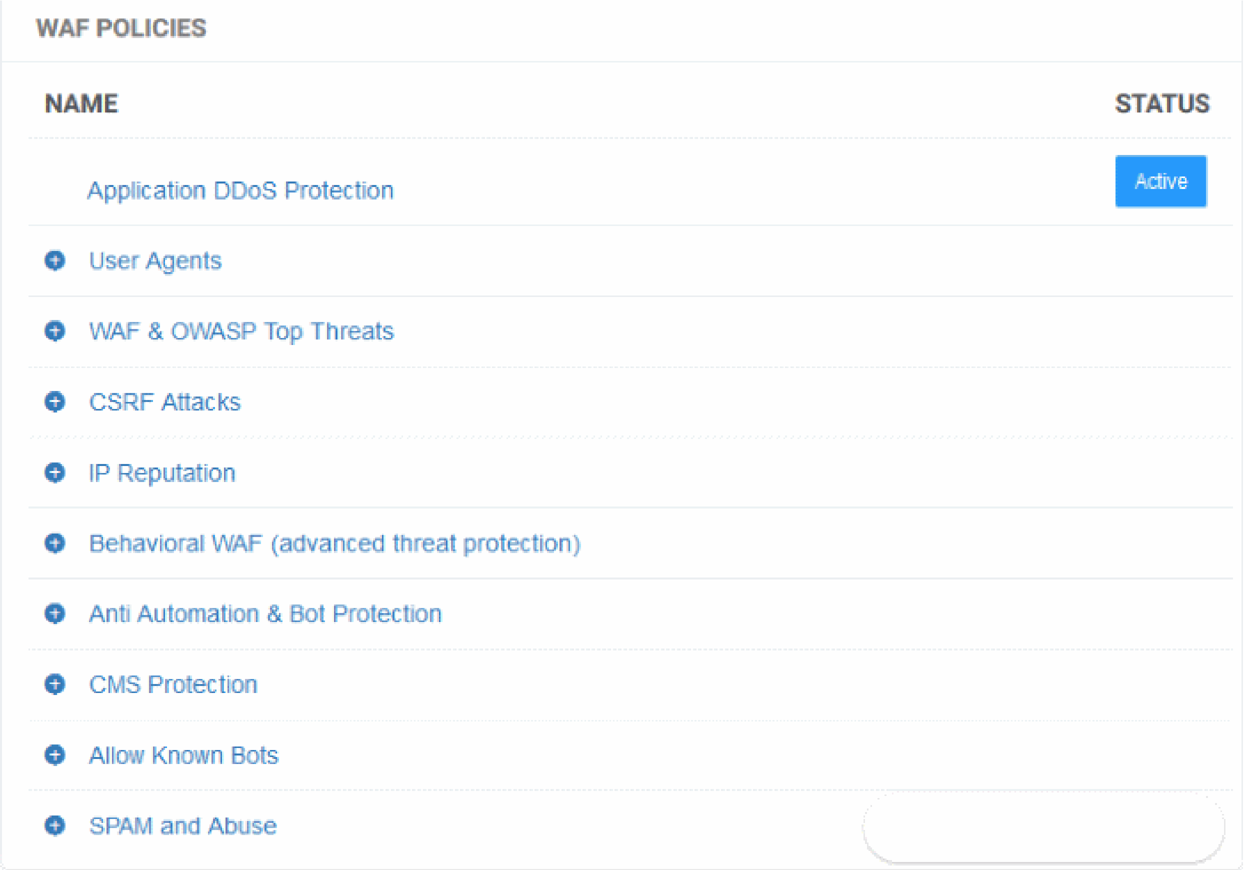
WAF Status ● WAF is enabled

* If WAF is disabled, WAF policies also will be disabled.

WAF POLICIES

WAF Polices

- This area shows all firewall policies that have been saved on your account.
- Click the '+' symbol to view the constituent rules in a policy. You can enable / disable rules as required.



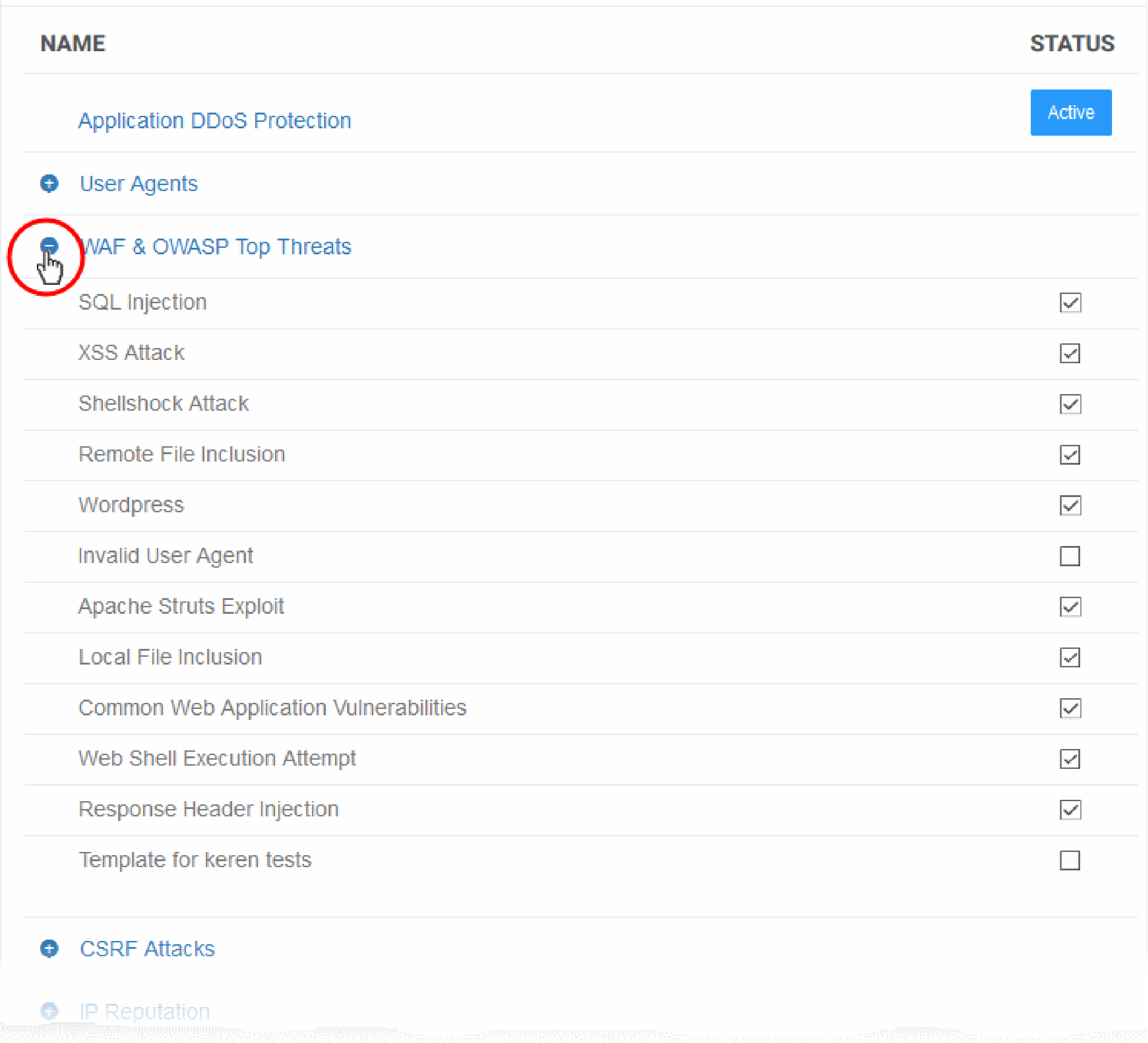
WAF POLICIES

NAME	STATUS
Application DDoS Protection	Active
User Agents	
WAF & OWASP Top Threats	
CSRF Attacks	
IP Reputation	
Behavioral WAF (advanced threat protection)	
Anti Automation & Bot Protection	
CMS Protection	
Allow Known Bots	
SPAM and Abuse	

- **Status** - Indicates whether the firewall is enabled or not. 'Passive' means the firewall is disabled.

Enable / disable firewall rule(s)

- Click a firewall category to expand / collapse its subcategories:



NAME	STATUS
Application DDoS Protection	Active
⊕ User Agents	
⊖ WAF & OWASP Top Threats	
SQL Injection	☑
XSS Attack	☑
Shellshock Attack	☑
Remote File Inclusion	☑
Wordpress	☑
Invalid User Agent	☐
Apache Struts Exploit	☑
Local File Inclusion	☑
Common Web Application Vulnerabilities	☑
Web Shell Execution Attempt	☑
Response Header Injection	☑
Template for keren tests	☐
⊕ CSRF Attacks	
⊕ IP Reputation	

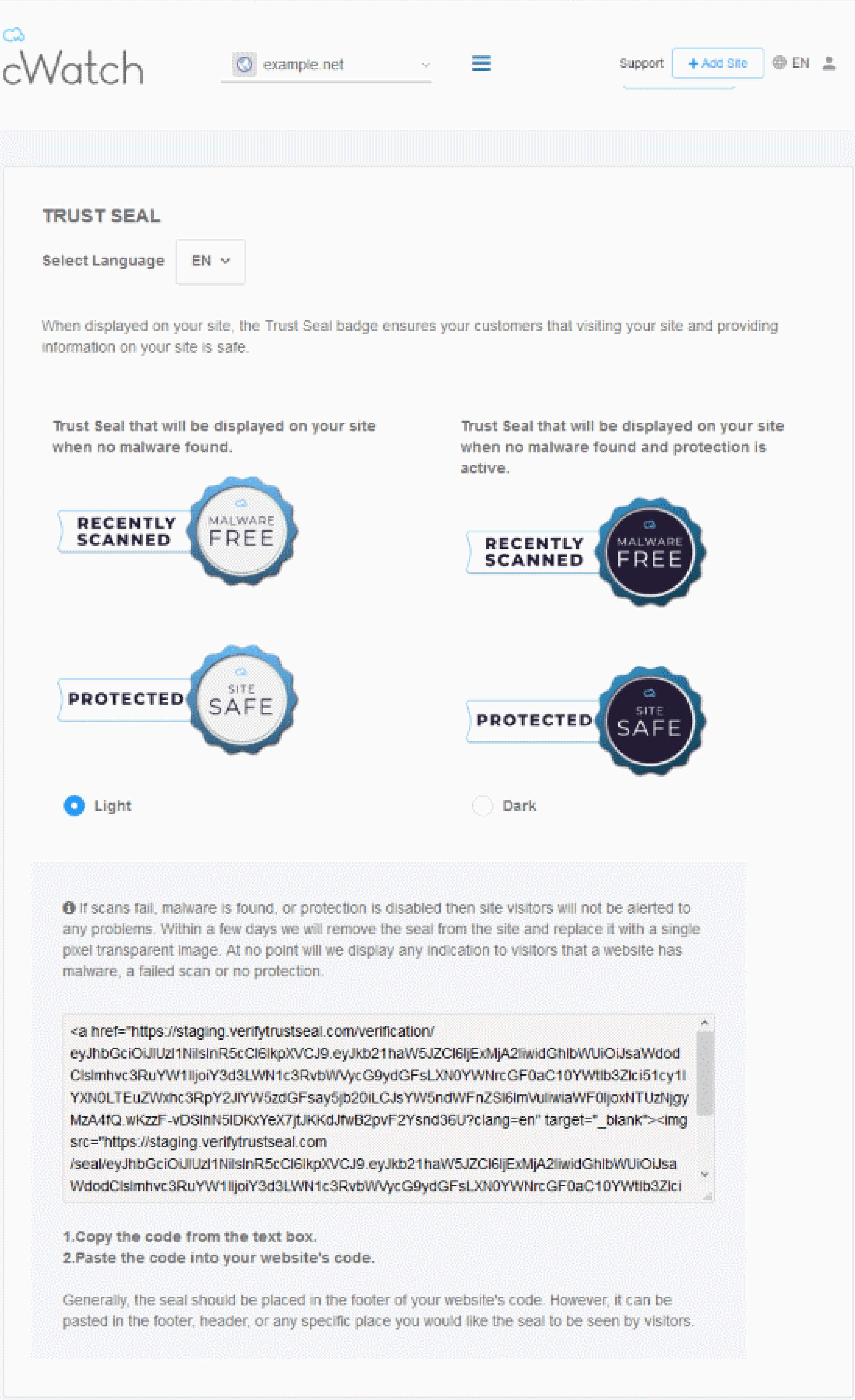
- Use the check-boxes to enable or disable a particular rule.
- Changes are auto-saved and deployed to the site in approximately a minute.

Add Trust Seal to Your Sites

- Select a site from the drop-down at top-left then choose 'Trust Seal'
- The trust seal is a website badge that proves your site is malware free and is protected by one of the leaders in online security.
- This helps build the trust you so often need to convert website visitors into paying customers.
- The site seal is available in multiple languages.

Add the trust seal to your site

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Trust Seal' tab



TRUST SEAL

Select Language EN

When displayed on your site, the Trust Seal badge ensures your customers that visiting your site and providing information on your site is safe.

Trust Seal that will be displayed on your site when no malware found.

Trust Seal that will be displayed on your site when no malware found and protection is active.

● Light ○ Dark

If scans fail, malware is found, or protection is disabled then site visitors will not be alerted to any problems. Within a few days we will remove the seal from the site and replace it with a single pixel transparent image. At no point will we display any indication to visitors that a website has malware, a failed scan or no protection.

```
<a href="https://staging.verifytrustseal.com/verification/
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkb21haW5JZCI6IjExMjA2IiwidGhlbWUiOiJsaWdod
CIsImhvc3RuYW1lIjoiY3d3LWN1c3RvbWVycG9ydGFsLXN0YWNrcGF0aC10YWtlb3Zlci51cy1l
YXN0LTEuZWxhc3RpY2JlYW5zdGFsay5jb20iLCJsYW5ndWFnZSI6ImVuIiwiaWF0IjoxNTUzNjgy
MzA4fQ.wKzzF-vDSIhN5IDKxYeX7jtJKKdJfwB2pvF2Ysnd36U?clang=en" target="_blank"><img
src="https://staging.verifytrustseal.com
/seal/eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkb21haW5JZCI6IjExMjA2IiwidGhlbWUiOiJsa
WdodCIsImhvc3RuYW1lIjoiY3d3LWN1c3RvbWVycG9ydGFsLXN0YWNrcGF0aC10YWtlb3ZIci
```

1.Copy the code from the text box.
2.Paste the code into your website's code.

Generally, the seal should be placed in the footer of your website's code. However, it can be pasted in the footer, header, or any specific place you would like the seal to be seen by visitors.

- There are two types of seal - 'Malware Free' and 'Protected'. The type shown on your site depends on the following conditions:

- '**Malware Free**' - Shown if your site is not blacklisted and has no malware.
- '**Protected**' - Shown if your site is not blacklisted, has no malware, and both the CDN and Web Application Firewall (WAF) are active.

Here are some sample scenarios:

Trust Seal Conditions						
Blacklisted	Malware Scanner	Last Malware Scan	CDN		WAF	Trust Seal shown
			CName	A Record		
No	Enabled	Clean	Yes	Yes	Yes	'Protected' Trust Seal
No	Enabled	Clean	No	Yes	Yes	'Protected' Trust Seal
No	Enabled	Clean	No	No	Yes	'Malware Free' Trust Seal
No	Enabled	Clean	No	No	No	'Malware Free' Trust Seal

- No negative messaging is shown if your site fails a scan/appears on a blacklist. After a grace period, the seal will simply disappear, replaced by a transparent single-pixel image. The seal will reappear when the issues are fixed.
- Select the language which should be used in the trust seal
- Follow the instructions in the settings page to add the seal to your web pages.

Back up your Website

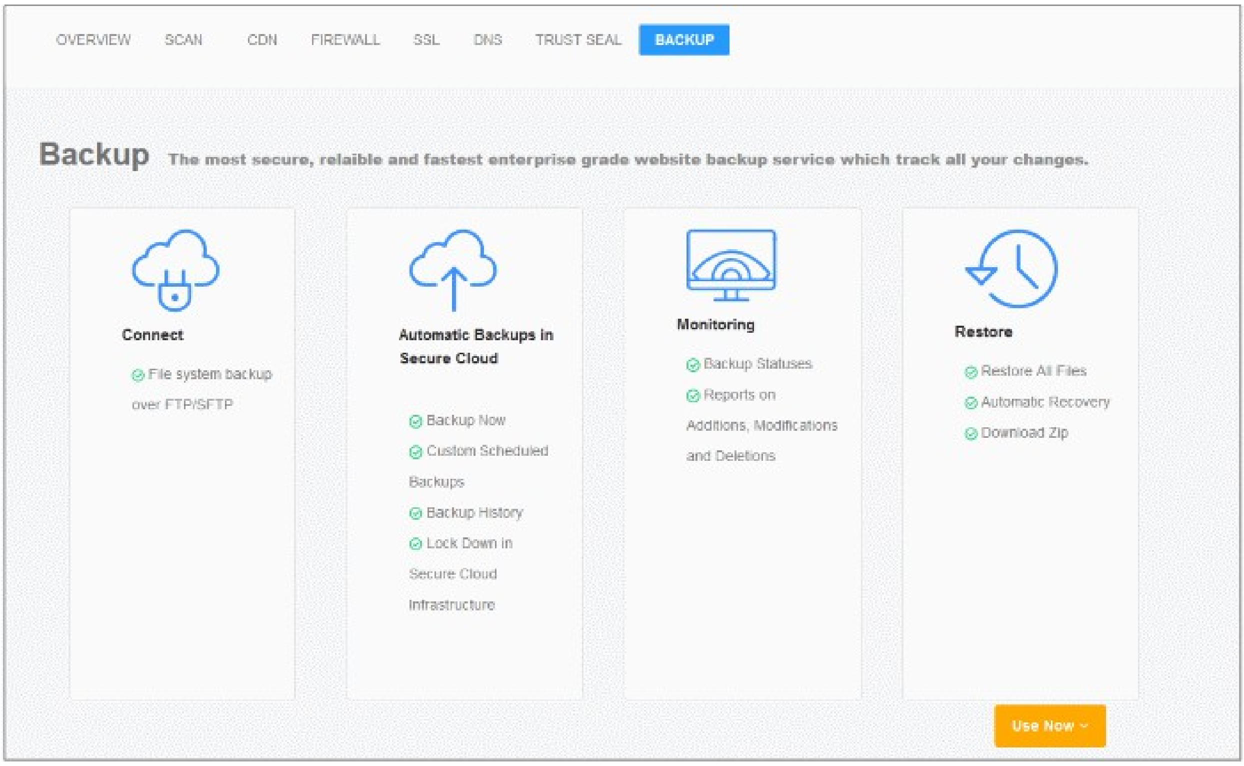
- cWatch backup is a robust disaster recovery solution which automatically creates a backup of your website at regular intervals. Using state of the art storage and security technologies, the service lets you quickly and easily restore your site in the event of catastrophic data loss.
- The backup service is an add-on available after you have purchased a cWatch license.
- Each backup license covers one site. You must purchase separate licenses for each site you want to backup.

See the following sections for help with:

- **Subscribe for a Backup License**
- **Configure Backup Settings**
- **Manual Backup and Restore**

Purchase a Backup License

- Select the target website from the menu at top-left
- Click the 'Backup' tab
- Click 'Use Now' at bottom-left:



Backup The most secure, relaible and fastest enterprise grade website backup service which track all your changes.

Connect

- File system backup over FTP/SFTP

Automatic Backups in Secure Cloud

- Backup Now
- Custom Scheduled Backups
- Backup History
- Lock Down in Secure Cloud Infrastructure

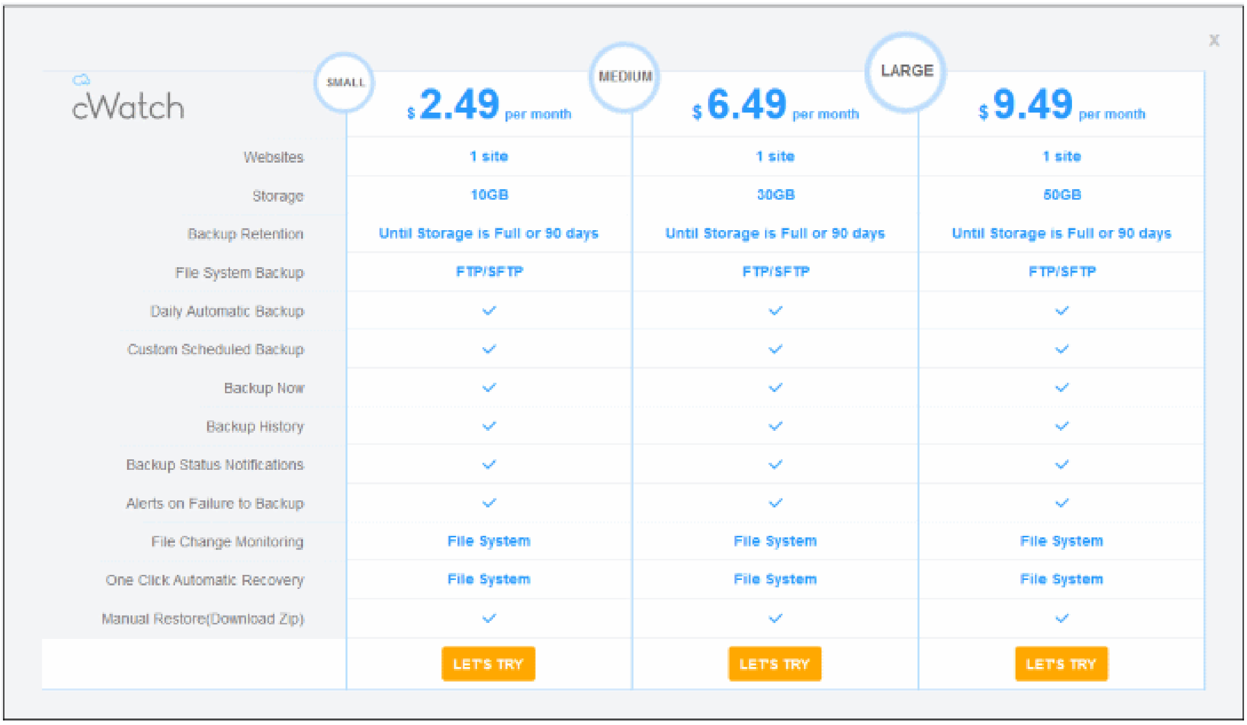
Monitoring

- Backup Statuses
- Reports on Additions, Modifications and Deletions

Restore

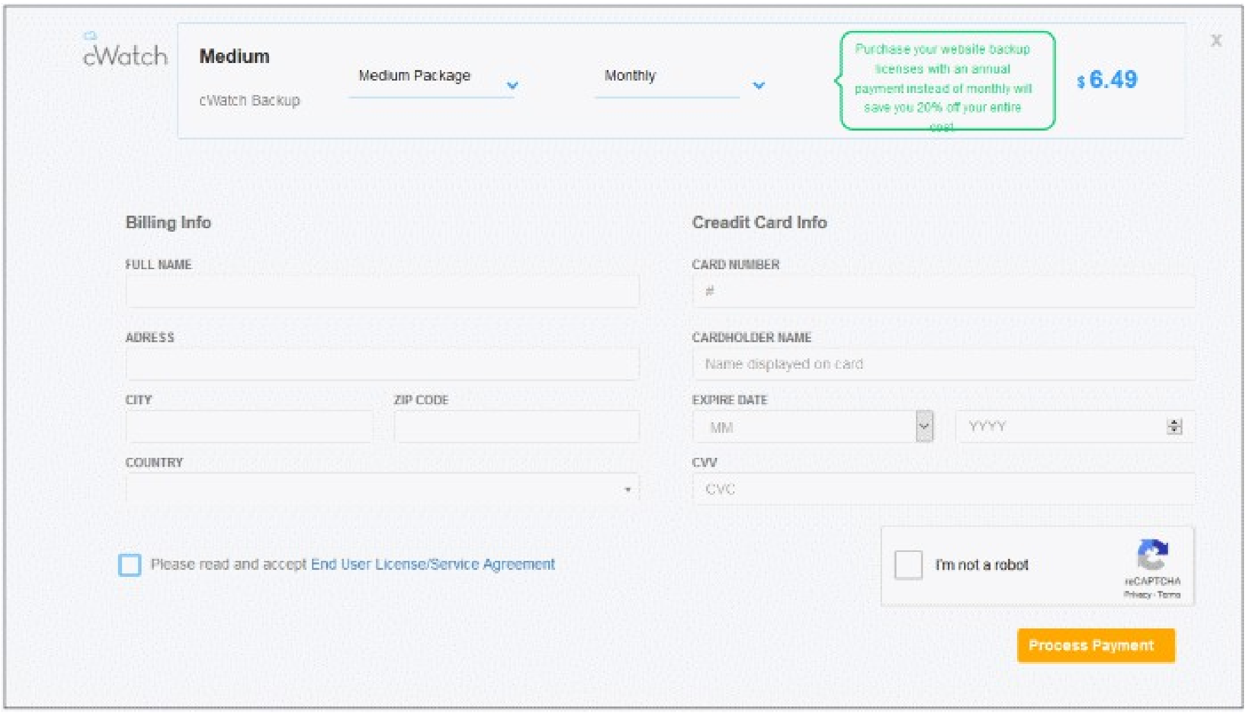
- Restore All Files
- Automatic Recovery
- Download Zip

- Click ‘Let’s Try’ under the plan you want to purchase:



cWatch	SMALL $2.49 per month	MEDIUM $6.49 per month	LARGE $9.49 per month
Websites	1 site	1 site	1 site
Storage	10GB	30GB	50GB
Backup Retention	Until Storage is Full or 90 days	Until Storage is Full or 90 days	Until Storage is Full or 90 days
File System Backup	FTP/SFTP	FTP/SFTP	FTP/SFTP
Daily Automatic Backup	✓	✓	✓
Custom Scheduled Backup	✓	✓	✓
Backup Now	✓	✓	✓
Backup History	✓	✓	✓
Backup Status Notifications	✓	✓	✓
Alerts on Failure to Backup	✓	✓	✓
File Change Monitoring	File System	File System	File System
One Click Automatic Recovery	File System	File System	File System
Manual Restore(Download Zip)	✓	✓	✓
	LET'S TRY	LET'S TRY	LET'S TRY

- Enter your payment information in the license order form.
- Remember to agree to the EULA and tick the captcha box:



cWatch

Medium

cWatch Backup

Medium Package

Monthly

Purchase your website backup licenses with an annual payment instead of monthly will save you 20% off your entire cost

$6.49

x

Billing Info

FULL NAME

ADRESS

CITY

ZIP CODE

COUNTRY

Creadit Card Info

CARD NUMBER

#

CARDHOLDER NAME

Name displayed on card

EXPIRE DATE

MM

YYYY

CVV

CVC

□ Please read and accept End User License/Service Agreement

□ I'm not a robot

Process Payment

- Click 'Process Payment' to submit your order
- Repeat the process to purchase licenses for other sites on your account.
  - We will notify you when your license is due for renewal, or when you are approaching your storage limit.
- Next, **configure your backup**

Configure Your Backup

- The backup settings area is where you establish the connection between your web host server and the backup server.
- You can also configure backup schedule, exclusions, and notifications.
- Once connected, your site files and databases are backed as per your schedule

Open the backup settings page

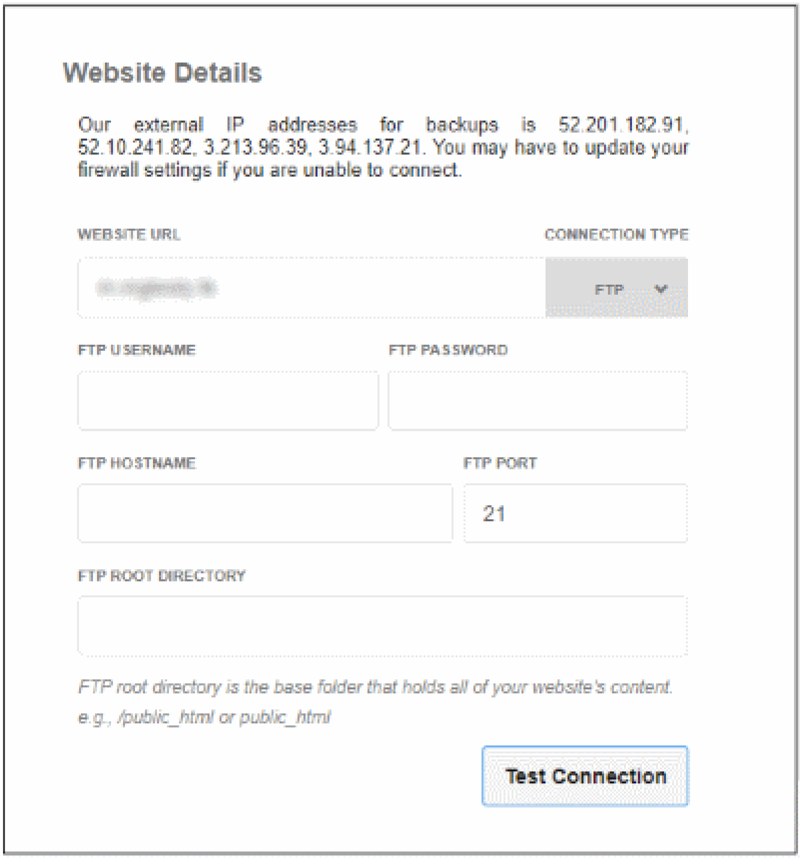
- Select the target website from the menu at top-left
- Click the 'Backup' tab
- Click 'Settings' on the upper-left

The settings page allows you to configure:

- **Website backup settings**
- **Database backup settings**
- **Schedule your backup**
- **Notification settings**
- **Backup exclusions**

Website Backup Settings

This section explains how to connect your site to the backup servers.



Website Details

Our external IP addresses for backups is 52.201.182.91, 52.10.241.82, 3.213.96.39, 3.94.137.21. You may have to update your firewall settings if you are unable to connect.

WEBSITE URL: [redacted]

CONNECTION TYPE: FTP

FTP USERNAME:

FTP PASSWORD:

FTP HOSTNAME:

FTP PORT: 21

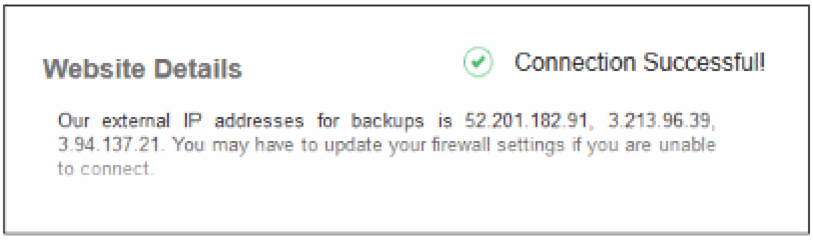
FTP ROOT DIRECTORY:

FTP root directory is the base folder that holds all of your website's content.

e.g., /public_html or public_html

- **Website URL** – Enter the domain of your site. Do not include http:// or https:// at the start.
- **Connection Type** – Select one of the following:
  - **FTP** – Enter the username and password of your FTP server
  - **SSH-KEY** – Add the private key shown in the interface to your authorized keys file (…/ssh/authorized_keys) on the FTP server
- **FTP Port** - The port over which cWatch should connect to your FTP server
- **FTP Directory** - The path of your web root folder. For example '/public_html/
- **Test Connection** - Click this after completing all fields

cWatch will check your settings and, if successful, show a confirmation message as follows:



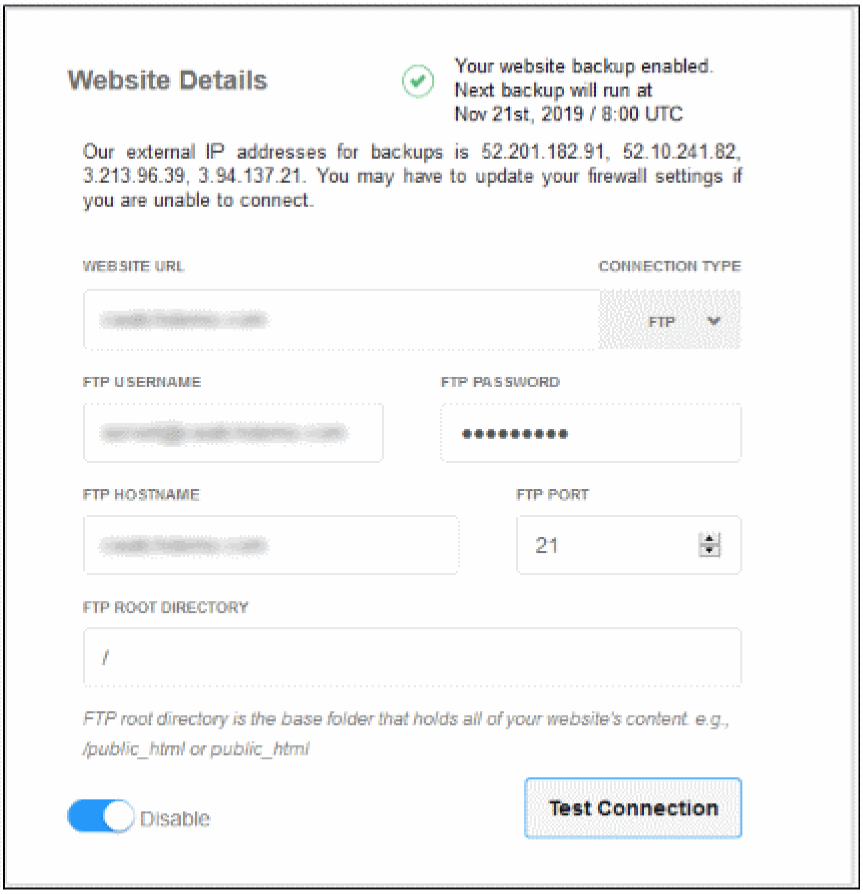
Website Details

✓ Connection Successful!

Our external IP addresses for backups is 52.201.182.91, 3.213.96.39, 3.94.137.21. You may have to update your firewall settings if you are unable to connect.

- Click 'Save'

The backup service is activated. You can enable or disable the service using the switch at the bottom.



Website Details

✓ Your website backup enabled. Next backup will run at Nov 21st, 2019 / 8:00 UTC

Our external IP addresses for backups is 52.201.182.91, 52.10.241.82, 3.213.96.39, 3.94.137.21. You may have to update your firewall settings if you are unable to connect.

WEBSITE URL

CONNECTION TYPE: FTP

FTP USERNAME

FTP PASSWORD: ●●●●●●●●●●

FTP HOSTNAME

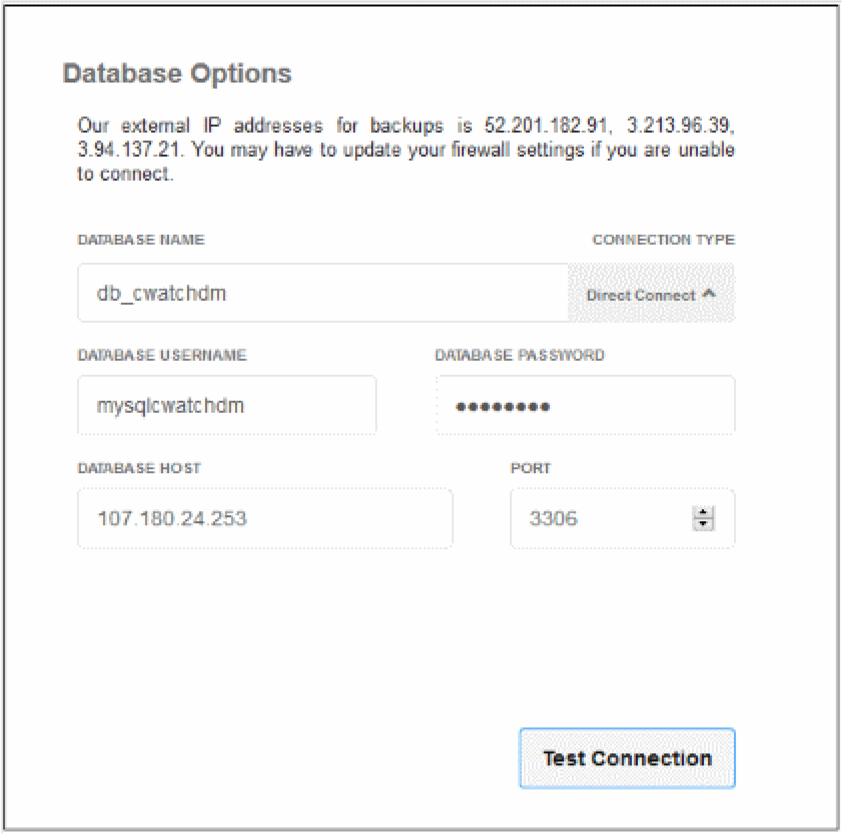
FTP PORT: 21

FTP ROOT DIRECTORY: /

FTP root directory is the base folder that holds all of your website's content. e.g., /public_html or public_html

Database Backup Settings

Configure settings to back up your site database to cWatch servers:



Database Options

Our external IP addresses for backups is 52.201.182.91, 3.213.96.39, 3.94.137.21. You may have to update your firewall settings if you are unable to connect.

DATABASE NAME: db_cwatchdm

CONNECTION TYPE: Direct Connect

DATABASE USERNAME: mysqlcwatchdm

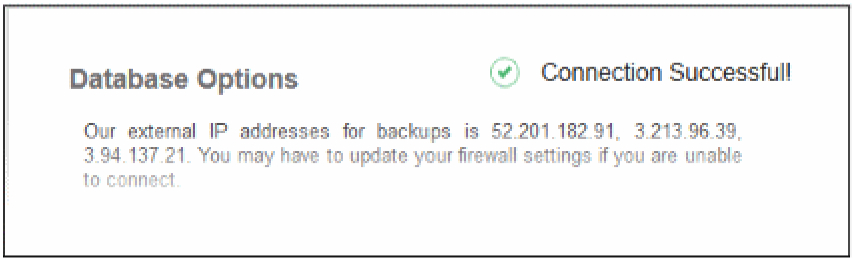
DATABASE PASSWORD: ••••••••

DATABASE HOST: 107.180.24.253

PORT: 3306

- **Database Name** – Your database's label
- **Connection Type** – Select one of the following:
  - **Direct Connect** – An AWS network connection from your database server to the cWatch server.
  - **SSH-KEY** - Add the private key shown in the interface to your authorized keys file (…/ssh/authorized_keys) on your database host
- **Database Username / Password** – The credentials to access the database
- **Database Host** – IP address or host name of the database server
- **Port** – The port over which cWatch should connect to the database server
- **Test Connection** – Click this after completing all fields

You will see the following confirmation message if the test is successful:



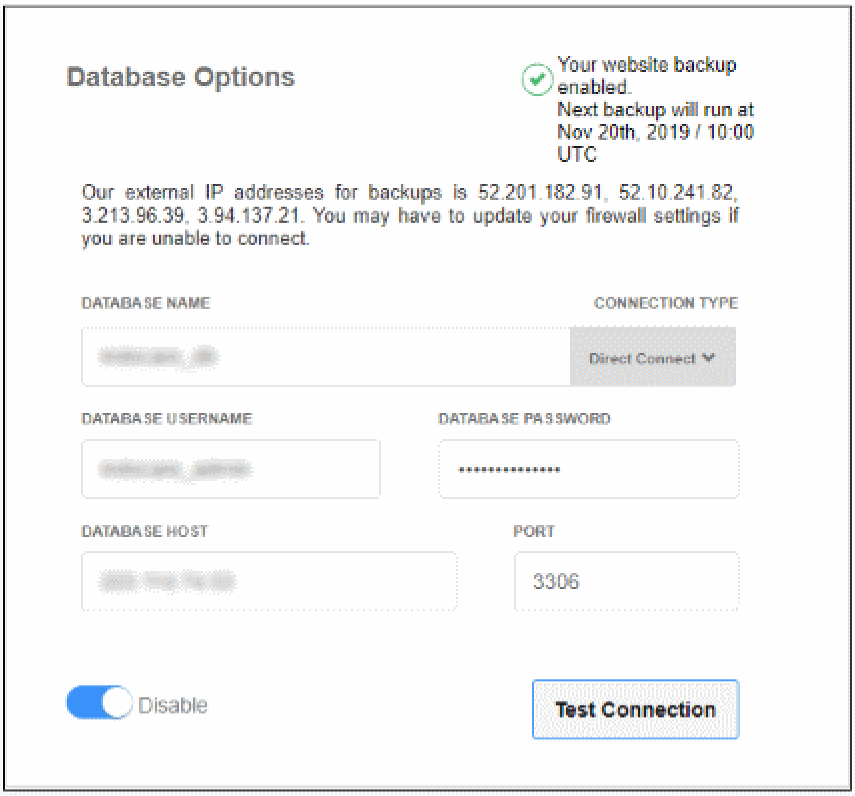
Database Options

Connection Successful!

Our external IP addresses for backups is 52.201.182.91, 3.213.96.39, 3.94.137.21. You may have to update your firewall settings if you are unable to connect.

- Click 'Save'

The database backup service is activated and you have the option to enable or disable it using the button at the bottom.



Database Options

✓ Your website backup enabled.
Next backup will run at Nov 20th, 2019 / 10:00 UTC

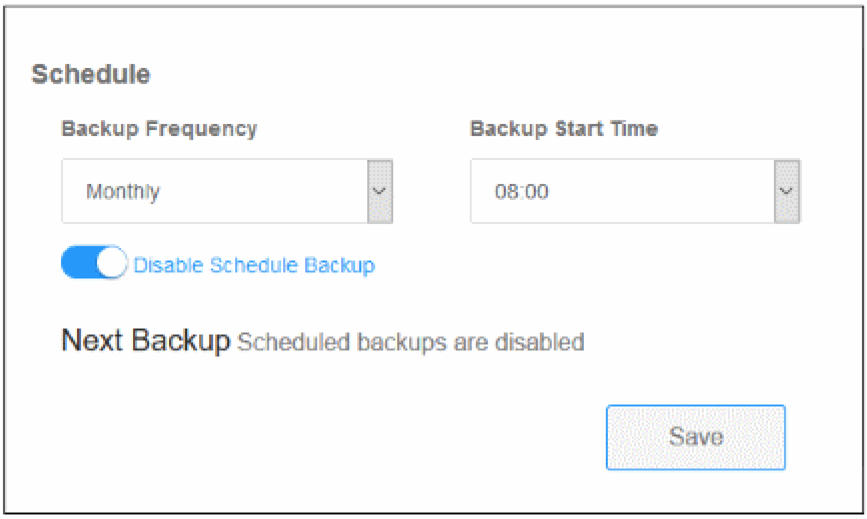
Our external IP addresses for backups is 52.201.182.91, 52.10.241.82, 3.213.96.39, 3.94.137.21. You may have to update your firewall settings if you are unable to connect.

DATABASE NAME:
CONNECTION TYPE: Direct Connect
DATABASE USERNAME:
DATABASE PASSWORD: ••••••••••••••
DATABASE HOST:
PORT: 3306

Disable

Schedule your Backup

This section lets you configure regular, automatic, backups of your site.



Schedule

Backup Frequency: Monthly

Backup Start Time: 08:00

Disable Schedule Backup

Next Backup Scheduled backups are disabled

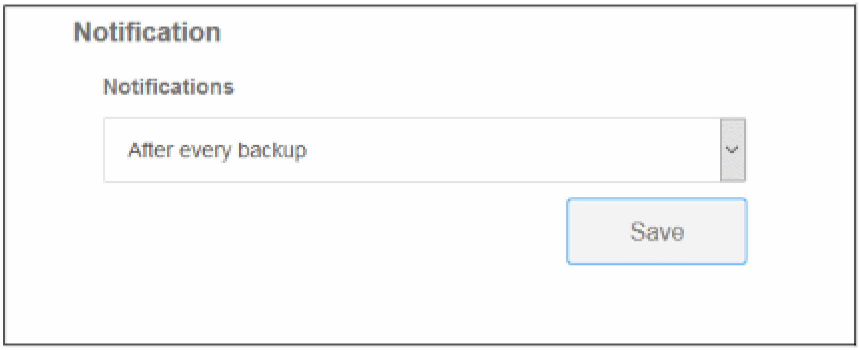
- **Backup Frequency** – Four options are available:
  - **Daily** - Backups start at the date/time shown in 'Next Backup', then run every day at the same time thereafter
  - **Every 2 days** - Backups start at the date/time shown in 'Next Backup', then run every other day thereafter.
  - **Weekly** – Backups start at the date/time shown in 'Next Backup', then run every 7 days thereafter.
  - **Monthly** - Backups start at the date/time shown in 'Next Backup', then run at the same date/time

of every calendar month thereafter.

- Click 'Save'

Notification Settings

cWatch can send email alerts to admins about the success or failure of each backup operation.



Notification

Notifications

After every backup

Choose one of the following options:

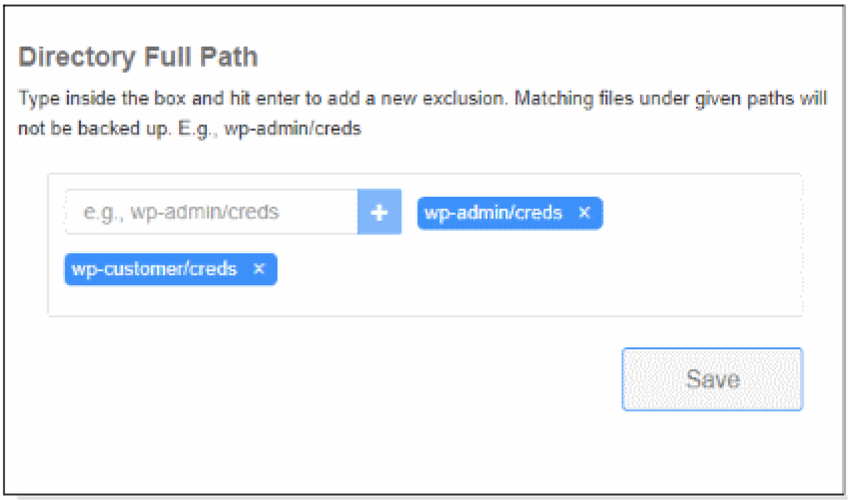
- **After every backup** – You receive a notification after each backup. The message states whether the operation was successful or not.
- **Only on failure** – You only receive a notification when a backup fails
- **Disable notifications** – No notification mails are sent

Click 'Save'

Backup Exclusions

Exclusions are folders and files that you do not want to backup. This might be because they contain sensitive information, or simply because you don't want certain files to eat into your storage limit.

Directory Full Path



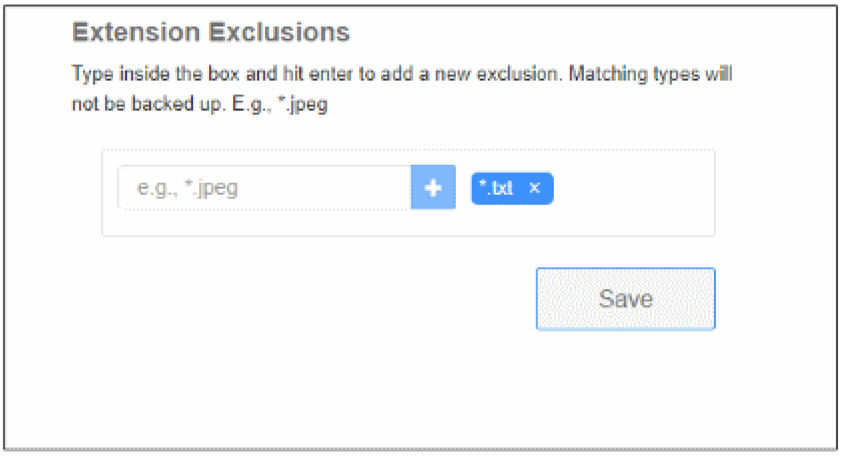
Directory Full Path

Type inside the box and hit enter to add a new exclusion. Matching files under given paths will not be backed up. E.g., wp-admin/creds

- Type the location of the folder that you want to exclude. For example, wp-admin/creds
- Click '+'.
- Repeat the procedure to add more paths
- Click 'Save'

Extension Exclusions

Files with matching extensions are not backed up to cWatch servers.



Extension Exclusions

Type inside the box and hit enter to add a new exclusion. Matching types will not be backed up. E.g., *.jpeg

- Type the extension of the file that you want to exclude. You must prefix the extension with *.
  - For example, *.txt
- Click '+'.
- Repeat the procedure to add more file extensions.
- Click 'Save'

Click here for more information.

Manual Backup and Restore

An on-demand backup is one that you run at any time as circumstances demand. For example, you might want to run an on-demand backup just prior to putting some website changes live.

A manual backup includes both website files and database. You can run two on-demand backups per-day.

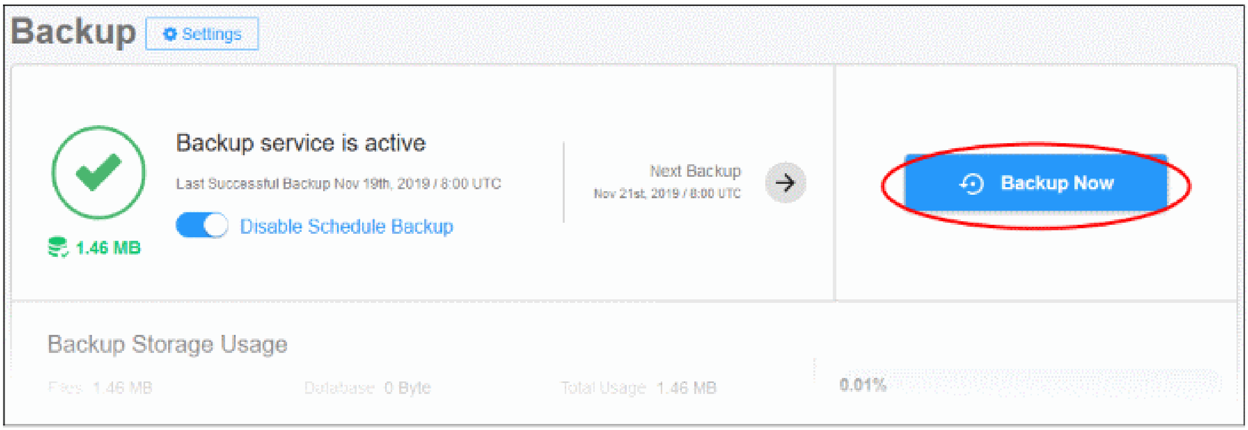
- Select the target website from the menu at top-left
- Click the 'Backup' tab

This section allows you to:

- **Run an on-demand backup**
- **Restore and download website files**
- **View backup records and file statistics**

Run an On-Demand Backup

- Click the 'Backup Now' button:



Backup ⚙ Settings

Backup service is active

Last Successful Backup Nov 19th, 2019 / 8:00 UTC

Disable Schedule Backup

1.46 MB

Next Backup Nov 21st, 2019 / 8:00 UTC

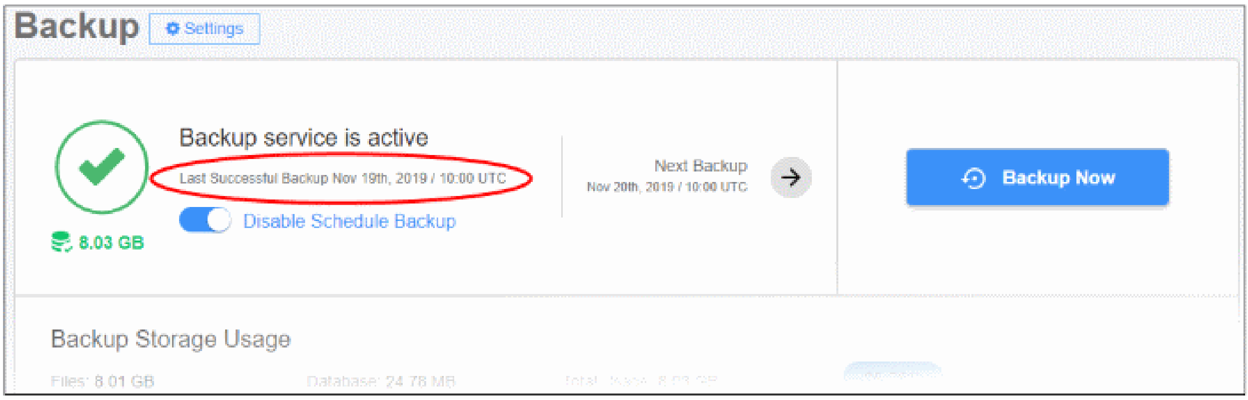
Backup Now

Backup Storage Usage

Files: 1.46 MB Database: 0 Byte Total Usage: 1.46 MB 0.01%

- Note – You will be prompted to upgrade your license if the backup size exceeds your quota.

The date of the most recent backup is refreshed when the operation finishes:



Backup ⚙ Settings

Backup service is active

Last Successful Backup Nov 19th, 2019 / 10:00 UTC

Disable Schedule Backup

8.03 GB

Next Backup Nov 20th, 2019 / 10:00 UTC

Backup Now

Backup Storage Usage

Files: 8.01 GB Database: 24.78 MB Total Usage: 8.03 GB

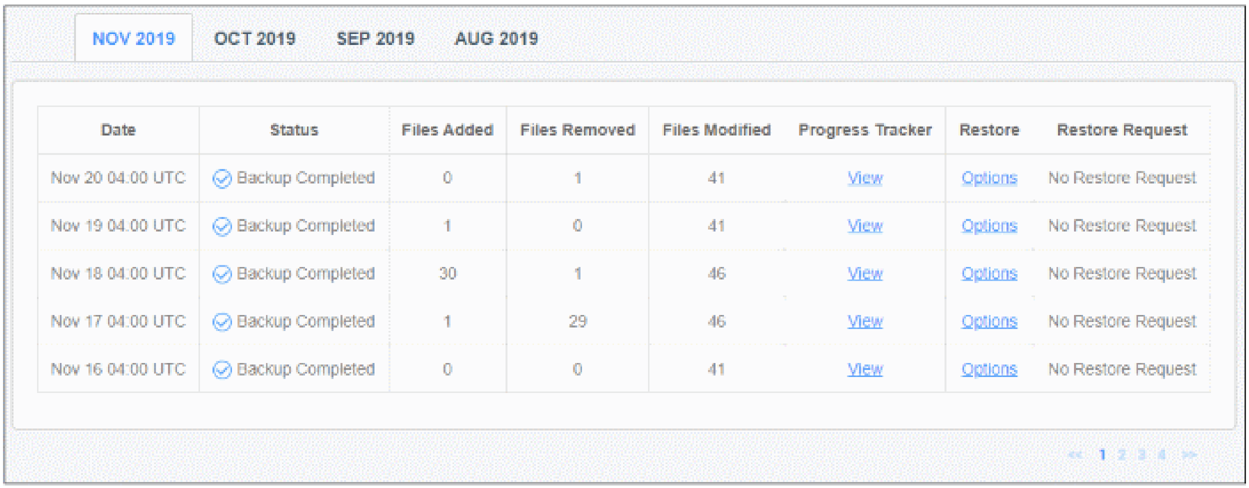
Restore and Download Website Files

- You can restore your site from any backup you have taken in the past.
- You can restore all files or selected files
- There are two steps to a restore process:

1. **Restore website files**. Done automatically when you click ‘Options’ > ‘Auto-restore All Files’ or ‘Selective Auto Restore’. This does not overwrite your current database.
2. **Restore database**. You must do this manually. You can download the database from the ‘Restore’ options. You can get the database from a different backup-row if required.

Run a restore operation

- Scroll down to the backup history table:

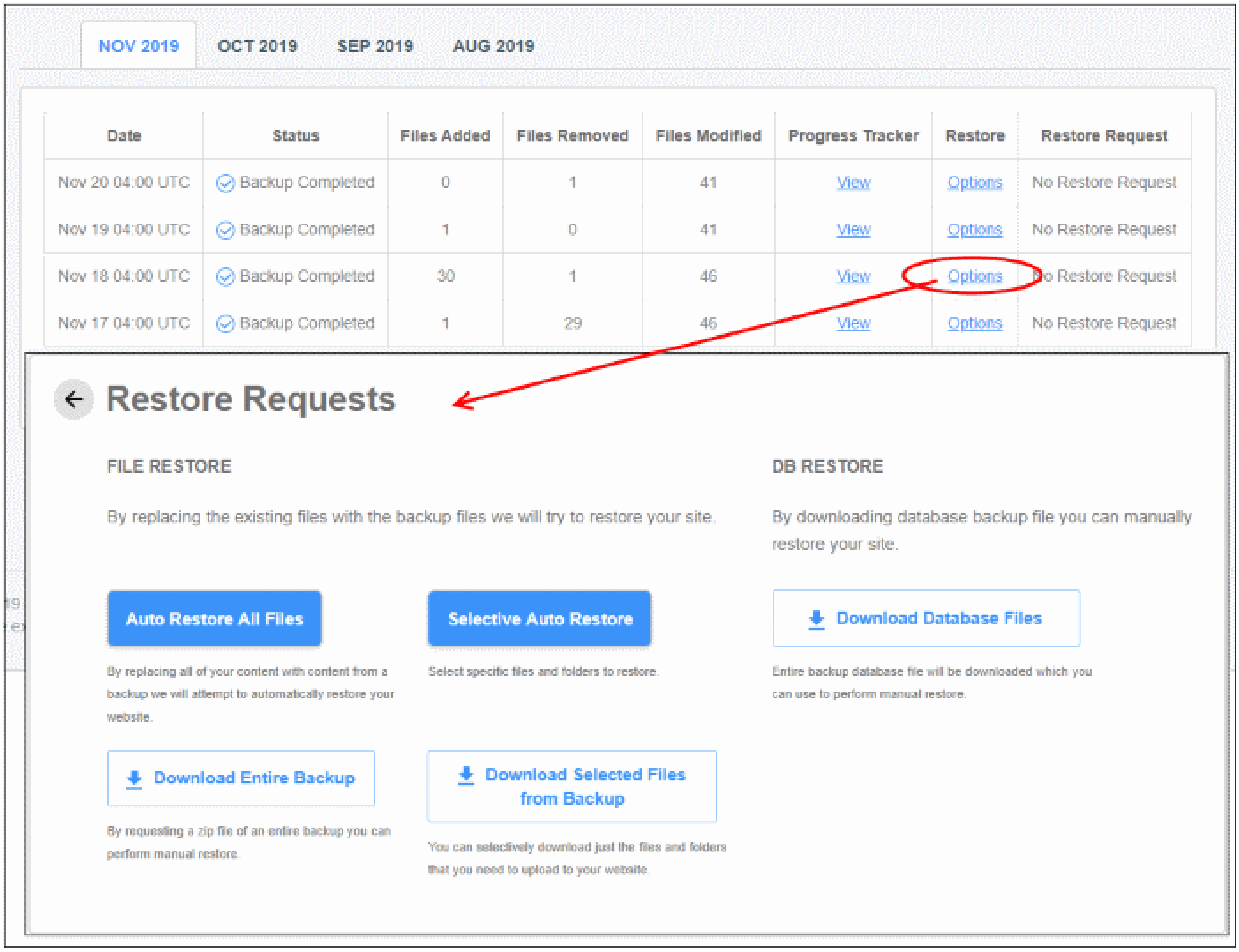


NOV 2019 | OCT 2019 | SEP 2019 | AUG 2019

Date	Status	Files Added	Files Removed	Files Modified	Progress Tracker	Restore	Restore Request
Nov 20 04:00 UTC	Backup Completed	0	1	41	View	Options	No Restore Request
Nov 19 04:00 UTC	Backup Completed	1	0	41	View	Options	No Restore Request
Nov 18 04:00 UTC	Backup Completed	30	1	46	View	Options	No Restore Request
Nov 17 04:00 UTC	Backup Completed	1	29	46	View	Options	No Restore Request
Nov 16 04:00 UTC	Backup Completed	0	0	41	View	Options	No Restore Request

<< 1 2 3 4 >>

- Use the month tabs and page numbers to find the backup you require
- Click 'Options' in the row of the backup you want to use:



NOV 2019 | OCT 2019 | SEP 2019 | AUG 2019

Date	Status	Files Added	Files Removed	Files Modified	Progress Tracker	Restore	Restore Request
Nov 20 04:00 UTC	Backup Completed	0	1	41	View	Options	No Restore Request
Nov 19 04:00 UTC	Backup Completed	1	0	41	View	Options	No Restore Request
Nov 18 04:00 UTC	Backup Completed	30	1	46	View	Options	No Restore Request
Nov 17 04:00 UTC	Backup Completed	1	29	46	View	Options	No Restore Request

Restore Requests

FILE RESTORE

By replacing the existing files with the backup files we will try to restore your site.

Auto Restore All Files

By replacing all of your content with content from a backup we will attempt to automatically restore your website.

Selective Auto Restore

Select specific files and folders to restore.

Download Entire Backup

By requesting a zip file of an entire backup you can perform manual restore.

Download Selected Files from Backup

You can selectively download just the files and folders that you need to upload to your website.

DB RESTORE

By downloading database backup file you can manually restore your site.

Download Database Files

Entire backup database file will be downloaded which you can use to perform manual restore.

File Restore:

- **Auto Restore all Files** - Starts the full restore process. Files in the destination will be replaced by those in the backup.
- **Selective Auto Restore** - Restore specific files and folders.
- **Download Entire Backup** - Download a .zip file of the backup. You can use this to manually restore files, or to run a partial restore, or to simply retrieve some lost / older versions of files.
- **Download Selected Files from Backup** – Retrieve specific files from the backup. This is a simple

download of files, rather than restoring them to their original location.

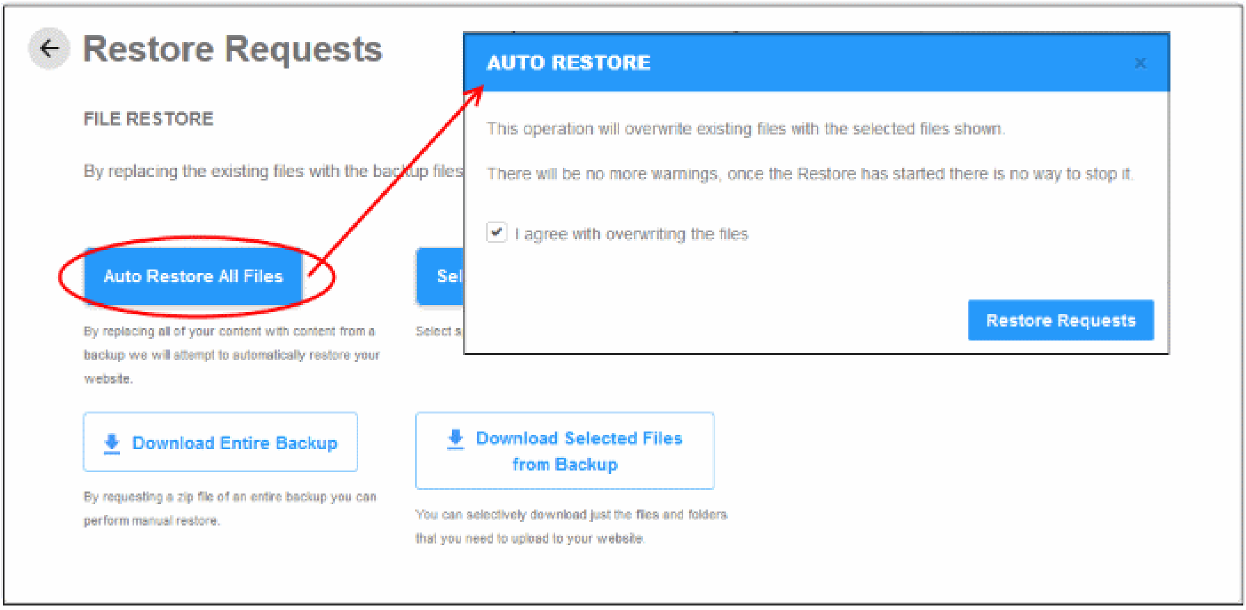
DB Restore:

- **Download Database Files** - Download a .zip file which contains all database records. You can manually unzip and restore the database as required.

The rest of this section is just screenshots to illustrate the processes above.

Auto Restore all Files

- Click 'Options' in the row of the backup you want to use
- Click 'Auto Restore All Files':



Restore Requests

FILE RESTORE

By replacing the existing files with the backup files

Auto Restore All Files

By replacing all of your content with content from a backup we will attempt to automatically restore your website.

Download Entire Backup

By requesting a zip file of an entire backup you can perform manual restore.

Download Selected Files from Backup

You can selectively download just the files and folders that you need to upload to your website.

AUTO RESTORE

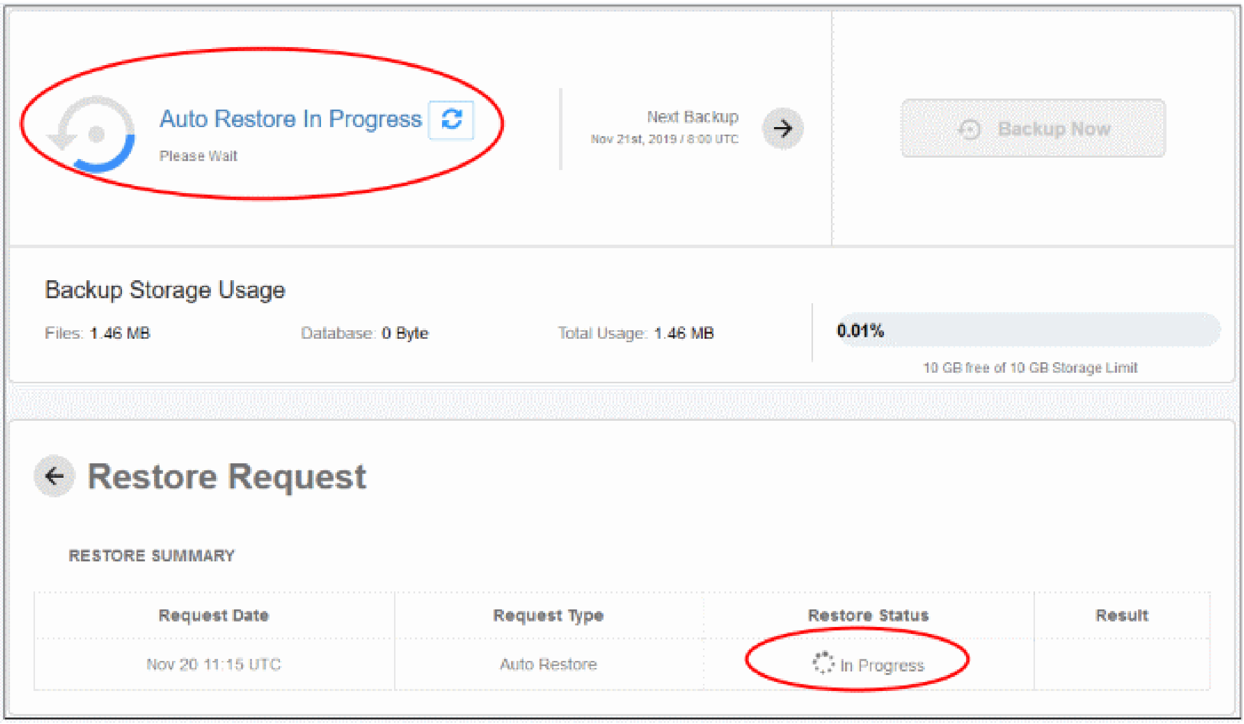
This operation will overwrite existing files with the selected files shown.

There will be no more warnings, once the Restore has started there is no way to stop it.

☑ I agree with overwriting the files

Restore Requests

- Agree to overwriting files and click 'Restore'
- You will see the following confirmation:



Auto Restore In Progress

Please Wait

Next Backup
Nov 21st, 2019 / 8:00 UTC

Backup Now

Backup Storage Usage

Files: 1.46 MB   Database: 0 Byte   Total Usage: 1.46 MB   0.01%

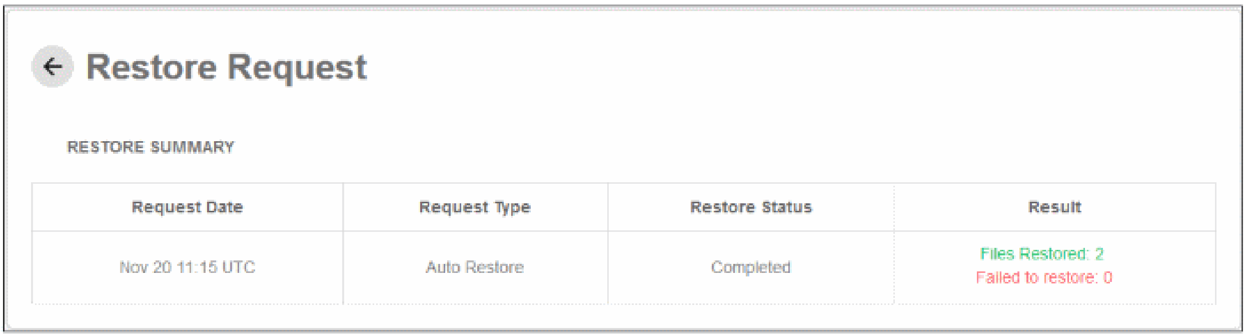
10 GB free of 10 GB Storage Limit

Restore Request

RESTORE SUMMARY

Request Date	Request Type	Restore Status	Result
Nov 20 11:15 UTC	Auto Restore	In Progress	

- Results are shown at the end of the operation:



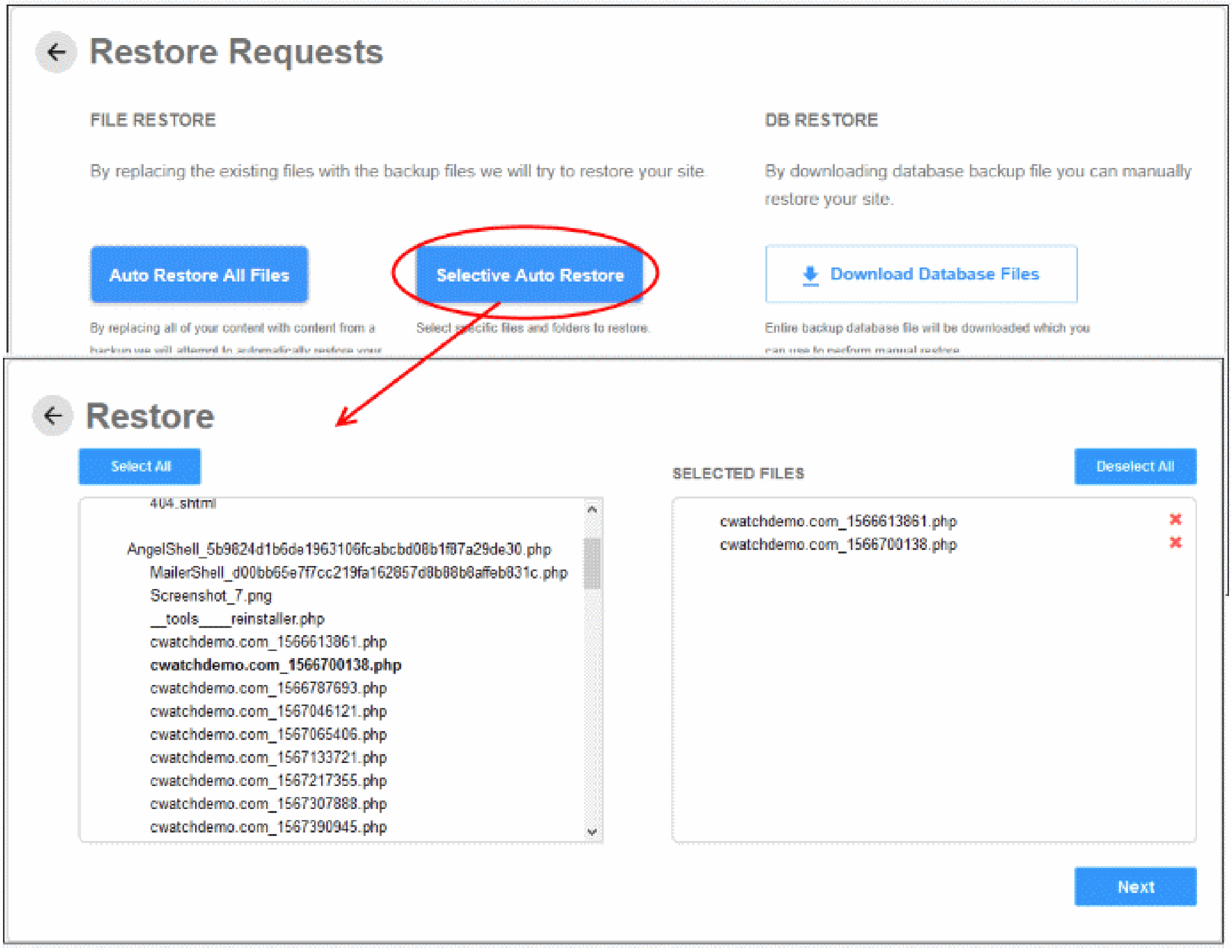
Restore Request

RESTORE SUMMARY

Request Date	Request Type	Restore Status	Result
Nov 20 11:15 UTC	Auto Restore	Completed	Files Restored: 2 Failed to restore: 0

Selective Auto Restore

- Click 'Options' in the row of the backup you want to use
- Click 'Selective Auto Restore':



Restore Requests

FILE RESTORE

By replacing the existing files with the backup files we will try to restore your site

DB RESTORE

By downloading database backup file you can manually restore your site.

By replacing all of your content with content from a backup we will attempt to automatically restore your

Select specific files and folders to restore.

Entire backup database file will be downloaded which you can use to perform manual restore

Restore

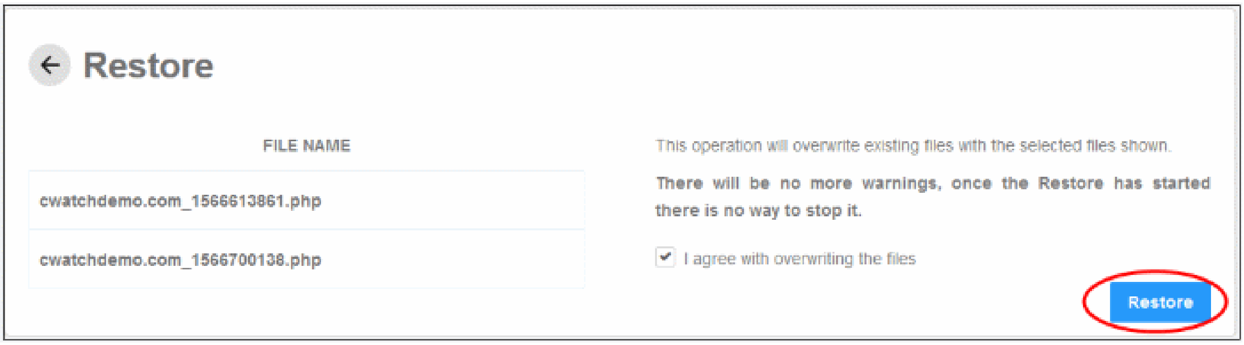
```
404.shtml

AngelShell_5b9824d1b6de1963106fcabcbd08b1f87a29de30.php
  MailerShell_d00bb65e7f7cc219fa162857d8b88b8affeb831c.php
  Screenshot_7.png
  __tools____reinstaller.php
  cwatchdemo.com_1566613861.php
  cwatchdemo.com_1566700138.php
  cwatchdemo.com_1566787693.php
  cwatchdemo.com_1567046121.php
  cwatchdemo.com_1567065406.php
  cwatchdemo.com_1567133721.php
  cwatchdemo.com_1567217355.php
  cwatchdemo.com_1567307888.php
  cwatchdemo.com_1567390945.php
```

SELECTED FILES

cwatchdemo.com_1566613861.php ✖
cwatchdemo.com_1566700138.php ✖

- Select the backed up file(s) on the left and click 'Next'



Restore

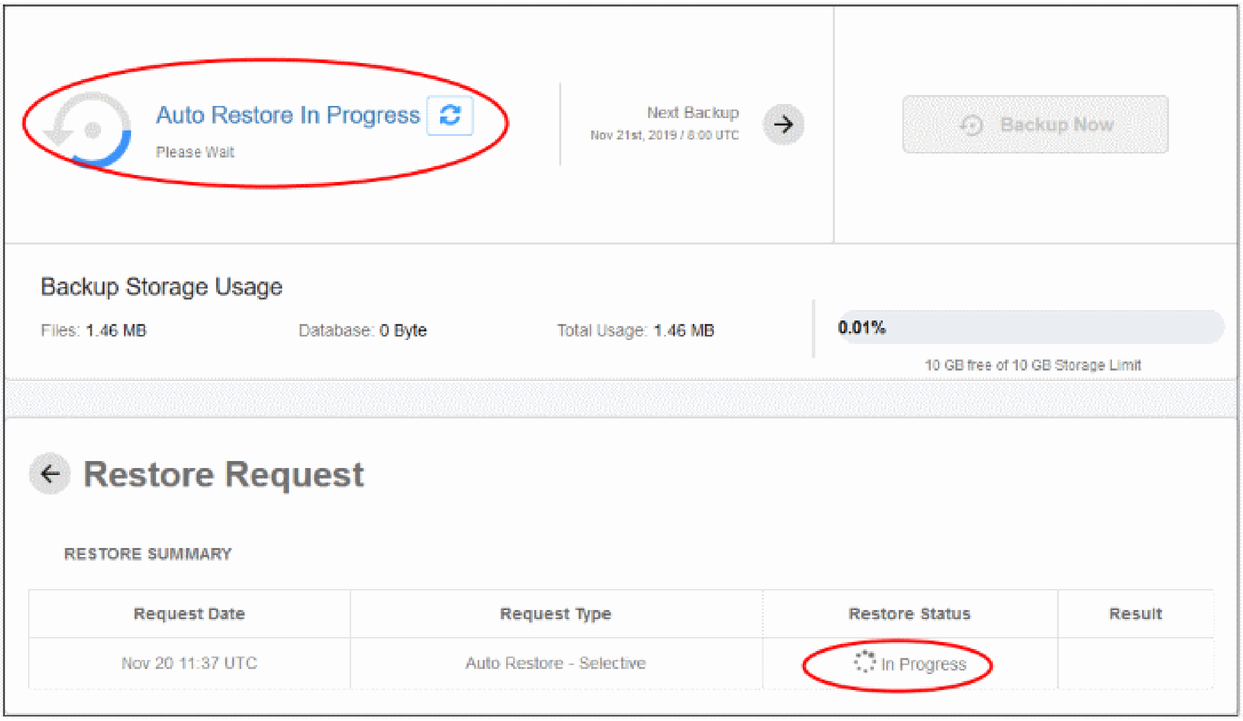
FILE NAME
cwatchdemo.com_1566613861.php
cwatchdemo.com_1566700138.php

This operation will overwrite existing files with the selected files shown.

There will be no more warnings, once the Restore has started there is no way to stop it.

☑ I agree with overwriting the files

- Check the selected files detail on the left, agree to overwrite the files and click 'Restore'.
- You will see the following confirmation:



Backup Storage Usage

Files: 1.46 MB Database: 0 Byte Total Usage: 1.46 MB

0.01%

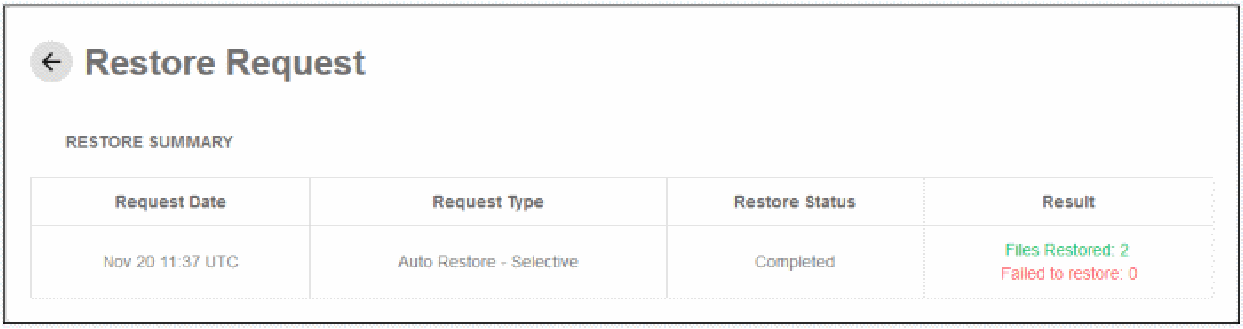
10 GB free of 10 GB Storage Limit

Restore Request

RESTORE SUMMARY

Request Date	Request Type	Restore Status	Result
Nov 20 11:37 UTC	Auto Restore - Selective	In Progress	

- Results are shown at the end of the operation:



Restore Request

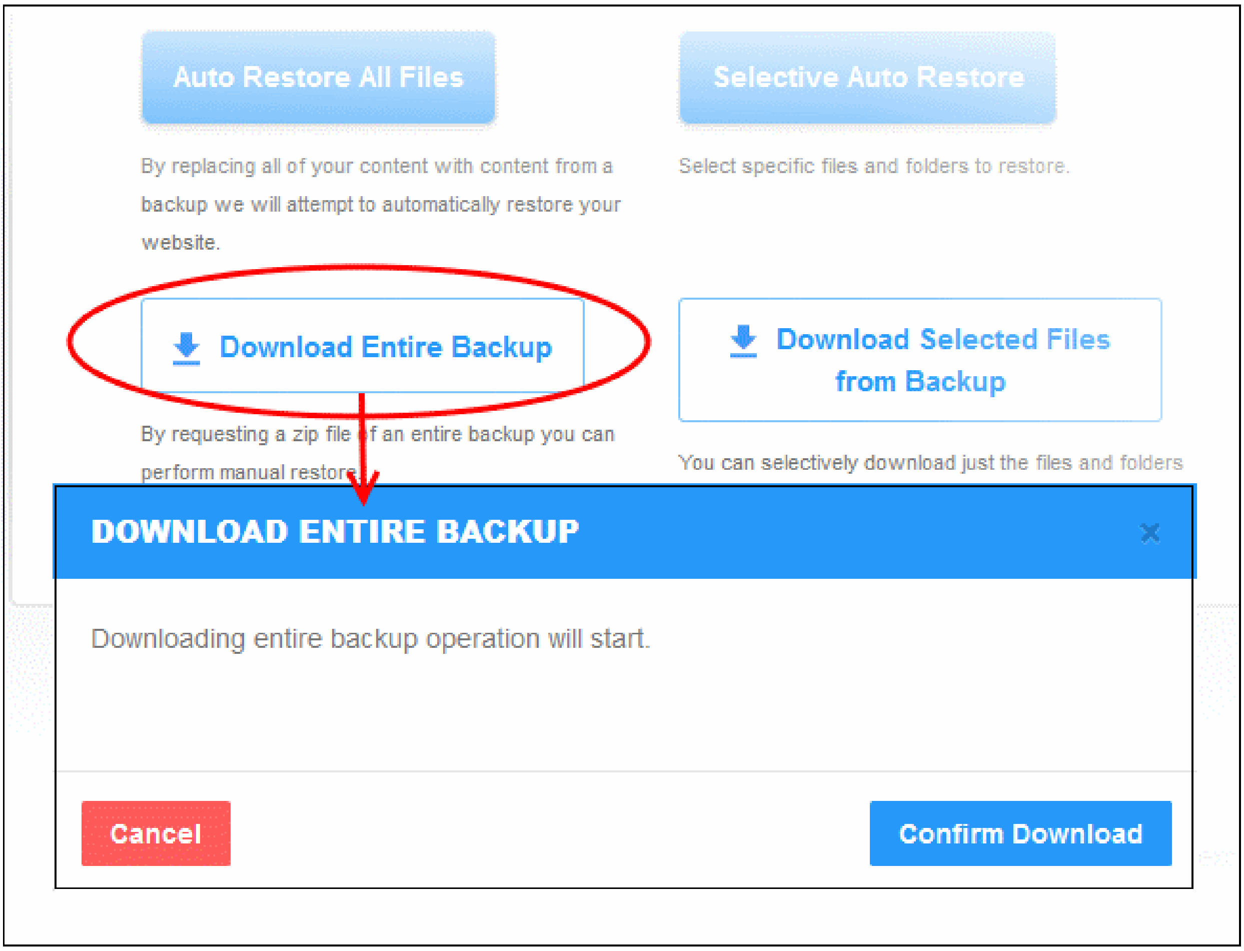
RESTORE SUMMARY

Request Date	Request Type	Restore Status	Result
Nov 20 11:37 UTC	Auto Restore - Selective	Completed	Files Restored: 2 Failed to restore: 0

Download Entire Backup

- Click 'Options' in the row of the backup you want to use

- Click ‘Download Entire Backup’ > ‘Confirm Download’:



By replacing all of your content with content from a backup we will attempt to automatically restore your website.

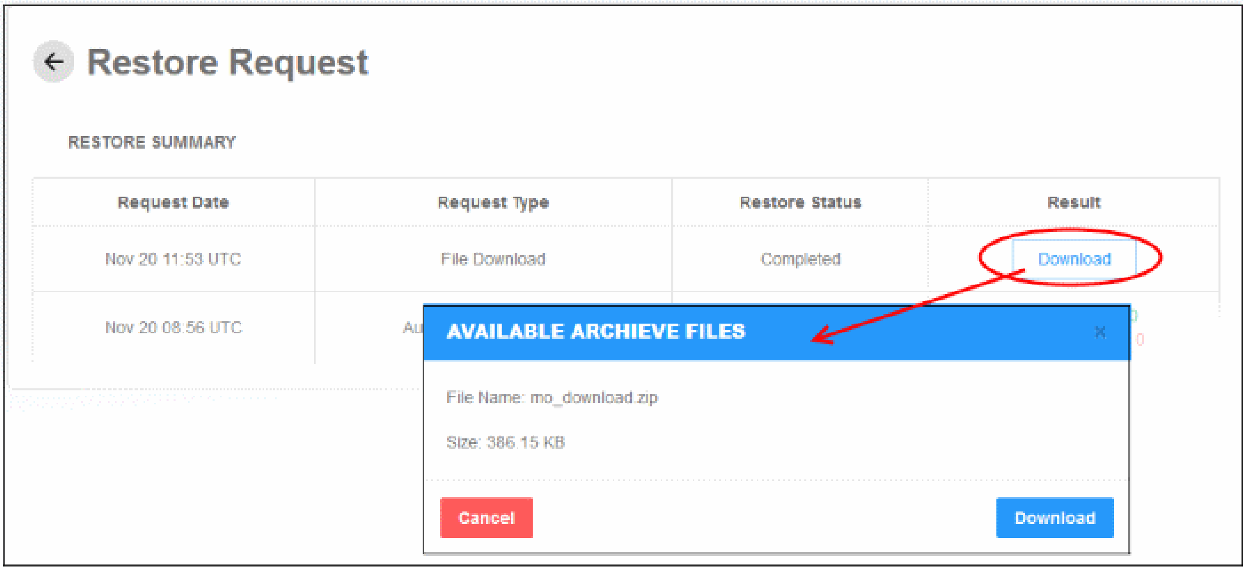
Select specific files and folders to restore.

By requesting a zip file of an entire backup you can perform manual restore

You can selectively download just the files and folders

Downloading entire backup operation will start.

- cWatch will retrieve your files and create a zip file of them. This process may take a few seconds.
- Once complete, click ‘Download’ in the ‘Result’ column:



Request Date	Request Type	Restore Status	Result
Nov 20 11:53 UTC	File Download	Completed	Download
Nov 20 08:56 UTC	Au		

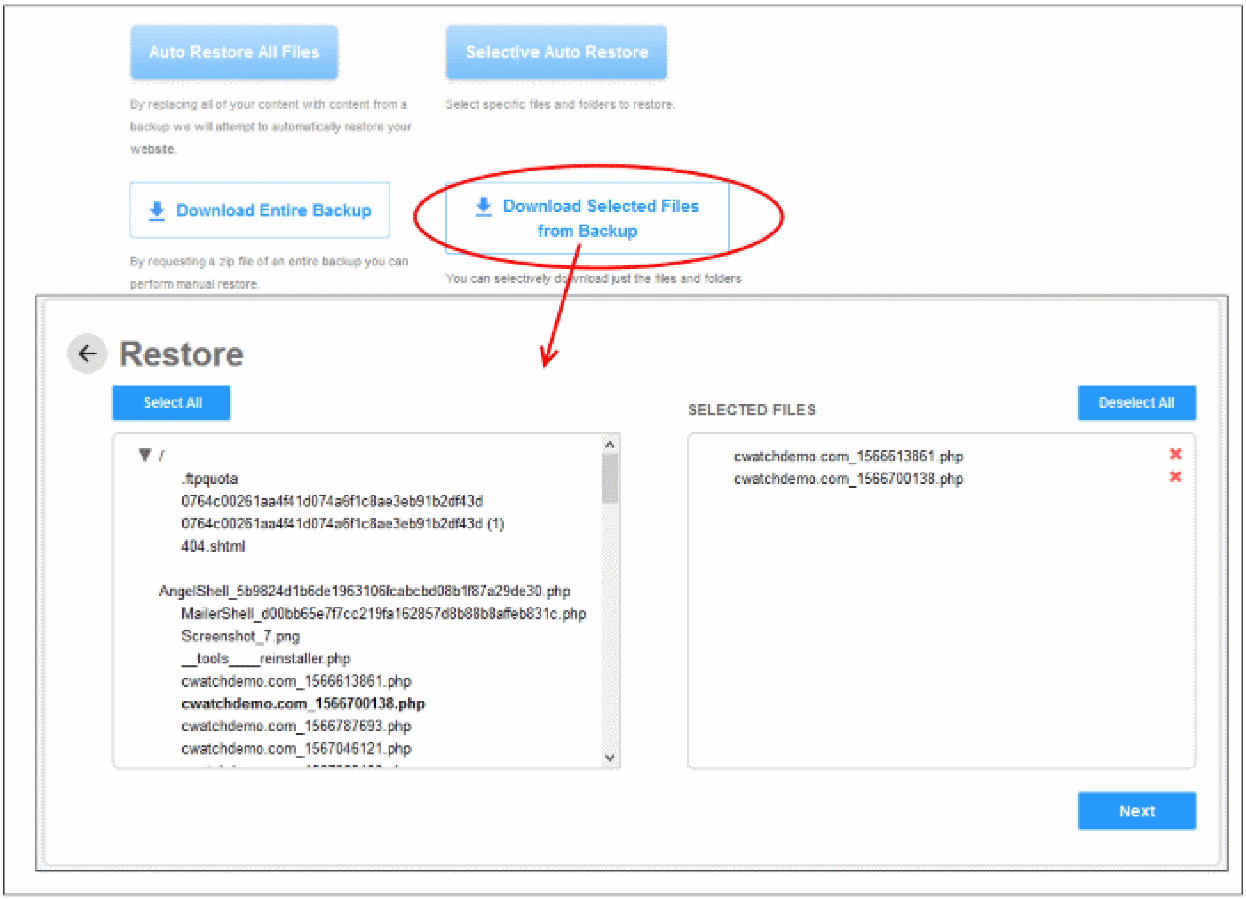
File Name: mo_download.zip

Size: 386.15 KB

- Click ‘Download’ to save the zip file

Download Selected Files from Backup

- Click ‘Options’ in the row of the backup you want to use
- Click ‘Download Selected Files from Backup’



By replacing all of your content with content from a backup we will attempt to automatically restore your website.

Select specific files and folders to restore.

By requesting a zip file of an entire backup you can perform manual restore.

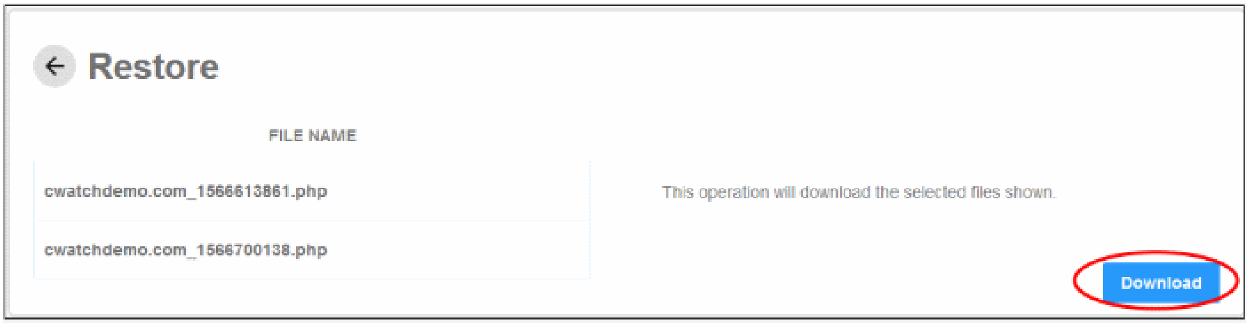
You can selectively download just the files and folders

```
▼ /
    .ftpquota
    0764c00261aa4f41d074a6f1c8ae3eb91b2df43d
    0764c00261aa4f41d074a6f1c8ae3eb91b2df43d (1)
    404.shtml

  AngelShell_5b9824d1b6de1963106fcabcbd08b1f87a29de30.php
    MailerShell_d00bb65e7f7cc219fa162857d8b88b8affeb831c.php
    Screenshot_7.png
    __tools___reinstaller.php
    cwatchdemo.com_1566613861.php
    cwatchdemo.com_1566700138.php
    cwatchdemo.com_1566787693.php
    cwatchdemo.com_1567046121.php
```

cwatchdemo.com_1566613861.php ✖
cwatchdemo.com_1566700138.php ✖

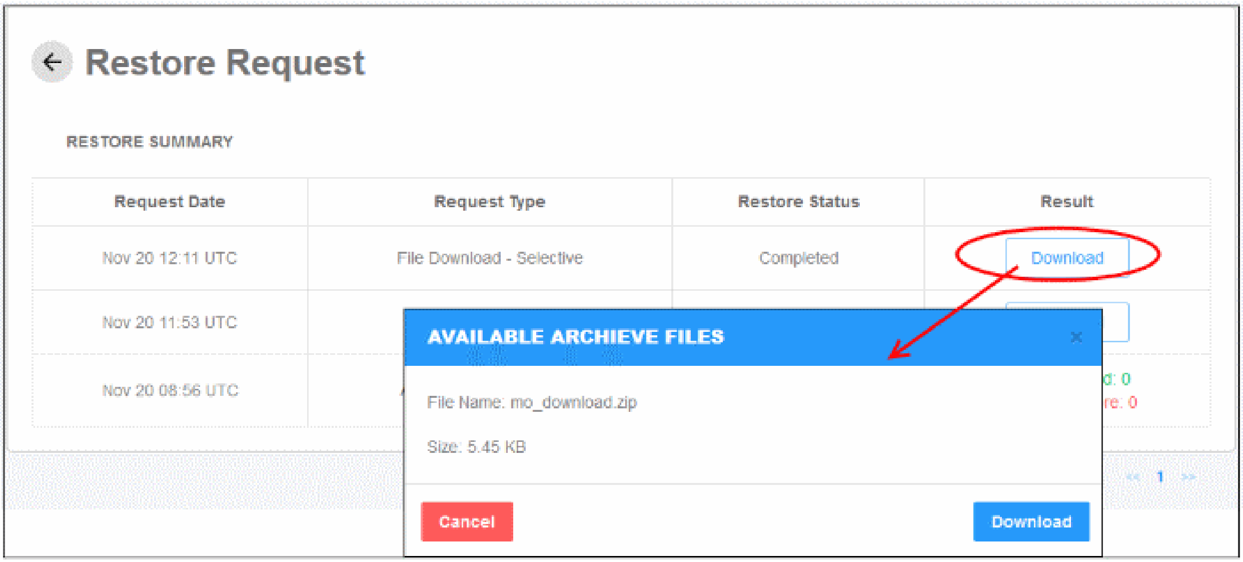
- Select the backed up file(s) on the left and click ‘Next’



FILE NAME
cwatchdemo.com_1566613861.php
cwatchdemo.com_1566700138.php

This operation will download the selected files shown.

- Check the selected files detail on the left and click ‘Download’.
- cWatch will retrieve your files and create a zip file of them. This process may take a few seconds.
- Once complete, click ‘Download’ in the ‘Result’ column:



Restore Request

RESTORE SUMMARY

Request Date	Request Type	Restore Status	Result
Nov 20 12:11 UTC	File Download - Selective	Completed	Download
Nov 20 11:53 UTC			
Nov 20 08:56 UTC			d: 0 re: 0

AVAILABLE ARCHIEVE FILES

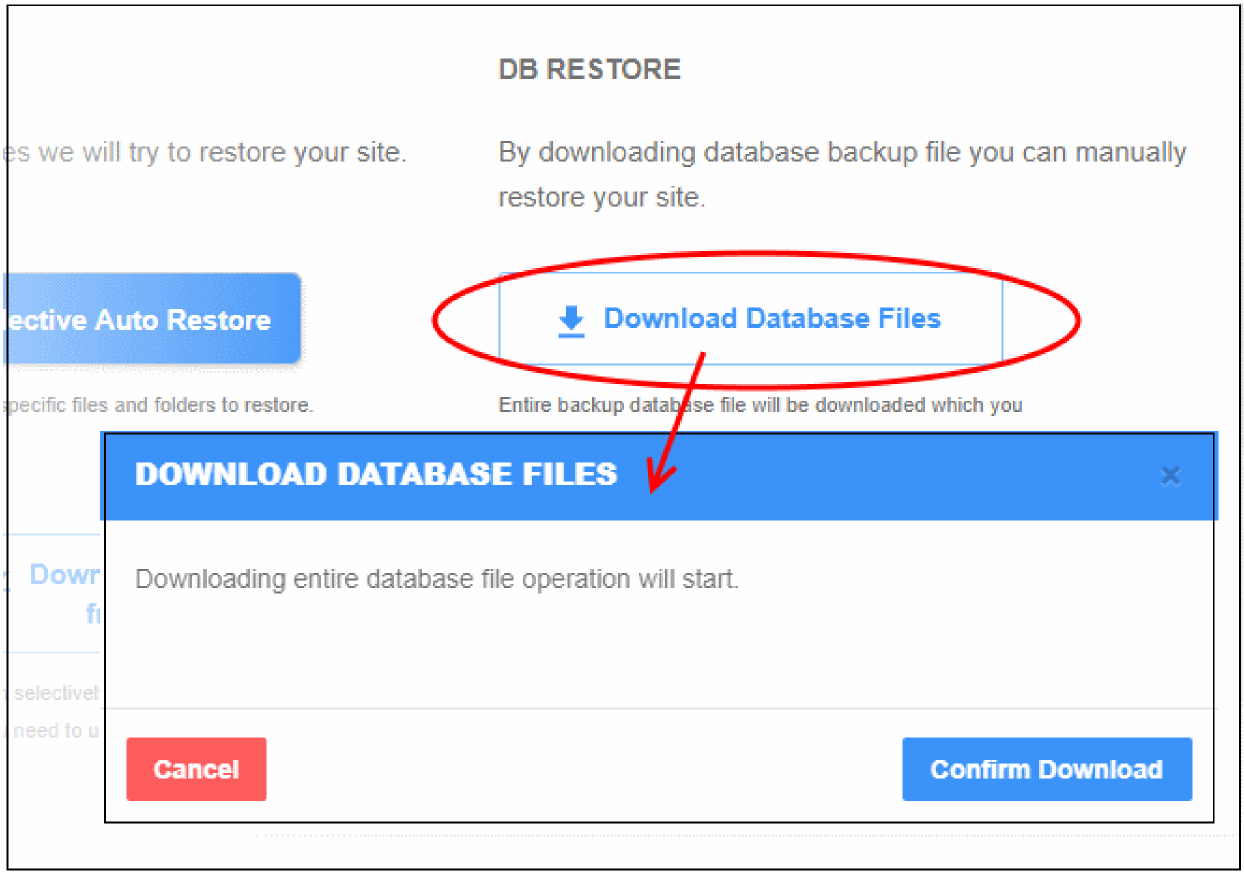
File Name: mo_download.zip

Size: 5.45 KB

- Click ‘Download’ to save the zip file

Database Restore

- Click ‘Options’ in the row of the backup you want to use
- Click ‘Download Database Files’ > ‘Confirm Download’:



DB RESTORE

es we will try to restore your site.

By downloading database backup file you can manually restore your site.

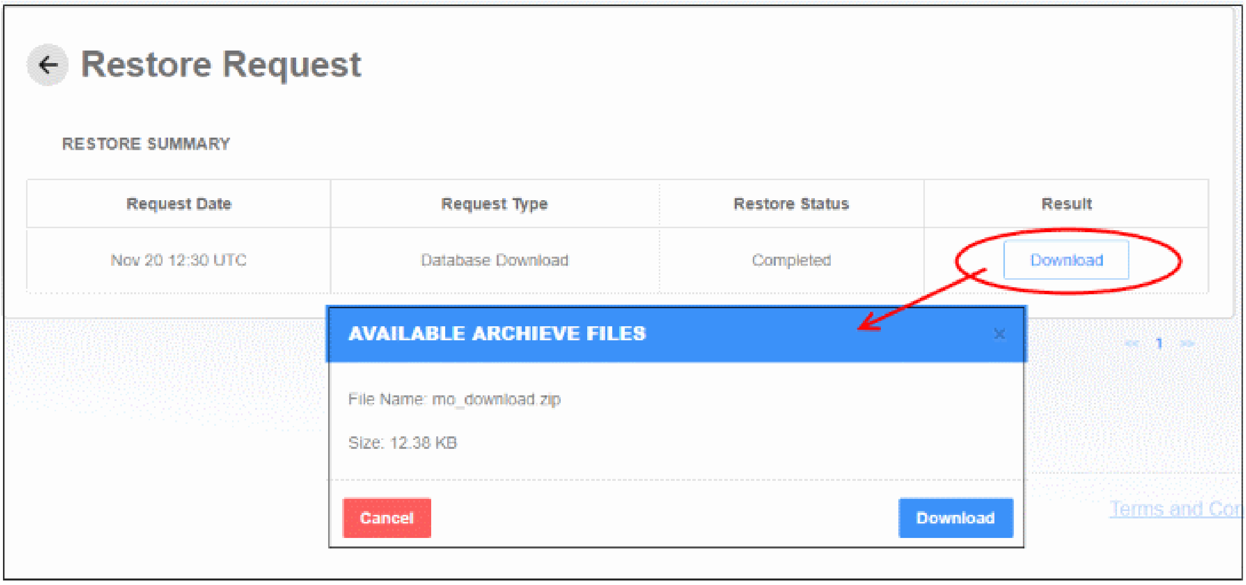
pecific files and folders to restore.

Entire backup database file will be downloaded which you

DOWNLOAD DATABASE FILES

Downloading entire database file operation will start.

- cWatch will create a zip file containing your database. This process may take a few seconds.
- Once complete, click 'Download' in the ‘Result’ column:



Restore Request

RESTORE SUMMARY

Request Date	Request Type	Restore Status	Result
Nov 20 12:30 UTC	Database Download	Completed	Download

AVAILABLE ARCHIEVE FILES

File Name: mo_download.zip

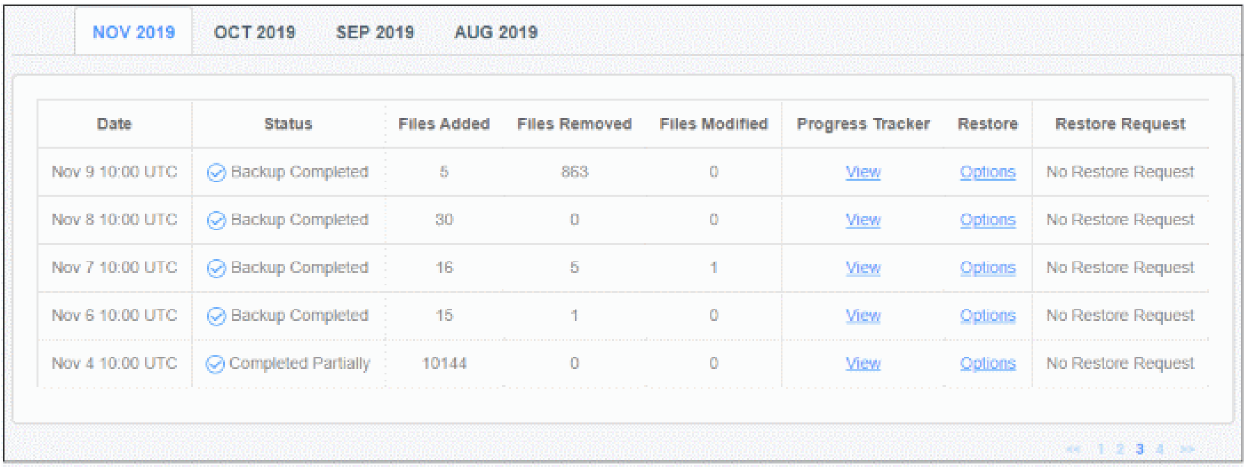
Size: 12.38 KB

- Click ‘Download’ to save the zip file

View Backup Records and File Statistics

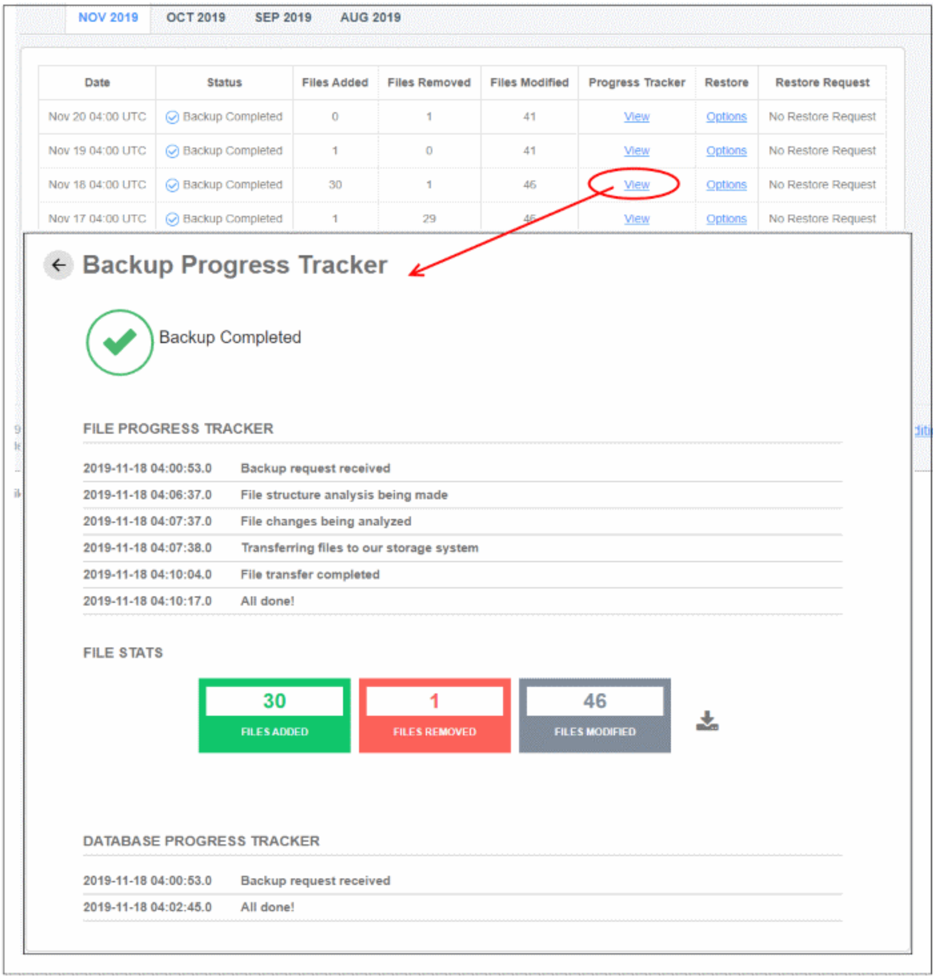
The lower-half of the backup home screen shows a full history of your previous backups. Details about each includes the date, the success or failure of the operation, and the exact files involved. You can also restore your site from any backup you have taken in the past.

The lower pane shows previous backups that you have run. Backups are grouped by month.



Date	Status	Files Added	Files Removed	Files Modified	Progress Tracker	Restore	Restore Request
Nov 9 10:00 UTC	✓ Backup Completed	5	863	0	View	Options	No Restore Request
Nov 8 10:00 UTC	✓ Backup Completed	30	0	0	View	Options	No Restore Request
Nov 7 10:00 UTC	✓ Backup Completed	16	5	1	View	Options	No Restore Request
Nov 6 10:00 UTC	✓ Backup Completed	15	1	0	View	Options	No Restore Request
Nov 4 10:00 UTC	✓ Completed Partially	10144	0	0	View	Options	No Restore Request

- Click 'View' in a backup record



Date	Status	Files Added	Files Removed	Files Modified	Progress Tracker	Restore	Restore Request
Nov 20 04:00 UTC	✓ Backup Completed	0	1	41	View	Options	No Restore Request
Nov 19 04:00 UTC	✓ Backup Completed	1	0	41	View	Options	No Restore Request
Nov 18 04:00 UTC	✓ Backup Completed	30	1	46	View	Options	No Restore Request
Nov 17 04:00 UTC	✓ Backup Completed	1	29	46	View	Options	No Restore Request

Backup Progress Tracker

✓ Backup Completed

FILE PROGRESS TRACKER

```
2019-11-18 04:00:53.0   Backup request received
2019-11-18 04:06:37.0   File structure analysis being made
2019-11-18 04:07:37.0   File changes being analyzed
2019-11-18 04:07:38.0   Transferring files to our storage system
2019-11-18 04:10:04.0   File transfer completed
2019-11-18 04:10:17.0   All done!
```

FILE STATS

DATABASE PROGRESS TRACKER

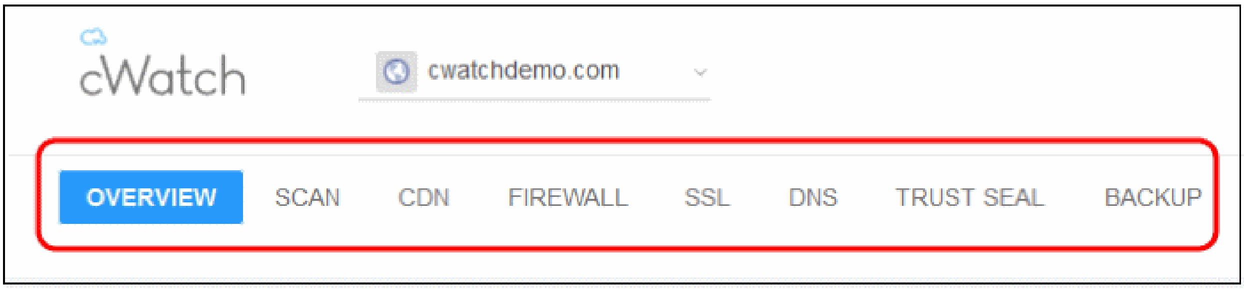
```
2019-11-18 04:00:53.0   Backup request received
2019-11-18 04:02:45.0   All done!
```

- **File Progress Tracker** – Step-by-step details of website files transferred to the backup server.
- **Database Progress Tracker** – Step-by-step details about the database backup operation.
- **File Stats** – The number of files added, removed or modified. Click the download button to view the exact files involved:

Click here for more information about backup records and file statistics.

Use the cWatch Interface

- The cWatch dashboard contains an at-a-glance summary of security status your websites
  - Click the 'cWatch' logo in the top-left corner to open the dashboard at any time
- The drop-down on the left lets you choose the domain you want to manage and to view threat statistics.
- Links to all major areas of the interface are in the top menu:



Overview – Shows security and performance data from each cWatch module. See **https://help.comodo.com/topic-285-1-848-11010-Website-Overview.html** for more details.

Scan – There are three types of scan:

1. **Website scan** - A first-level scan that checks front-end files for threats, blacklist status, missing headers, SSL errors, and more. The website scan runs automatically right after you add a site to cWatch. No configuration required. See **https://help.comodo.com/topic-285-1-848-15277-Website-Scans.html** for more details.

2. **Website Files Security scan** - A full, deep-scan of your website's front and back-end files for all known threats. You can schedule malware scans to run at a time that suits you, and you can also configure automatic removal of discovered threats. You need to upload our .php file to the server to enable malware scans. See **https://help.comodo.com/topic-285-1-848-11011-Website-Files-Security-Scans.html** for more details.

3. **Vulnerability scan** – there two types of vulnerability scan:
   i. **CMS vulnerability scans** - Identifies weaknesses in your content management system (CMS). You can enable weekly automatic scans on each protected site, and can also run on-demand scans at any time. The scanner supports the following types of CMS:
      WordPress
      Joomla
      Drupal
      ModX
      Typo3

   ii. **OWASP top-ten threats** – Scans for the top-10 threats identified by the Open Web Application Security Project (OWASP). You can schedule weekly automatic scans on each protected site, and run on-demand scans at any time.

See **https://help.comodo.com/topic-285-1-848-11492-Vulnerability-Scans.html** for more details.

- **CDN** - Configure the cWatch content delivery network and view traffic for your site. This includes total data usage, status/error-code distribution, and the geographic locations from which your site was accessed. See **https://help.comodo.com/topic-285-1-848-11495-Content-Delivery-Network.html** to find out more.
- **Firewall** - Configure Web Application Firewall (WAF) policies for the domain and create your own custom firewall rules. View attack and threat statistics on your domains. See **https://help.comodo.com/topic-285-1-848-13906-Firewall-Rules.html** for more information.
- **SSL** - Secure the traffic between the CDN edge servers and your website visitors. You can get a complimentary SSL certificate from Comodo. Alternatively, you can upload an existing certificate. See **https://help.comodo.com/topic-285-1-848-12464-SSL-Configuration.html** for more details.
- **DNS** - Configure DNS and nameservers in order to enable cWatch protection. See **https://help.comodo.com/topic-285-1-848-12463-DNS-Configuration.html** for more information.
- **Trust Seal** - Add a cWatch site seal on managed websites. There are two types of seals: 'Malware Free' and 'Protected'. See **https://help.comodo.com/topic-285-1-848-13683-Add-Trust-Seal-to-your-Websites.html** for more details.
- **Backup** – Backup your entire website and databases to our highly secure cWatch servers. Restore your website with a single click. See **https://help.comodo.com/topic-285-1-848-15272-Back-up-your-Website.html** for more information.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street
Clifton, NJ 07013
United States
Tel : +1.888.266.6361
Tel : +1.703.581.6361
https://www.comodo.com
Email: **EnterpriseSolutions@Comodo.com**