COMODO
Creating Trust Online®

Comodo
cWatch Web Security

Software Version 4.6

Quick Start Guide

Guide Version 4.6.010419

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 Web Security includes a subscription to a content delivery network (CDN) service, helping to accelerate site performance.

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

Purchase Website Licenses

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

- Licenses are charged per-website. Sub-domains are not covered if you buy a license for a primary domain. Each sub–domain must be purchased as a separate license.
- You can add multiple license types if you want to implement different levels of protection on each site.
- You can associate websites with licenses in the cWatch interface. See **Add Websites** for more details.

Available license types are:

- Basic
- Pro
- Premium

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

Feature/Service	Premium	Pro	Basic
Malware Detection and Removal			
Hack repair and restoration	✓	✓	One time/month
Complete blacklist site removal	✓	✓	✗
Spam and website filtering	✓	✓	✓

Daily vulnerability (OWASP) detection scan	✓	✓	✓
Trojan detection and protection	✓	✓	✓
Vulnerability repair and restoration	✓	✓	One time/month
Brand reputation monitoring	✓	✓	✓
Traffic hijacking recovery	✓	✓	One time/month
SEO poisoning recovery	✓	✓	One time/month
Automatic advanced threat discovery	✓	✓	✓
Automated malware removal	✓	✓	One time/month
Command and control server comm detection	✓	✓	✓
Security Information and Event Management			
Real time threat and breach protection	✓	✓	✗
Advanced persistent threat identification	✓	✓	✗
Incident management and remediation	✓	✓	✗
Anomaly search and detection	✓	✓	✗
24/7 Cyber Security Operations Center			
Dedicated c.s.o.c. analyst	✓	✗	✗
Expert tuning and configuration mgmt.	✓	✗	✗
Reverse malware and suspect engineering	✓	✗	✗
Threat investigation and analysis	✓	✗	✗
Correlations over multiple incidents	✓	✓	✗
Integration with threat intelligence	✓	✓	✓
Alerting and incident escalations	✓	✓	✓
Managed Web Application Firewall (WAF)			
Managed updates	✓	✓	✗
Fine grained control	✓	✗	✗
Bot protection	✓	✓	✗
Scraping protection	✓	✓	✗
Enterprise control	✓	✓	✗
SQL injection prevention	✓	✓	✗
XSS injection - cross site scripting protection	✓	✓	✗
XMLRPC protection	✓	✓	✗
Bruteforce protection	✓	✓	✗

Block access via backdoor files	✓	✓	✗
Illegal resource access protection	✓	✓	✗
Blacklisting of clients, countries and Ips	✓	✓	✗
Information reveal prevention	✓	✓	✗
OWASP top 10 protection	✓	✓	✗
WAF Rule update with customer request	✓	✗	✗
Content Delivery Network (CDN)			
Layer 7 DDoS protection	✓	✓	✓
Layer 3, 4, 5, 6 DDoS protection	✓	✓	✓
Instant purge	✓	✓	✓
Advanced website acceleration	✓	✓	✓
Asset preloading	✓	✓	✓
Cache / header settings	✓	✓	✓
Anycast DNS	✓	✓	✓
Uptime SLA	✓	✓	✓
Speed	✓	✓	✓
Scale	✓	✓	✓
Load Balancing	✓	✓	✓
HTTPS - SSL unique certificates	✓	✓	✓
Performance Optimization	✓	✓	✓
Technical Support			
24 / 7 chat	✓	✓	✓
Planning	✓	✓	✗
Installation	✓	✓	✓
Training	✓	✓	✗
Troubleshooting	✓	✓	✓
Maintenance	✓	✓	✗
Upgrades	✓	✓	✓
Removal	✓	✓	One time/month

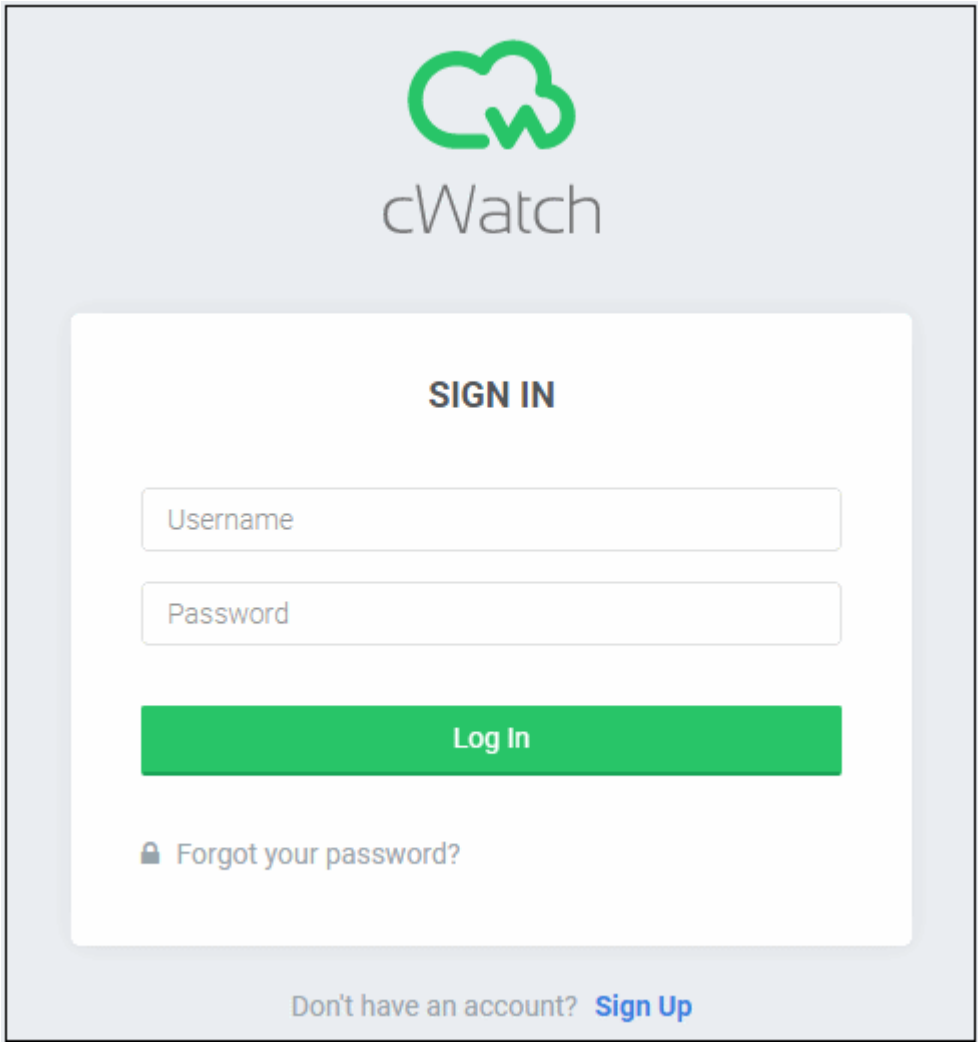
After completing the purchase process:

- New users - A Comodo account will be created for you at **https://accounts.comodo.com**. An email containing your subscription ID and the link to activate your account will be sent to you. You can activate your account by following the link in the mail.

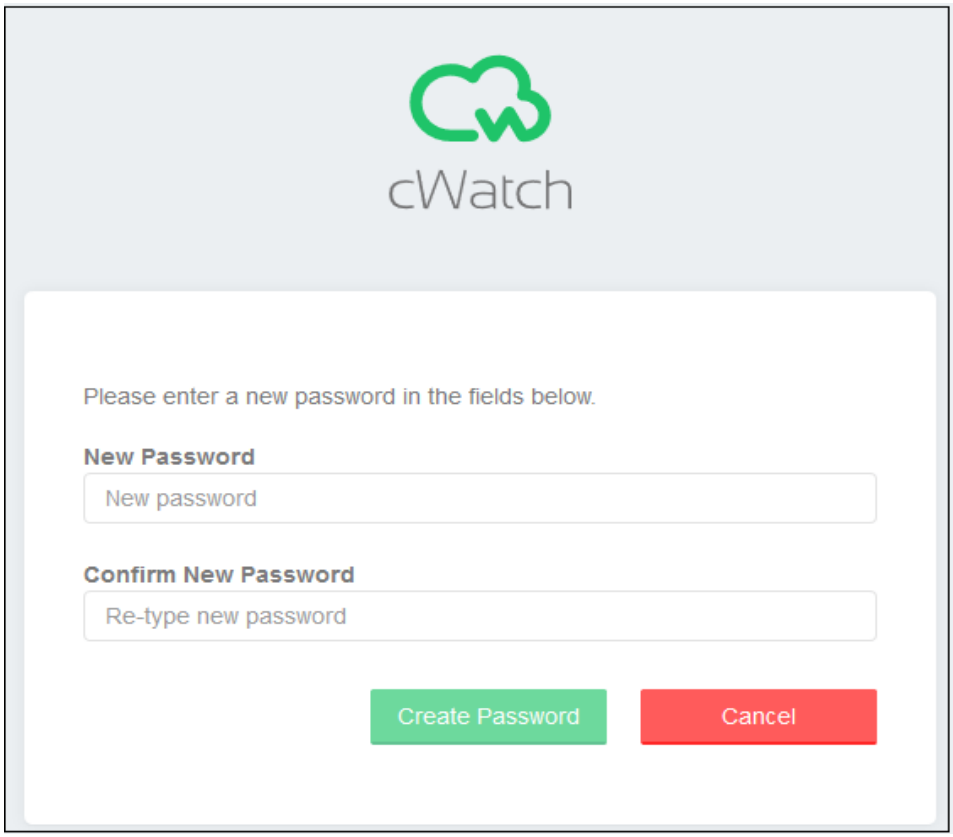
- Existing users - An acknowledgment mail will be sent to you containing your license key.
- Please save your license key in a safe location.
- Next, login to cWatch at **https://login.cwatch.comodo.com/login**

Login to cWatch

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



- First time login – get the username and password from the cWatch account creation email. We strongly recommend you change your password after first login.
  - Click 'Forgot your password?' to reset your password.
  - Enter your mail address and click 'Submit' on the confirmation screen.
  - You will receive a password reset mail.
  - Click 'Reset Password' to the open the password config page.
  - Create and confirm your new password then click 'Create Password':



-
- Click 'Go to Login' on the confirmation screen to access your account with your new password.

Add Websites

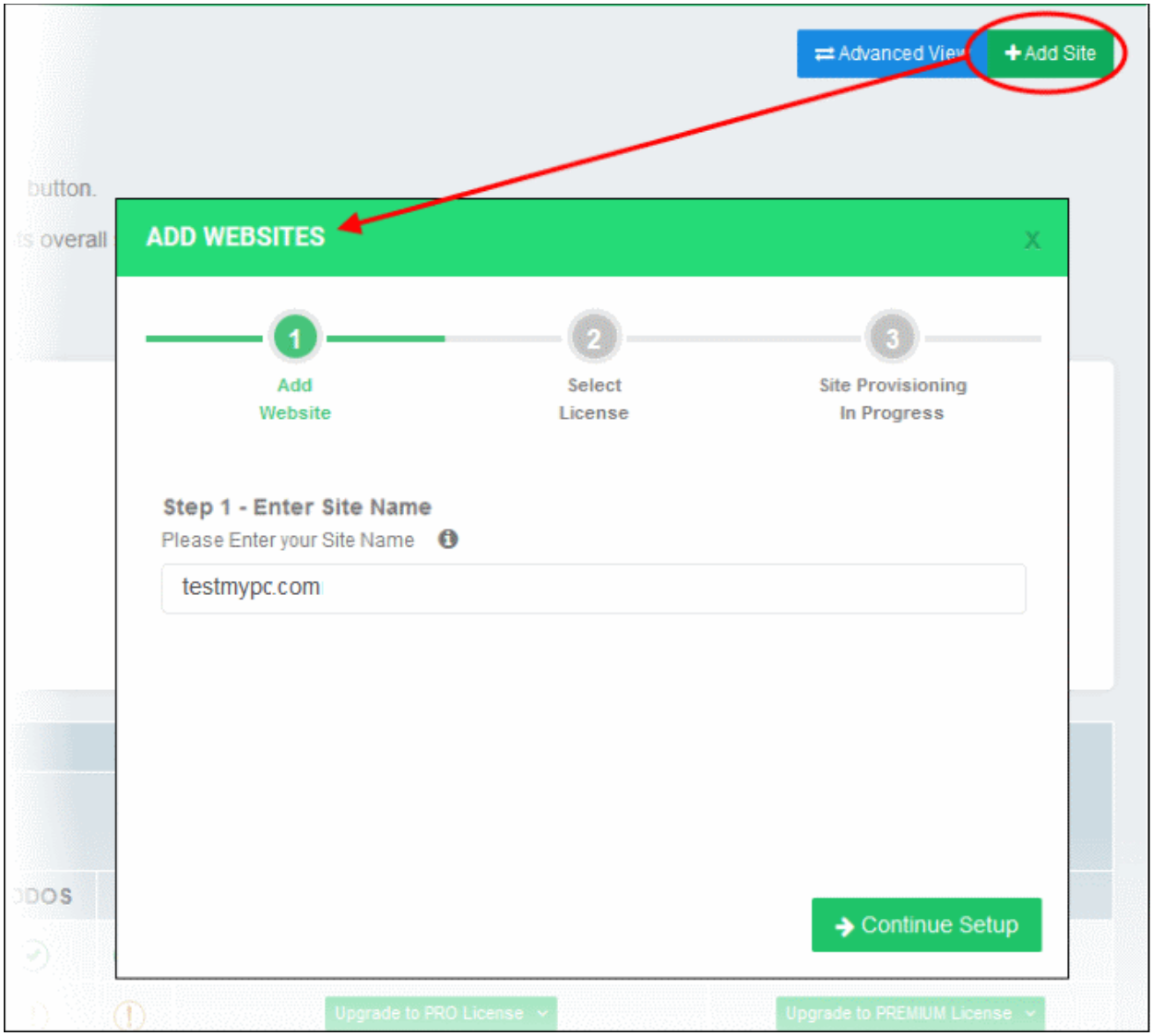
- You need to add websites to cWatch to enable protection and take advantage of the content delivery network (CDN).
- The number of domains you can add depends on your license (explained **here**).
- Once added, you can configure threat monitoring and CDN settings for each site. See the next section, **Configure your Websites**, for more details.

To add a new domain

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

The dashboard will appear by default

- Click 'Add Site' at top-right to start the 'Add Websites' wizard:



The wizard contains three steps:

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

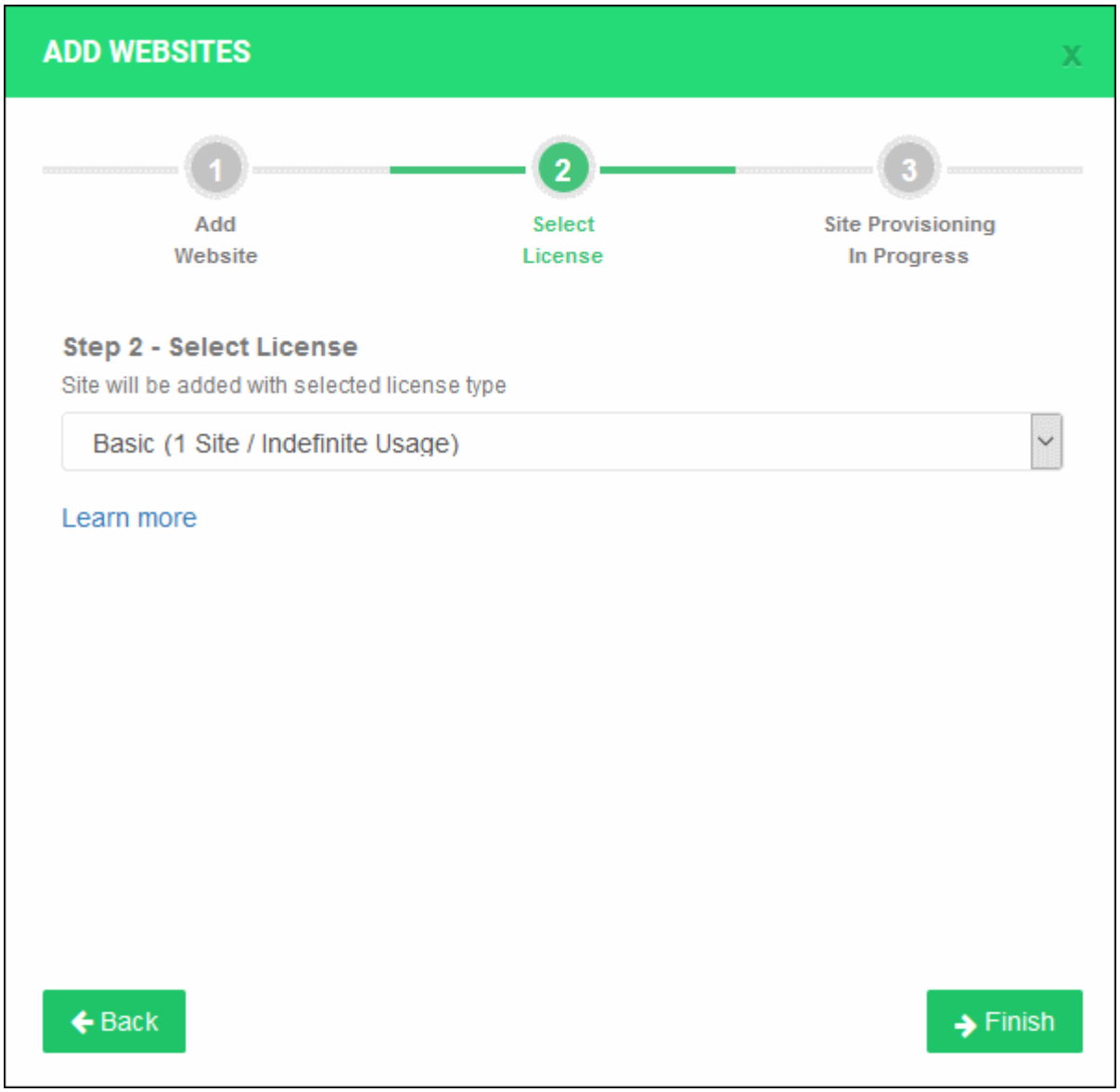
Step 1 - Register your website

- Enter the domain you want to register. Do not include 'www' at the start.
- Click 'Continue Setup'

Step 2 - Select License

Next, choose the license type you wish to activate on the site.

- cWatch features vary according to license type. Details are available **here.**
- The drop-down displays all licenses that you have purchased.
- Choose the type of license you wish to associate with the domain you entered in step 1
- Click 'Finish' to proceed



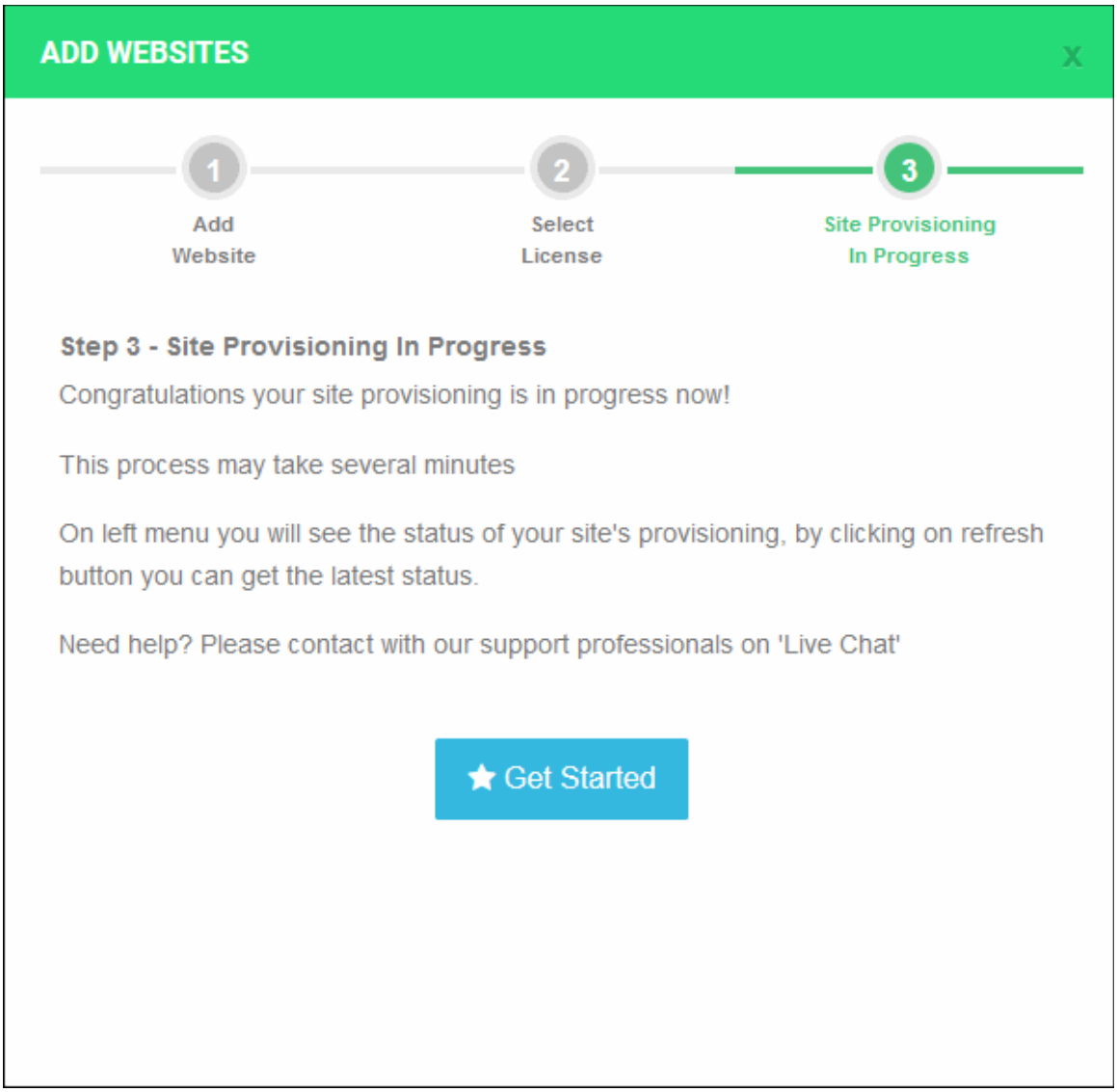
- Each 'Enterprise' license covers up to ten sub-domains of a primary domain.
- You have to specify each sub-domain after registering the primary domain.
- You should select 'Enterprise' as the license type for each sub-domain in order for it to be covered under the license of the primary domain.
- Each sub-domain also has to be configured separately for malware scanning and the CDN service. See the next section, **Configure your website(s)**, for more details.

Step 3 – Finalization

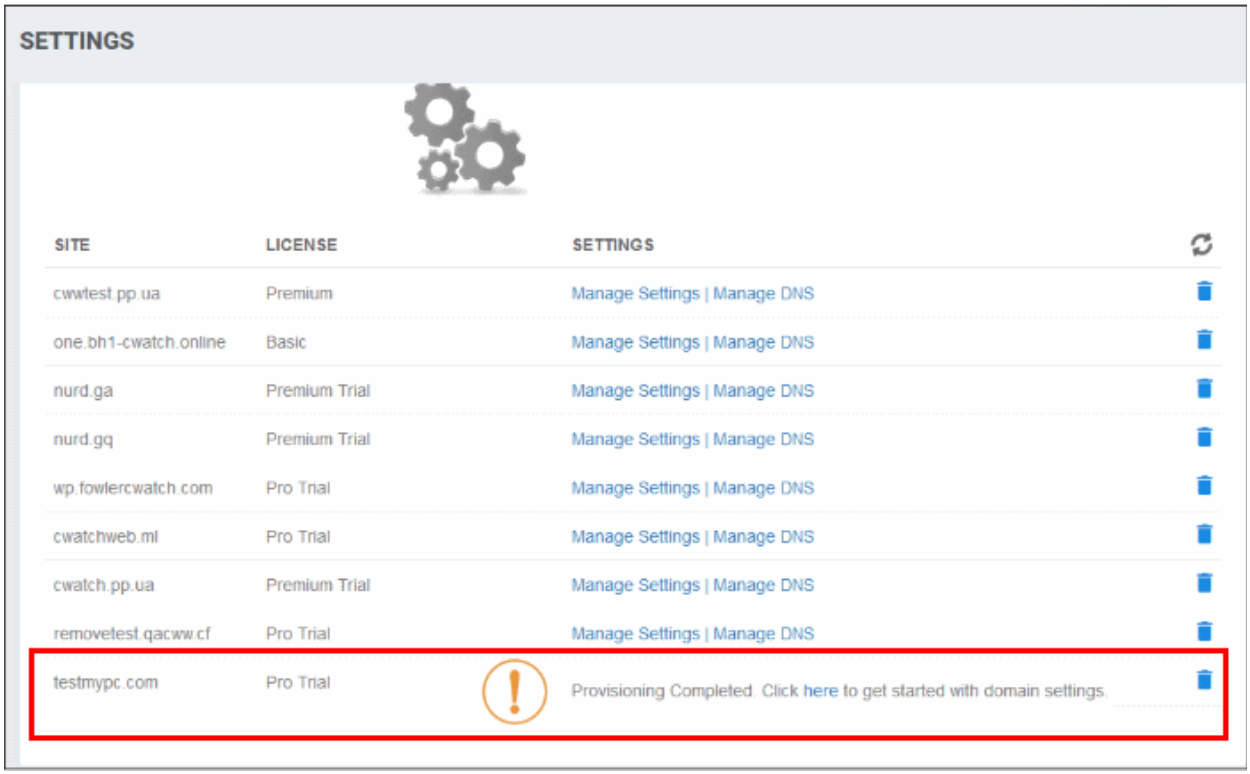
The final step is to configure your DNS settings.

- cWatch will generate a CNAME DNS record for the website you just enrolled
- You need to add this record to the DNS entry for your domain to route your site traffic through the CDN.
- To view the CNAME details:
  - Click the website name in the main menu on the left
  - Click 'Settings' > 'Domain'

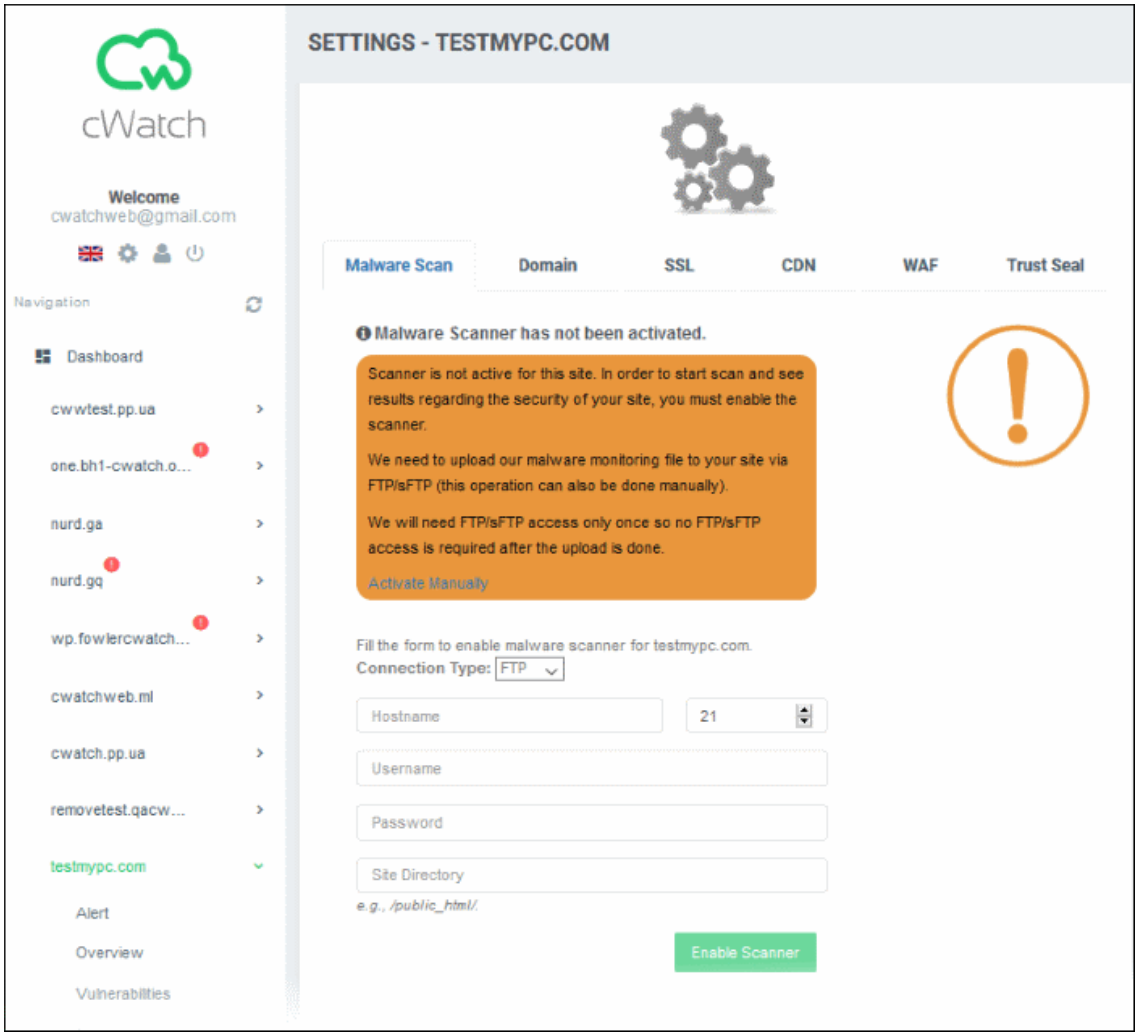
- Your web host may be able to help you with this step. Guidance is also available at **https://support.google.com/a/topic/1615038?hl=en**.



- Click 'Get Started'. You will be taken to the cWatch 'Settings' page:
- The 'Settings' page shows all websites added to your account.



- Click the 'here' link to setup protection (highlighted in red box):
- See '**Website Configuration**' for help to configure for malware scans, CDN, firewall rules and more.



Note:

- cWatch generates a CNAME DNS record for the website you just enrolled
- You need to add this record to the DNS entry for your domain to route site traffic through the CDN.
- To view the CNAME details:
  - Click the website name in the main menu on the left
  - Click '**Settings**' > '**Domain**'
- 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 can add the CNAME entry to the DNS records later. See **Domain Configuration Instructions** for more details.

- Repeat the process to add more websites.

Configure your Websites

The next steps are to:

- Upload or create an SSL certificate so https sessions can be protected. See **SSL Configuration** for more details.
- Configure DNS in order to enable cWatch protection, the content delivery network, and the Web Application

Firewall (WAF). See **Domain Configuration Instructions** for more details.

- Configure malware scans on the site. See **Configure Malware Scan** for more details.
- Configure CDN settings in order to accelerate site performance and add security to your websites. See **Configure CDN Settings** for more details.
- Configure Web Application Firewall (WAF) settings. See **Configure WAF Settings** for more details.
- Configure your site's trust seal. See **Trust Seal settings** for more details.

SSL Configuration

- An SSL/TLS certificate is placed on a website to encrypt data that passes between the user's browser and the web-server.
- Websites that use an SSL certificate have an address that begins with 'https', with the 's' standing for 'secure'. For example, **https://www.mywebsite.com**

There are two ways to enable HTTPS security:

- Complimentary SSL – get a free certificate from Comodo.
- Bring Your Own SSL (recommended)

Option A – Complimentary SSL

- A free certificate will be installed on the CDN edge servers. This will encrypt traffic between the CDN servers and your visitors who connect to those servers.
- The complimentary certificate will *not* secure the connection between your server (where your site is hosted) and the CDN (where your website is cached).
- You must change your domain's authoritative DNS servers to Comodo to get the certificate. **Click here** to find out how.
- **Click here** for help to install the free SSL certificate

Option B – Bring your Own SSL

- Secures traffic between your web-server and the cWatch CDN edge servers
- Eliminates privacy risks & vulnerabilities such as eavesdropping and 'Man-in-the-Middle' attacks
- **Click here** to find out how to upload your own SSL certificate to cWatch

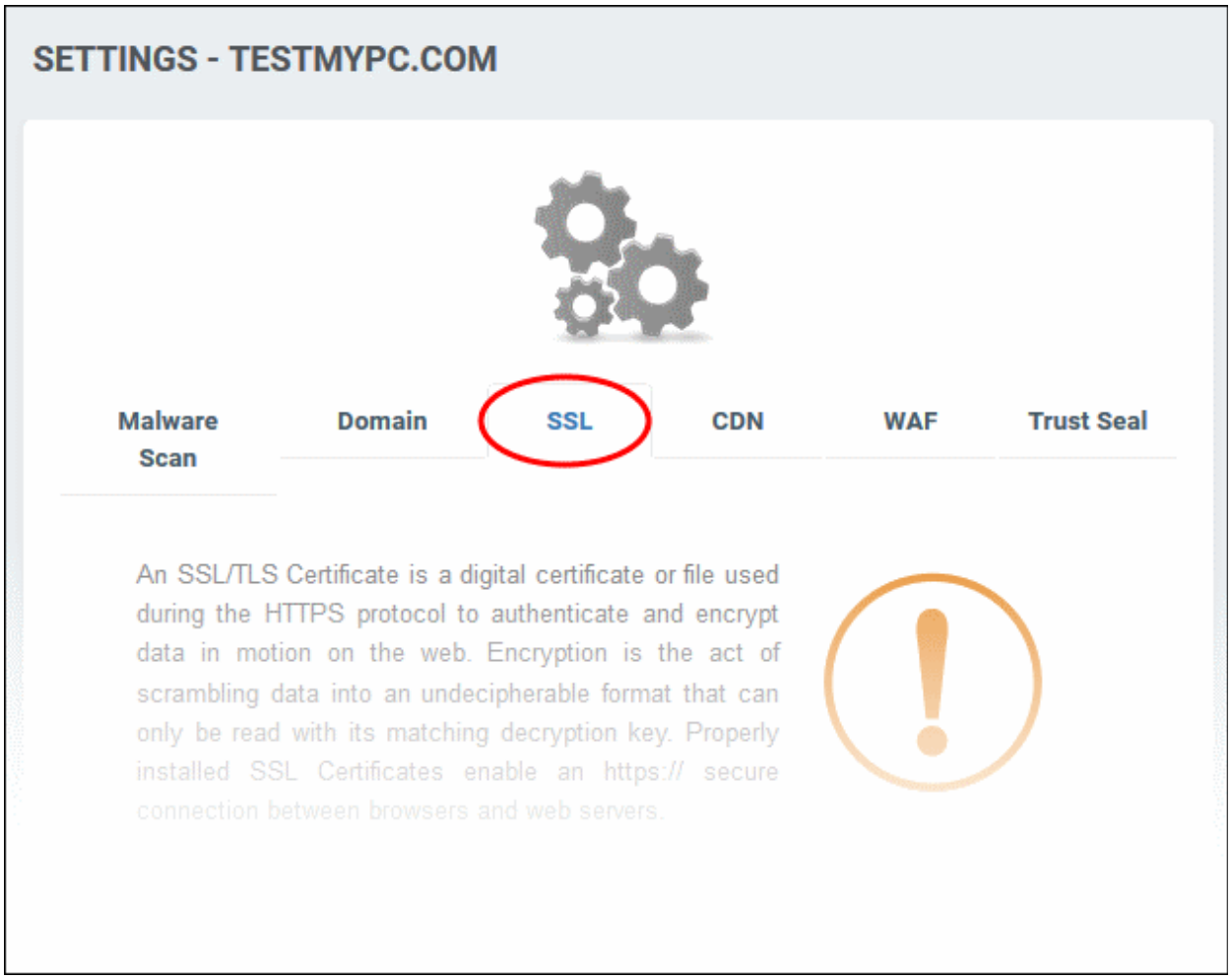
Install Complimentary SSL Certificate

- Click the settings cog under your username on the left
- Click 'Manage Settings' in the row of the site whose SSL you wish to manage.

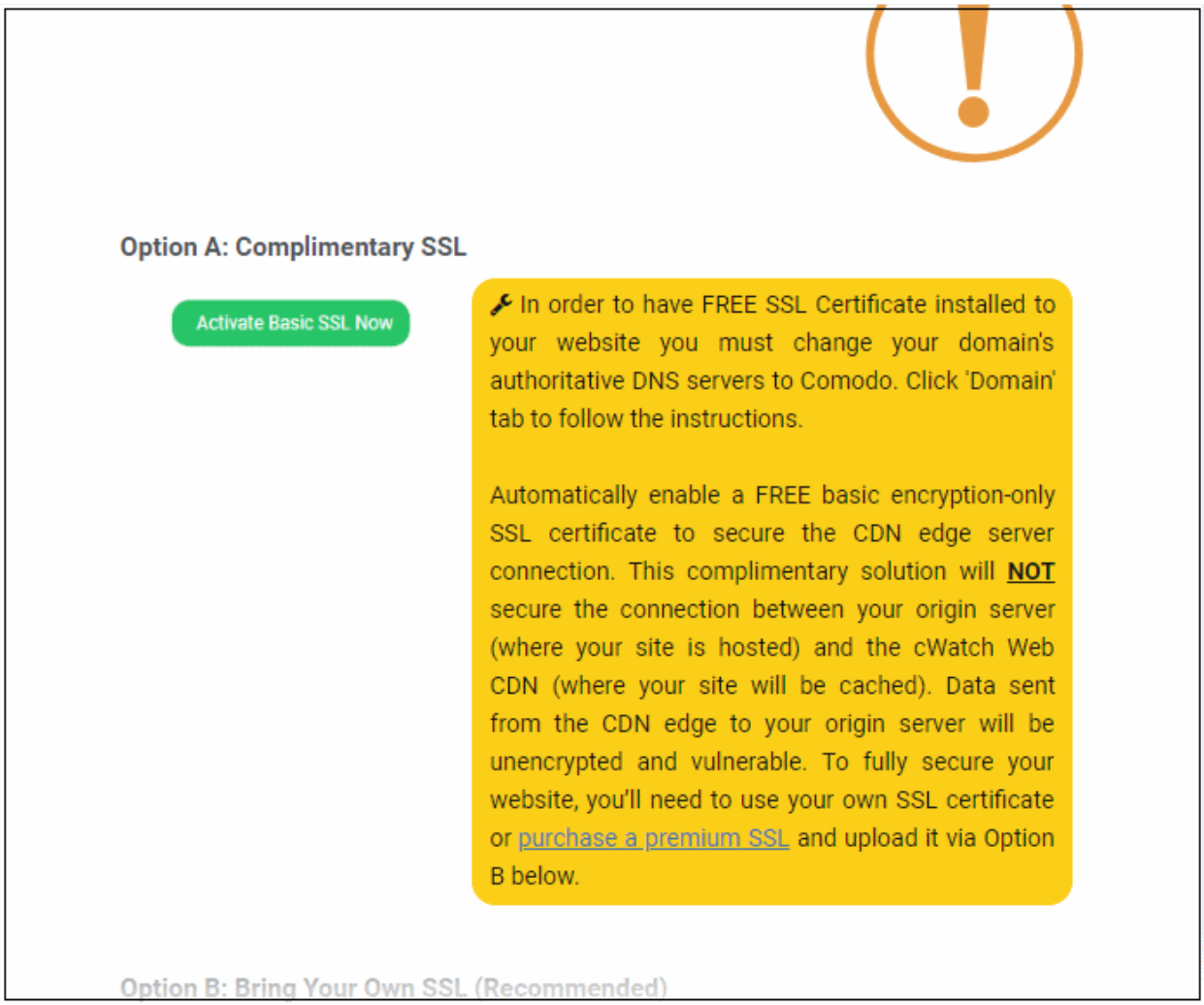
OR

- Click the website name in the left menu then 'Settings'

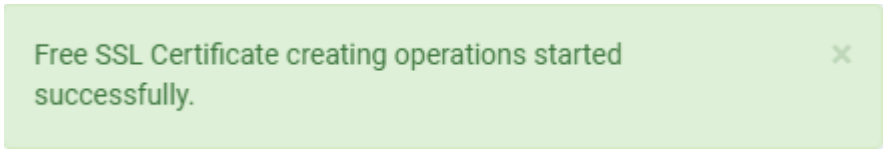
In the settings page, click the 'SSL' tab:

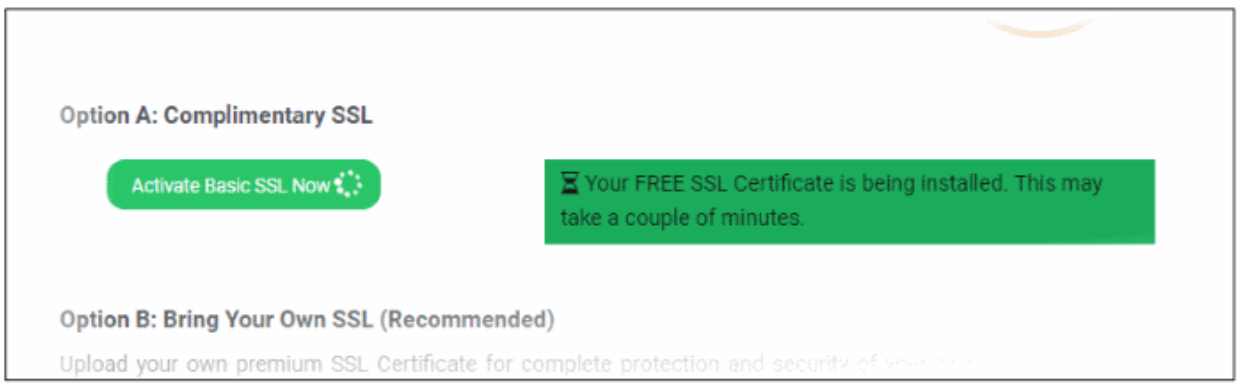


- Scroll down to 'Option A: Complimentary'

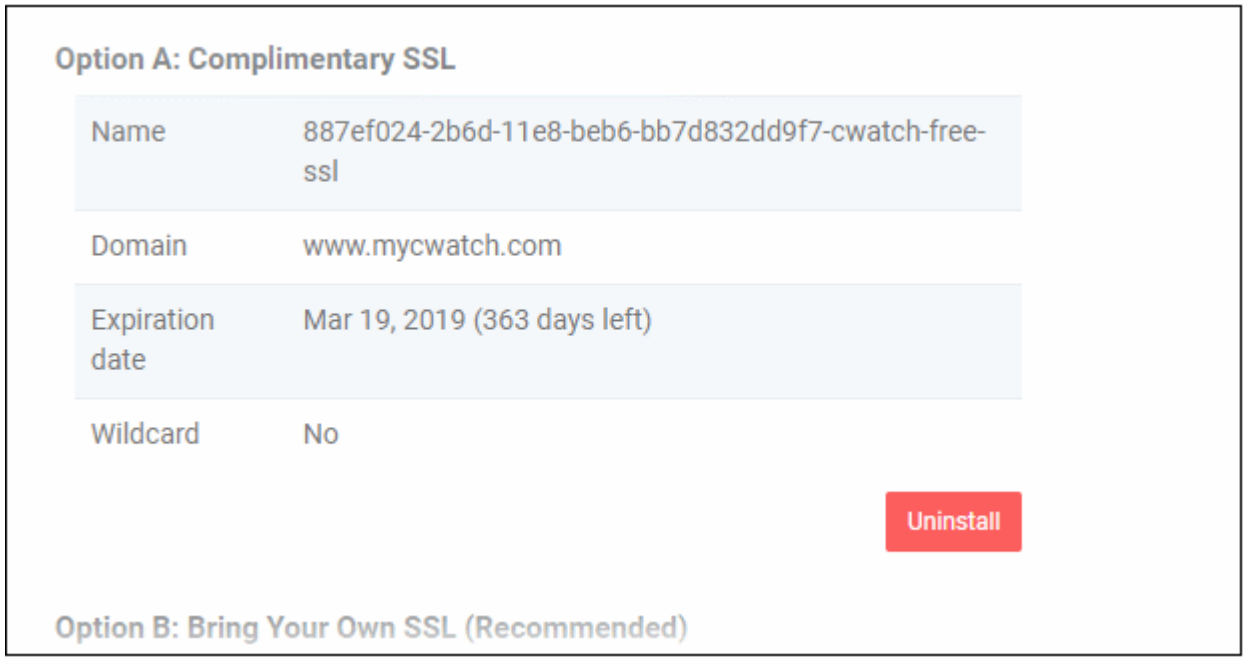


- Click 'Active Basic SSL Now'
- You will see the following alert to indicate certificate provisioning has started:





- The process will take a few minutes to complete.



- The certificate will be installed on the CDN edge servers and will encrypt traffic between the CDN and end-user clients.
- It will not encrypt the traffic between your web-server and the CDN. You need to upload your own certificate to encrypt this traffic. See '**Upload your own SSL Certificate**' for more details.

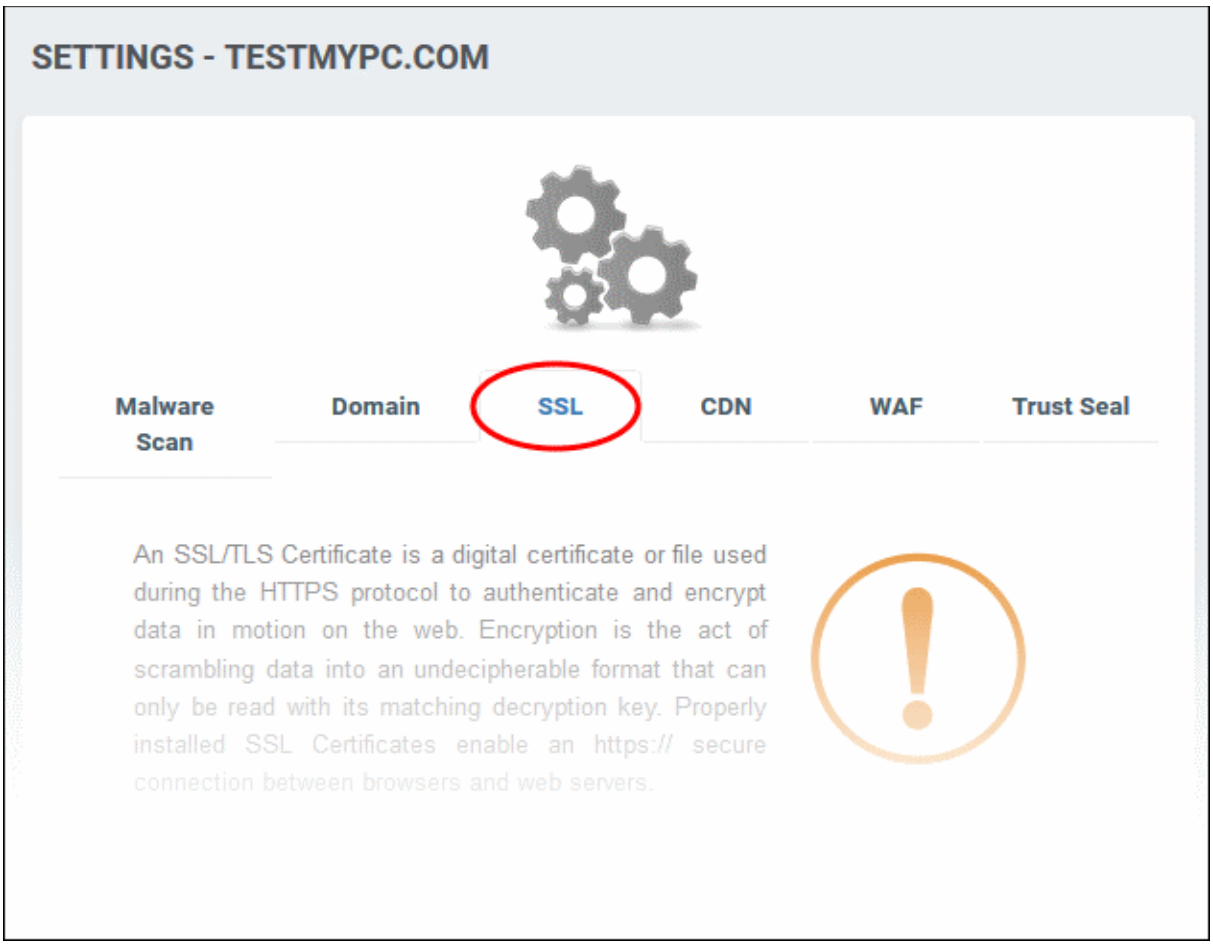
Upload your own SSL Certificate

- Click the settings cog under your username on the left
- Click 'Manage Settings' next to the site for which you want to configure SSL

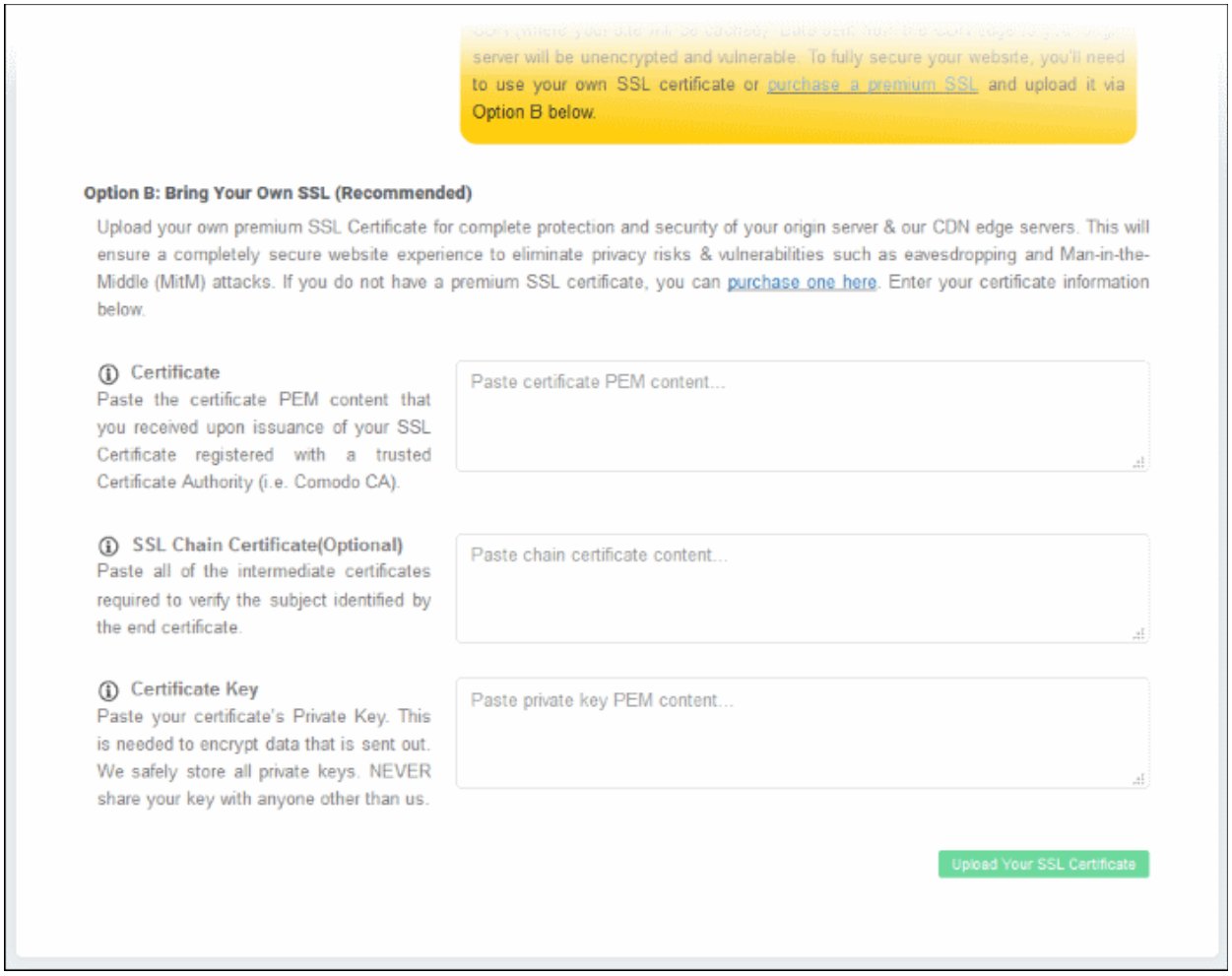
OR

- Click the website name on the left menu, then 'Settings'

Click the 'SSL' tab in the settings page:



- Scroll down to 'Option B: Bring Your Own SSL' section.



The form for adding your SSL certificate will appear.

SSL Protection Settings - Table of Parameters	
Parameter	**Description**
Certificate	Paste the content of your certificate. The content you need looks something like this: -----BEGIN CERTIFICATE----- MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGEwJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBAcTAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECxMC VU4xFDASBgNVBAMTC0hlcm9uZyBZYW5nMB4XDTA1MDcxNTIxMTk0N1oXDTA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAgTAlBOMQswCQYDVQQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTAlVOMRQwEgYDVQQDEwtIZXJvbmcgWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBewKE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbMOoRcKK9vEcgMtcLFuQTWDl3RAgMBAAGj gbEwga4wHQYDVR0OBBYEFFXI70krXeQDxZgbaCQoR4jUDncEMH8GA1UdIwR4MHaA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMQswCQYDVQQGEwJDTjELMAkGA1UE CBMCUE4xCzAJBgNVBAcTAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECxMCVU4xFDAS

	BgNVBAMTC0hlcm9uZyBZYW5nggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEE 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. This will encrypt the traffic between the CDN and your customers (the CDN hosts a cached version of your site).
- Note. You should already have installed this certificate on your own website. This ensure communications between your site and the CDN are also encrypted.

Domain Configuration Instructions

Important Note – If you are using an SSL certificate on your site, you must configure SSL settings in cWatch to avoid interruptions to HTTPS traffic. See **SSL Configuration** for more details.

After **adding a website** to cWatch, you next have to configure DNS settings. You need to do this in order to activate cWatch protection, the content delivery network, and the Web Application Firewall (WAF).

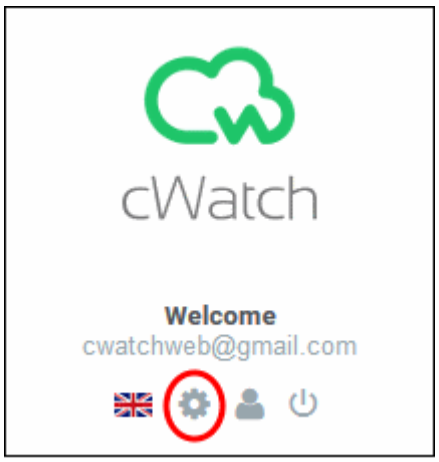
There are two ways this can be done:

- **Option A - Change your domain's authoritative DNS servers to Comodo**
- **Option B - Enter DNS records explicitly**

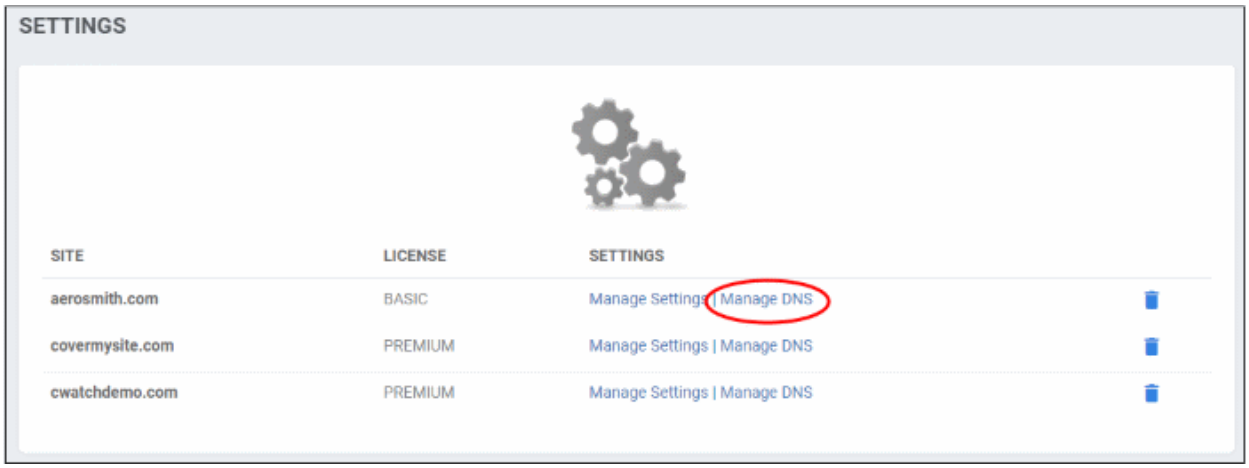
Option A – Change your domain's authoritative DNS servers to Comodo

Important Note – After changing your domain's DNS to Comodo, you have to use cWatch to manage your DNS. For example, changes to your MX records must be done in cWatch and can no longer be done in your web host's DNS management page.

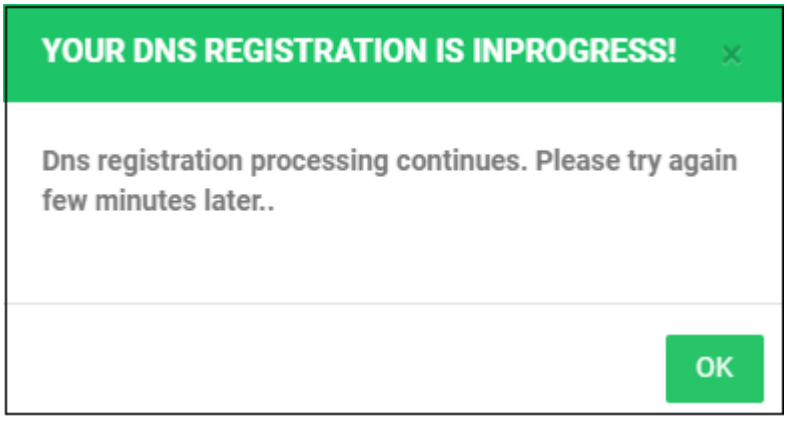
- Click the settings cog icon under your username



- Click 'Manage DNS' in the row of the website you are working on:

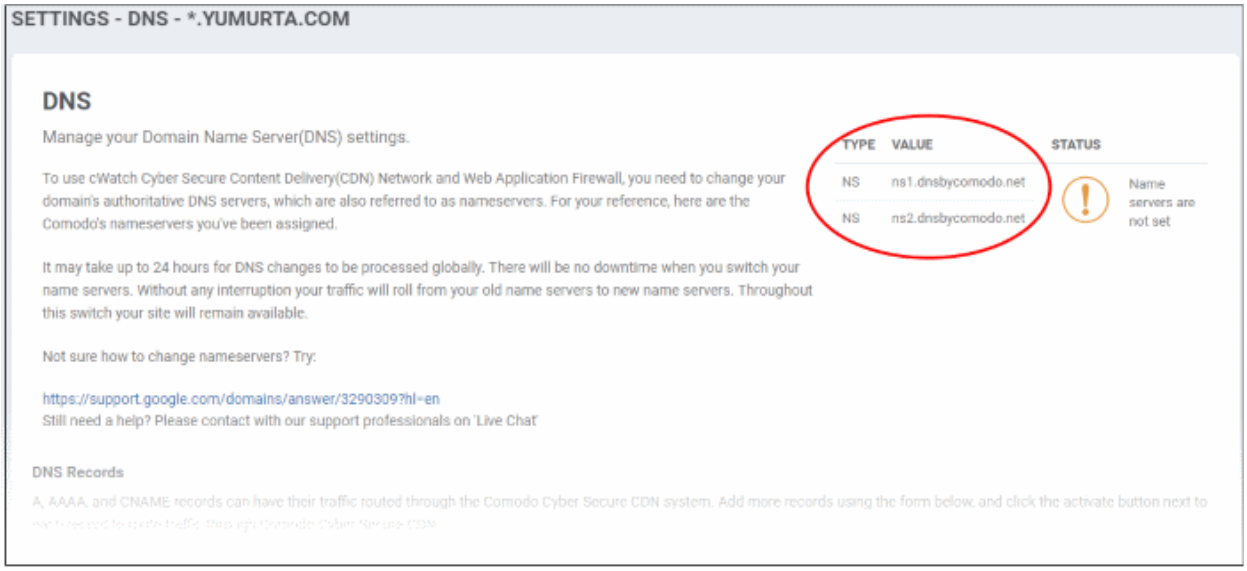


You will see the following message the first time you click:

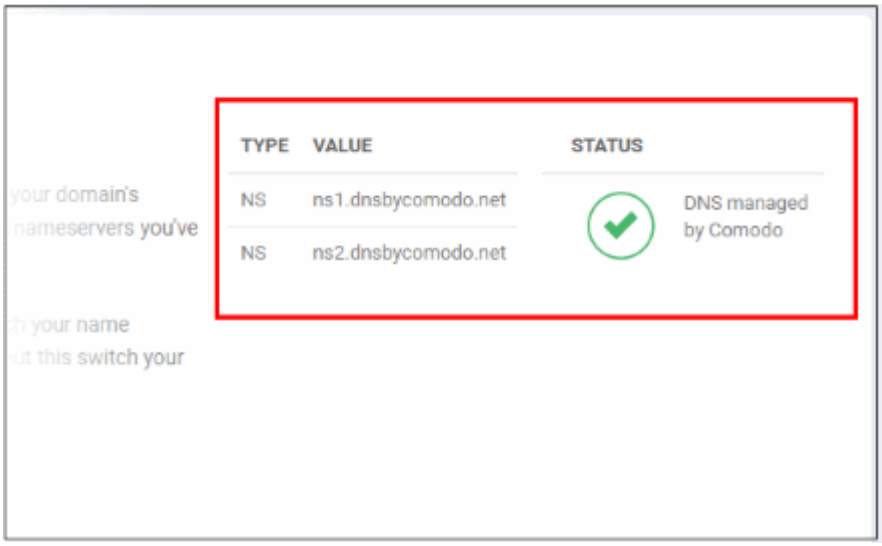


Registration takes a few minutes to complete. Once done:

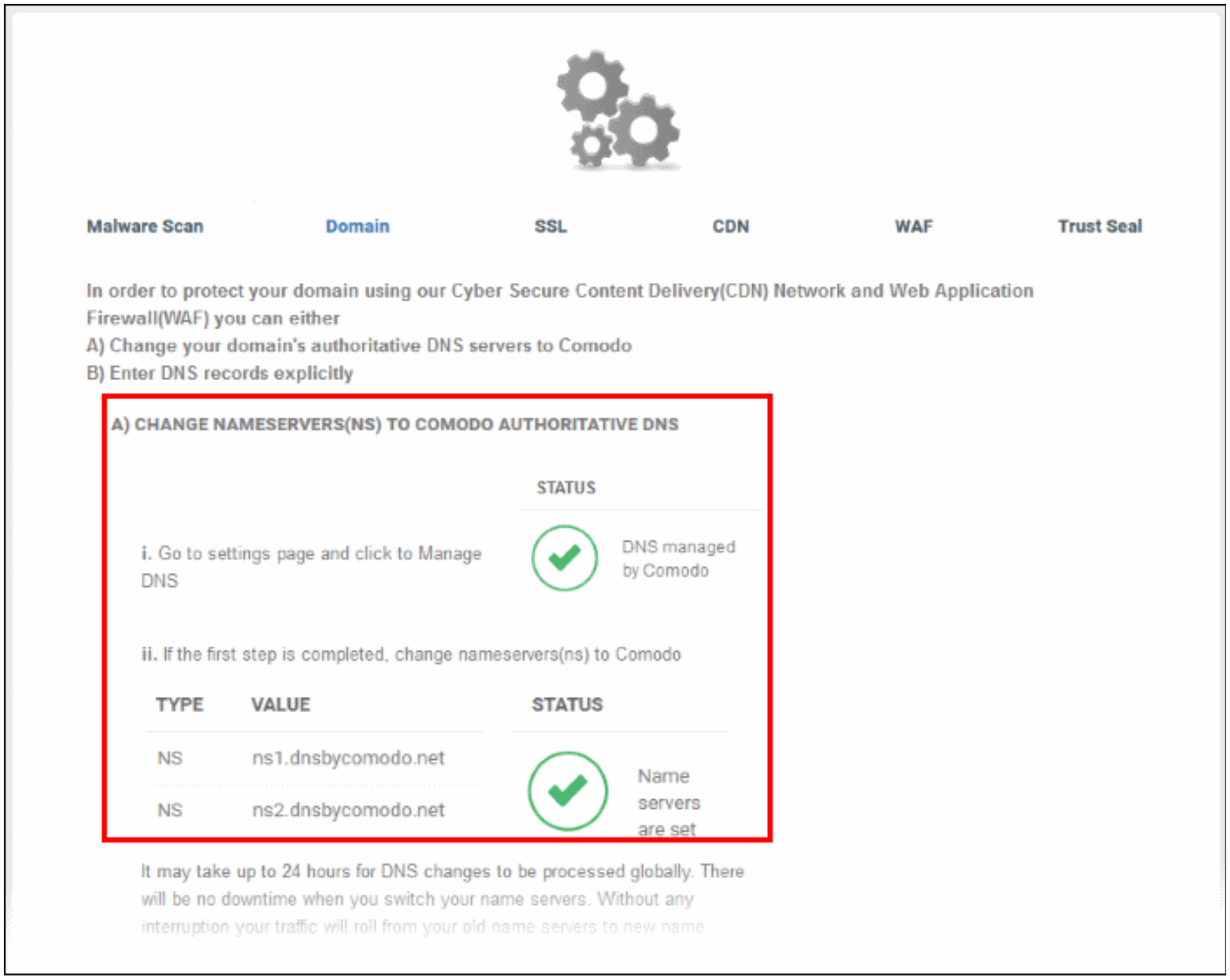
- Open the main settings page again and click 'Manage DNS'
- Take a note of the nameserver details shown at the top-right:



- Go to your website's DNS management page and enter the new nameservers
- See **https://support.google.com/domains/answer/3290309?hl=en** if you need more help changing nameservers
- DNS status will change to 'Managed by Comodo' once the nameservers have been successfully updated:



- You can also view nameserver update status in the 'Domain' tab:
  - Click the website name in menu on the left the left
  - Click 'Settings' > 'Domain' tab



You can view the nameserver update status in option A.

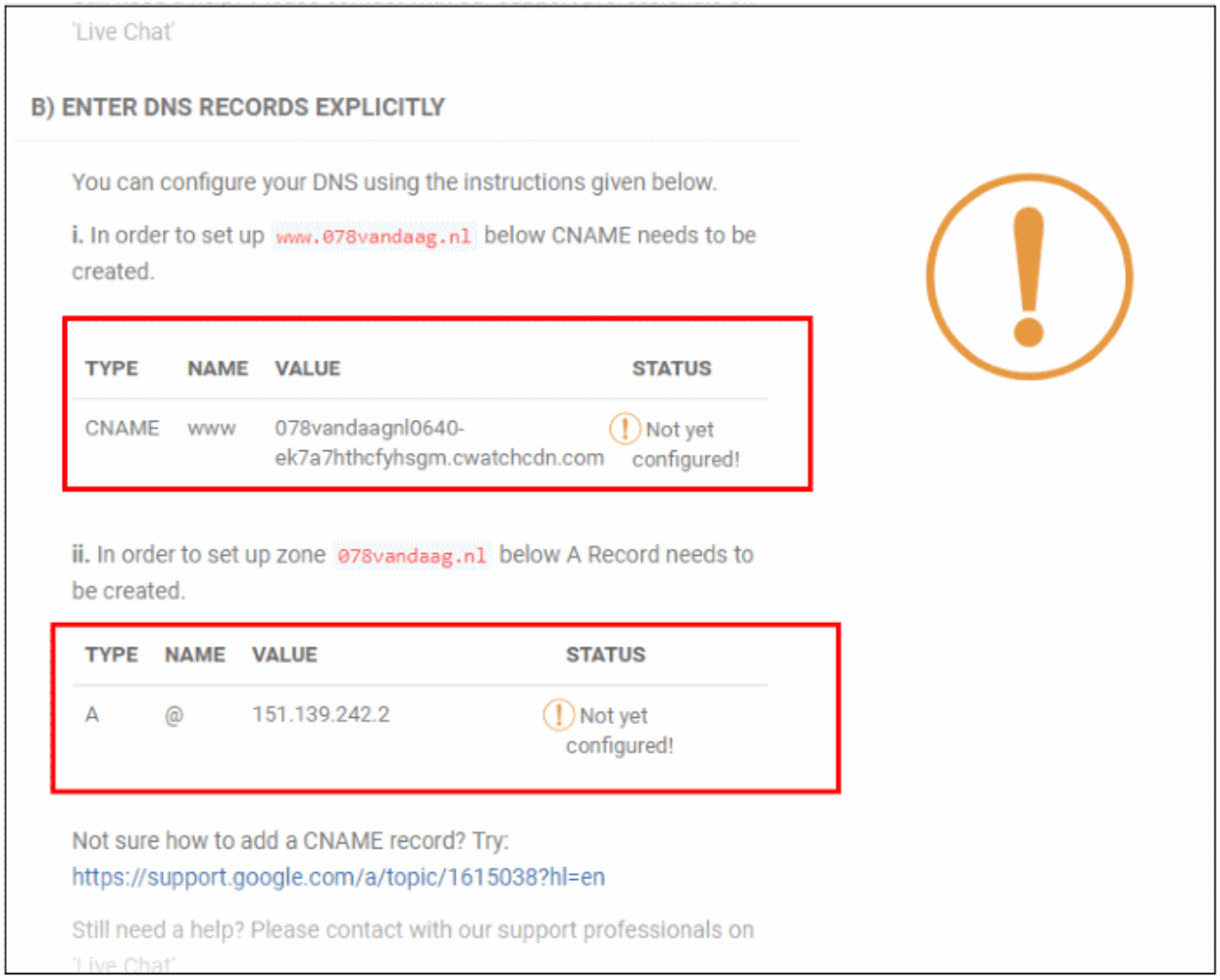
- It may take up to 24 hours for DNS changes to be processed globally.
- There will be no downtime on your site when you switch name servers.

Option B – Enter DNS records explicitly

Important Note – If you are using an SSL certificate on your website, you must configure SSL settings in cWatch to avoid interruptions to HTTPS traffic. See **SSL Configuration** for more details.

To enter DNS records explicitly:

- First note the 'CNAME' and 'A' records for the site
- You can find these records in 'Settings' > 'Manage Settings' > 'Domain' > scroll down to 'Option B – Enter DNS Records Explicitly':


'Live Chat'

B) ENTER DNS RECORDS EXPLICITLY

You can configure your DNS using the instructions given below.

i. In order to set up `www.078vandaag.nl` below CNAME needs to be created.

TYPE	NAME	VALUE	STATUS
CNAME	www	078vandaagnl0640-ek7a7hthcfyhsgm.cwatchcdn.com	Not yet configured!

ii. In order to set up zone `078vandaag.nl` below A Record needs to be created.

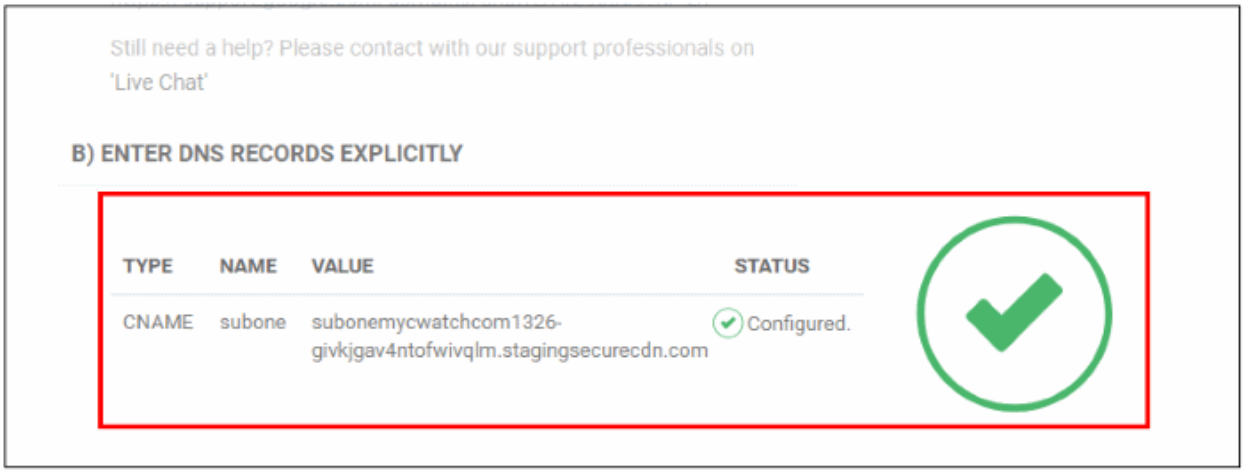
TYPE	NAME	VALUE	STATUS
A	@	151.139.242.2	Not yet configured!

Not sure how to add a CNAME record? Try:
https://support.google.com/a/topic/1615038?hl=en

Still need a help? Please contact with our support professionals on 'Live Chat'

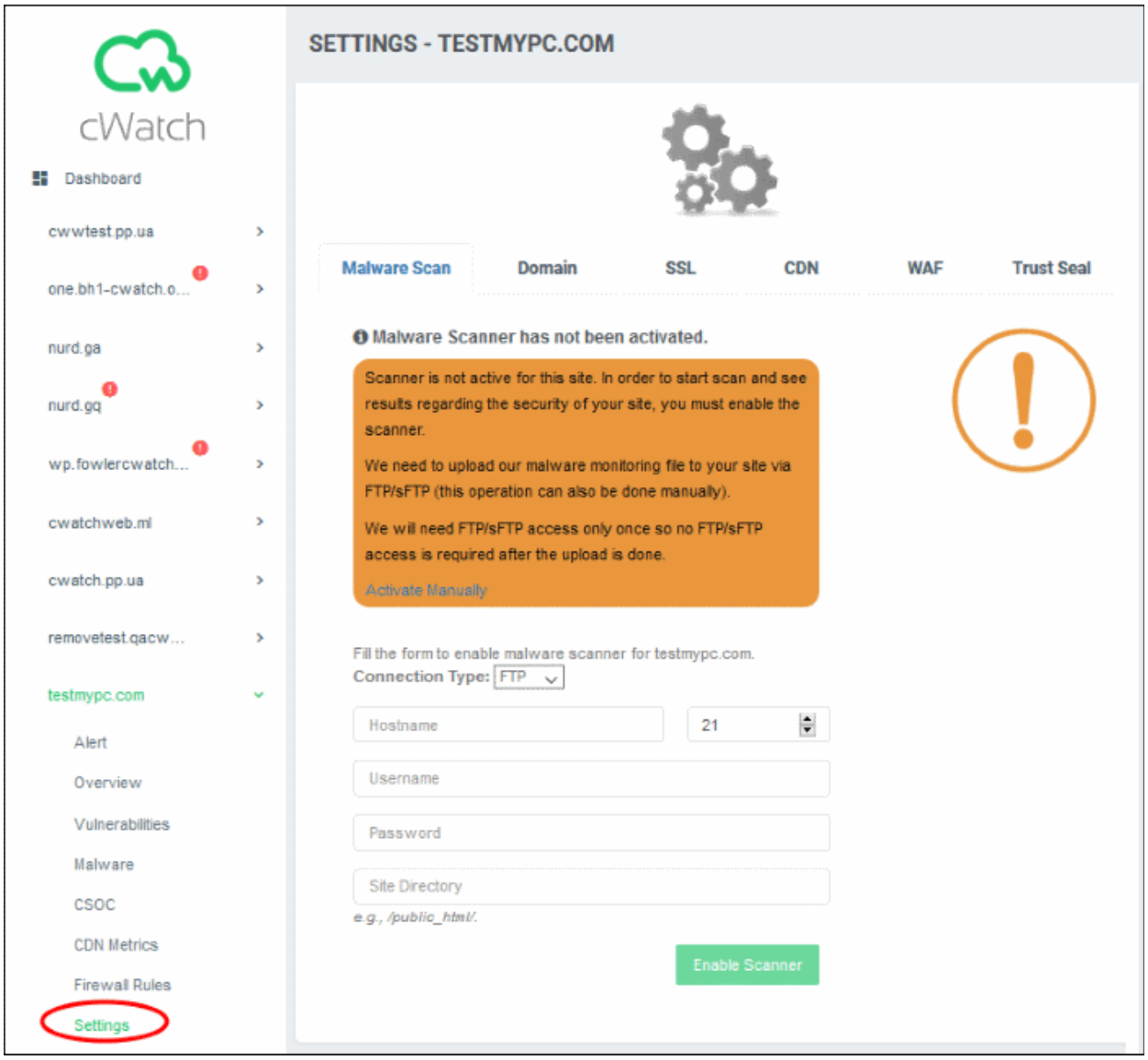
- Go to your website's DNS management page and enter the 'CNAME' and 'A' records
- See **https://support.google.com/a/topic/1615038?hl=en** if you need more help to add 'CNAME' and 'A' records
- DNS propagation may take around 30 minutes depending on your hosting provider
- Please note there will be no downtime on your site during these changes

The 'CNAME' and 'A' record statuses will change to 'Configured' once the update is complete:



Configure Malware Scans

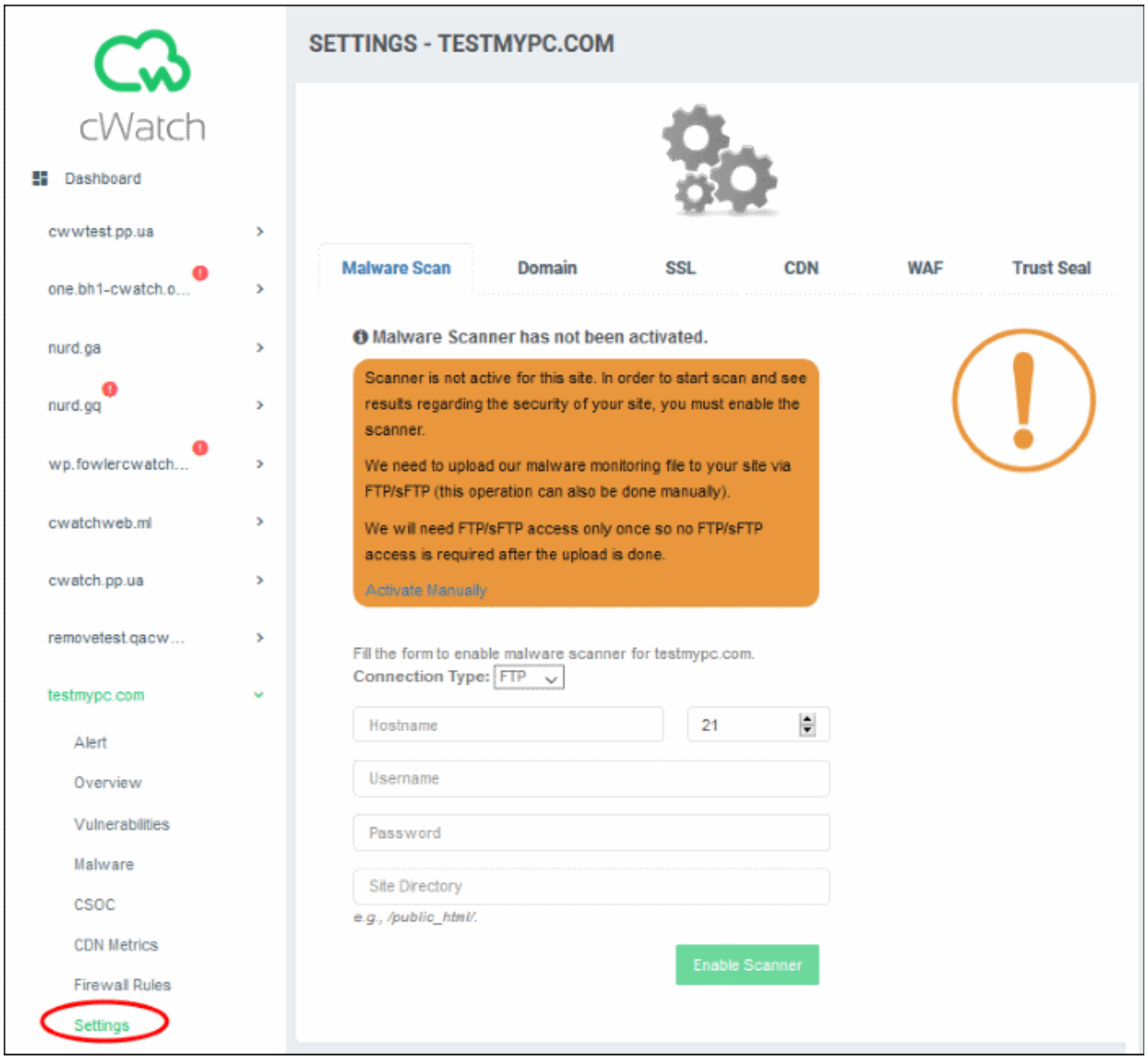
- Click the website name > 'Settings' > 'Malware Scan'
- You need to upload a file to your site to activate malware scans.
- You can have Dome upload the file for you by specifying your FTP or sFTP details. You can also manually upload the file yourself if you wish.



Configure Automatic Scan

You can automatically enable malware scans by configuring your FTP details in Dome:

- Click a website name on the left and choose 'Settings'
- Open the 'Malware Scan' tab
- Connection Type - select 'FTP' or 'sFTP'.
  - sFTP uses an encrypted connection.



s/FTP Settings – Table of Parameters	
Parameter	**Description**
Hostname	IP or hostname of your web-server
Username/ Password	Login credentials to your web-server.
Directory	Location to which Dome should upload the file. This must be publicly accessible.

- Click 'Enable Scanner' to upload the file.
- Note. These settings will also be used by our technicians to access your site IF you request them to remove malware.

Configure Manual Scan

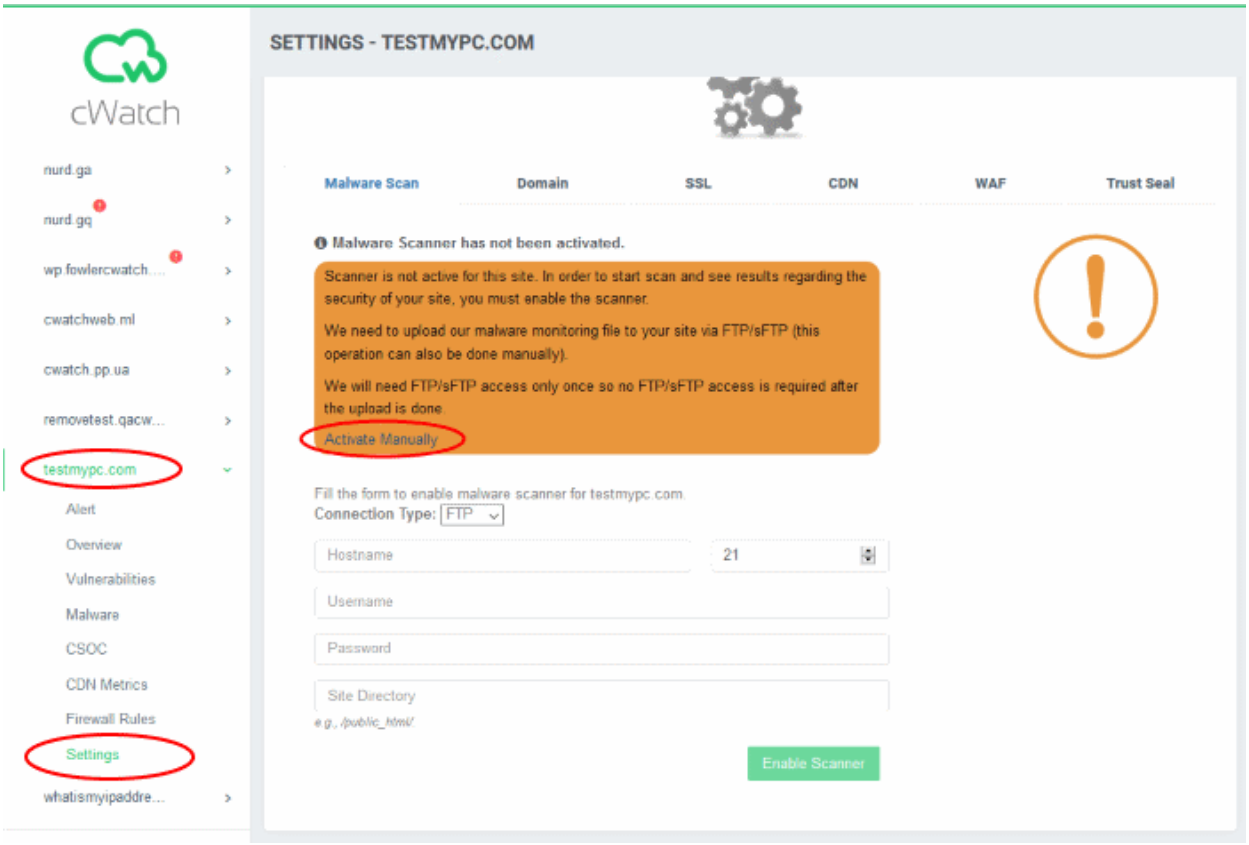
- You need to upload a .php file to your website to enable automatic malware scans.
- cWatch will verify the file at the location you specify and commence scanning.
- You have the option to automatically remove of malware at the end of every scan.

There are two ways to save the .php file on your site:

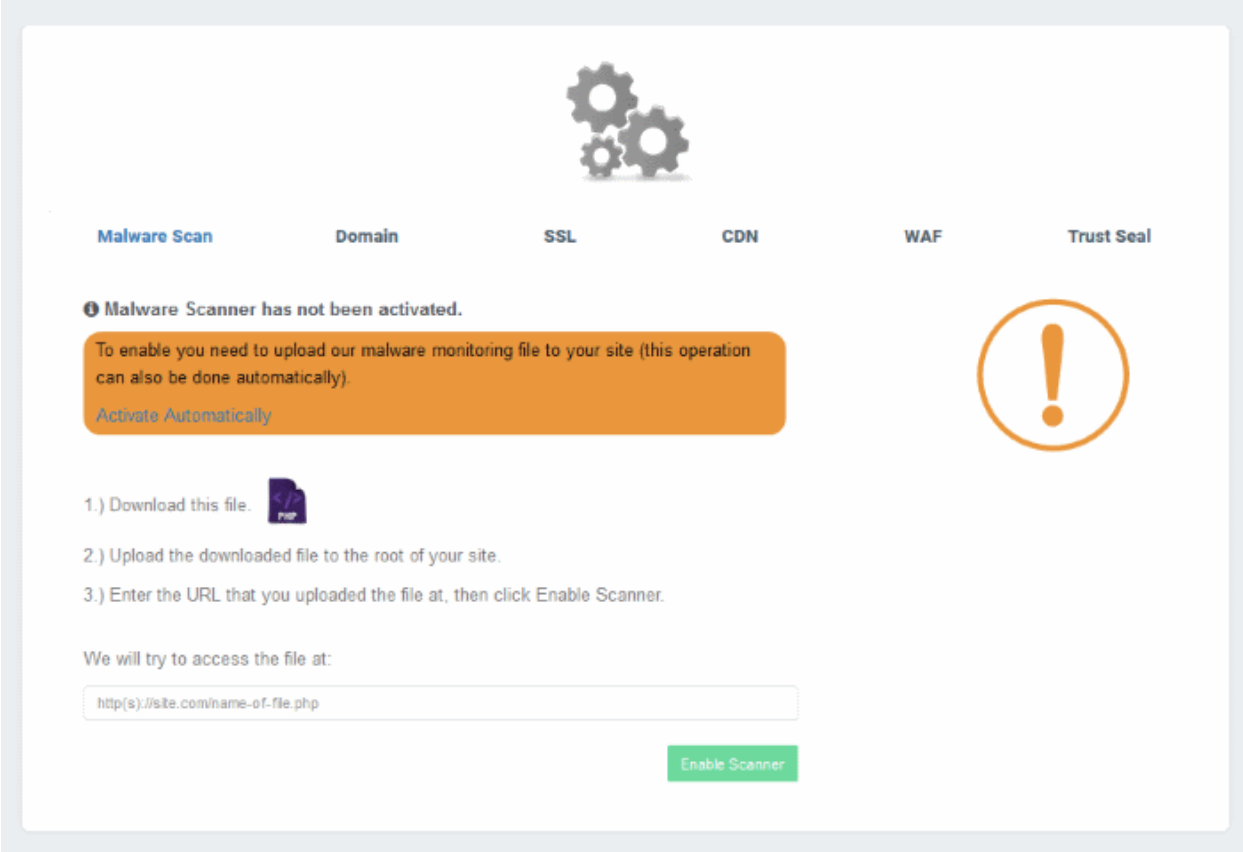
1. **Automatic** – Provide website access details and let Dome automatically upload the file via FTP.
   - Click the website name on the left and choose 'Malware'
   - Click 'Enable Scanner' and provide website details.
   - See '**Malware Scans**' if you need more help with this.
2. **Manual** - Download the .php file and save it on your website. The remainder of this section explains how to obtain the required file.

Manual Download

- Click the website name on the left and choose 'Settings'
- Open the 'Malware Scan' tab
- Click the 'Activate Manually' link:



- This opens the file download page:



- 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 'Enable Scanner' to run the check.
- Automatic scans on your site will be enabled if the file-check is successful.

Configure CDN Settings

- The Content Delivery Network (CDN) accelerates site performance and adds security to your websites.
- Make sure you have configured the DNS settings of your website to use the CDN. See '**Domain Configuration Instructions**' for more information.

Once configured, the CDN service will:

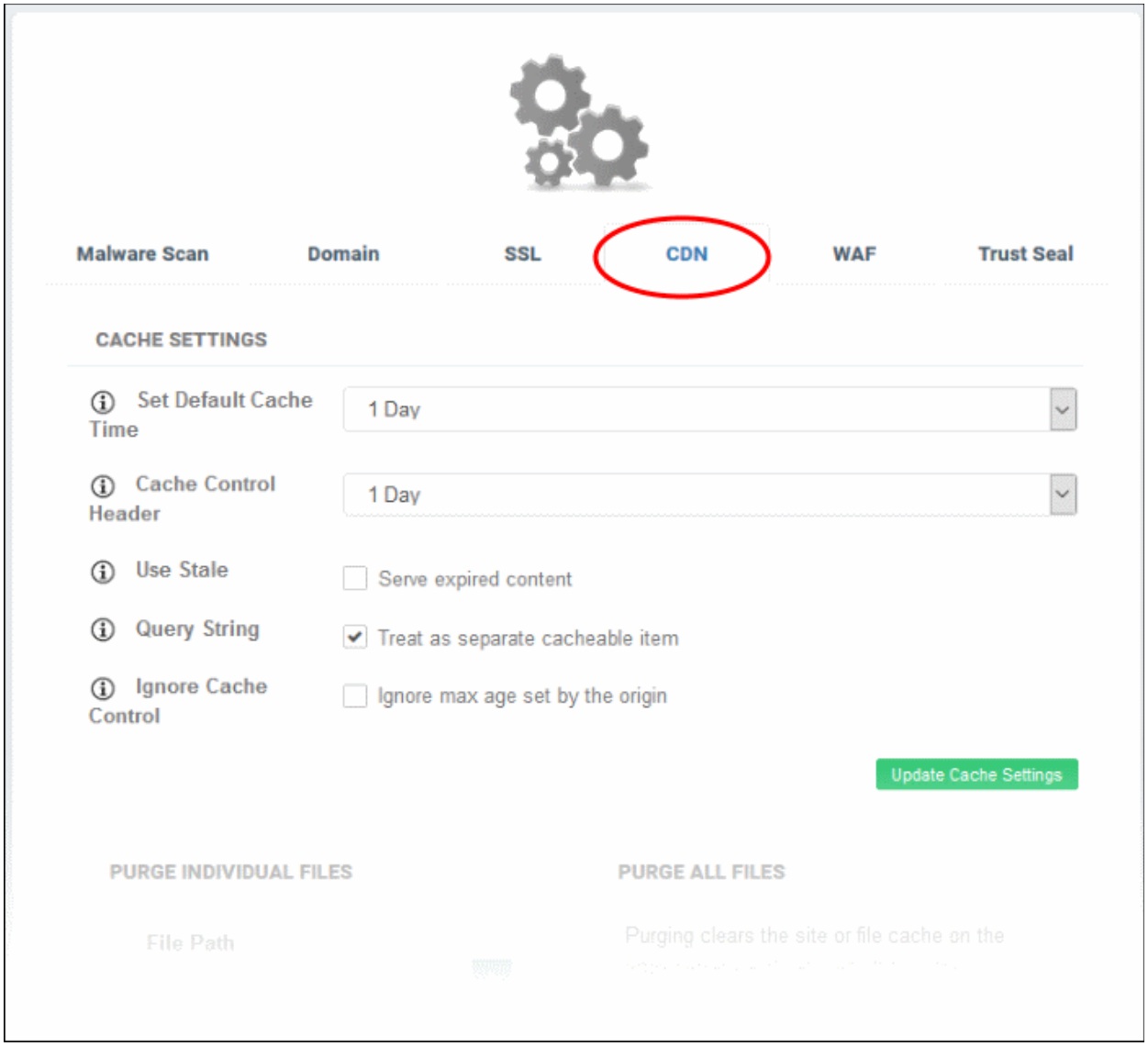
- Accelerate performance by delivering your website content to your visitors from data centers closest to their location.
- Forward event logs to the Comodo CSOC team who will monitor your traffic to identify anomalous behavior and threats.
- Provide Comodo web application firewall (CWAF) protection for your domains. The CSOC team constantly improves the Mod Security rules in the firewall to provide cutting edge protection for our customers.

To open the CDN Settings page

- Click the 'Settings' cog icon underneath your username
- Click 'Manage Settings' in the row of the site whose DNS settings you want to configure.
- Open the 'CDN' tab

OR

- Click on the website you wish to configure in the left-hand menu then choose 'Settings'
- Open the 'CDN' tab



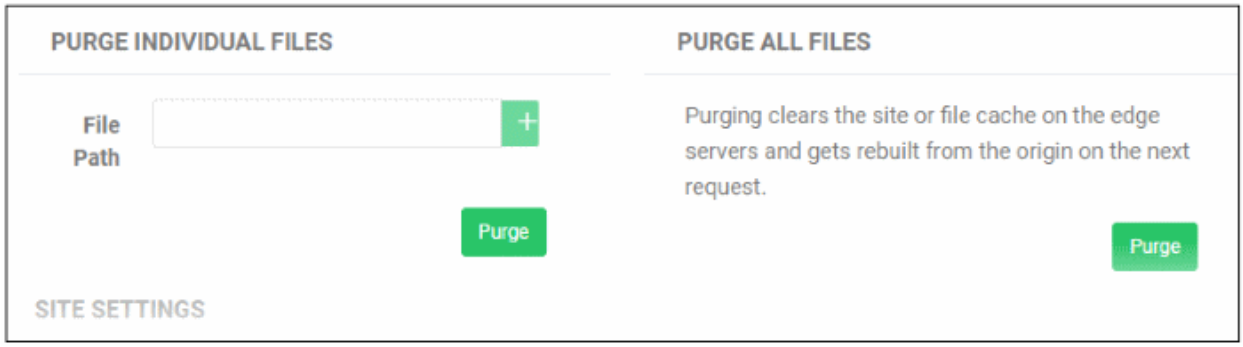
Cache Settings

Cache Settings - Table of Parameters	
Parameter	**Description**
Set Default Cache Time	Define how long content fetched from your web servers by the CDN should remain in the CDN cache. This is useful if your website's cache control headers (CCH) are not used or ignored by the browser on your visitors computer. **Background Note**: Cache Control Headers are used to specify how long content fetched from site should remain in the browser's cache. The local cache is used by the browser to render the site when it is re-visited by the user, avoiding the need to fetch the content again from the server.
Cache Control Header	The validity period of the CCH on the end-user's web browser. This defines how long cached content in the web browser can be reused without checking the web server for updates.

Use State	Select 'Serve expired content' if you want the CDN to deliver cached content when: • The CDN is currently checking the website for updated content • Your website is down.
Query String	Treat as separate cachable item' - web-pages with query string parameters (e.g. '?q=something') will be cached as separate files. This will instruct the CDN to update cached files whenever the original pages are updated.
Ignore Cache	'Ignore max age set by the origin' - Visitor's browsers will ignore the time to live (TTL) and header expiry settings of your web-pages. Web browsers will use the 'Set default cache time' setting for the cache time.

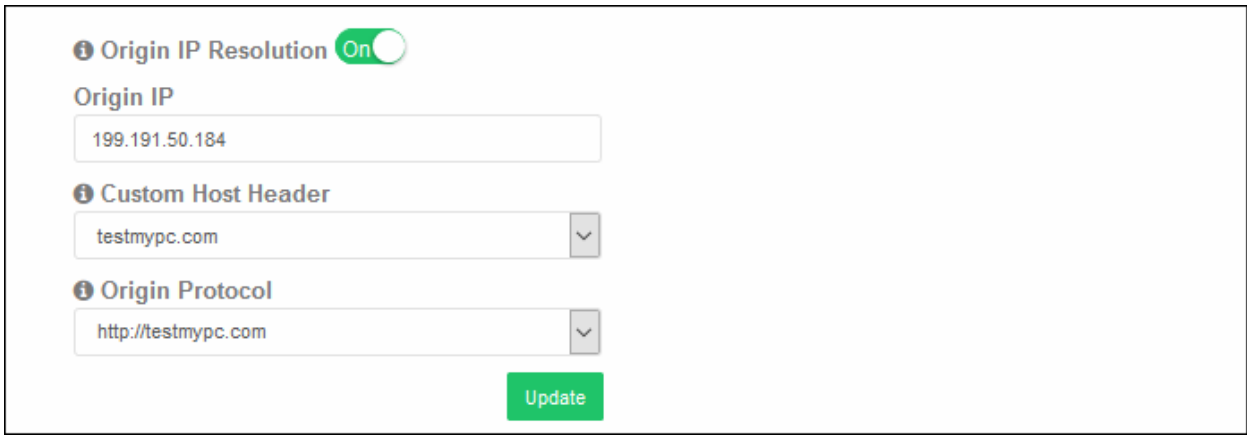
- Click 'Update Cache Settings' for your changes to take effect.

Purge Files



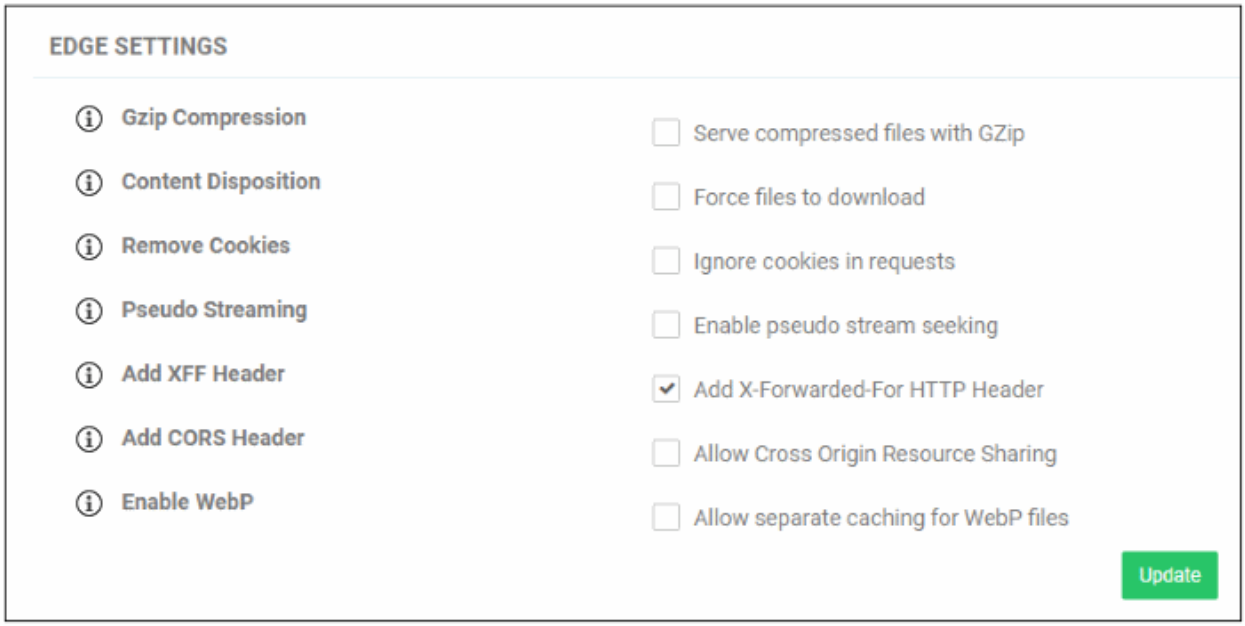
Purge CDN Cache on Edge Servers	
Purge Individual Files	Remove specific files from the cache so that the CDN is forced to check your website the next time the files are requested. • Enter the URI of the file in the text box and click the green '+' button • Repeat the process to add more files • Click 'Purge'
Purge All Files	Remove all files from the cache so that the CDN is forced to check your website the next time the files are requested. • Click 'Purge'

Site Settings



- **Origin IP Resolution** - Choose whether or not the CDN should use DNS servers to resolve the IP address of your web server. This depends on whether your server uses a static or dynamic IP address.
    - If your server uses a static IP address, enable 'Origin IP Resolution'. The CDN will fetch your IP address by domain look-up, save it and display it in the 'Origin IP' field. The CDN will use this IP address to fetch the files from your web server. This will save time for content delivery to your website visitors.
    - If your server uses dynamic IP address, disable this option. The CDN will use DNS services to resolve your IP address.
- **Custom Host Header** - If the host header for your site is different to the domain name, enter the custom host header in this field.
- **Origin Protocol** – Choose whether the CDN should use website with SSL certificate or not.
- Click 'Update' for your settings to take effect.

Edge Settings



Edge Settings - Table of Parameters	
Parameter	**Description**
Gzip Compression – Server compressed files	Reduces the size of files for faster network transfers. Optimizes bandwidth usage and increases transfer speeds to browsers.

with GZip	
Content Disposition – Force Files to download	Forces the files to download instead of showing the content in the browser
Remove Cookies – Ignore cookies in requests	CDN ignores header cookies
Pseudo Streaming – Enable pseudo stream seeking	Plays media files (FLV and MP4 files only with H. 264 encoding)
Add XFF Header – Add X-Forwarded for HTTP Header	Identifies the actual client source IP address.
Add CORS Header – Allow Cross Origin Resource Sharing	Adds 'Access-Control-Allow-Origin' header to responses
Enable WebP – Allow separate caching for WebP files	Currently being developed by Google, WebP is an image format that provides both lossy and lossless compression. If enabled, cWatch will have separate cache for these files.

- Click 'Update' for your settings to take effect.

Configure WAF Settings

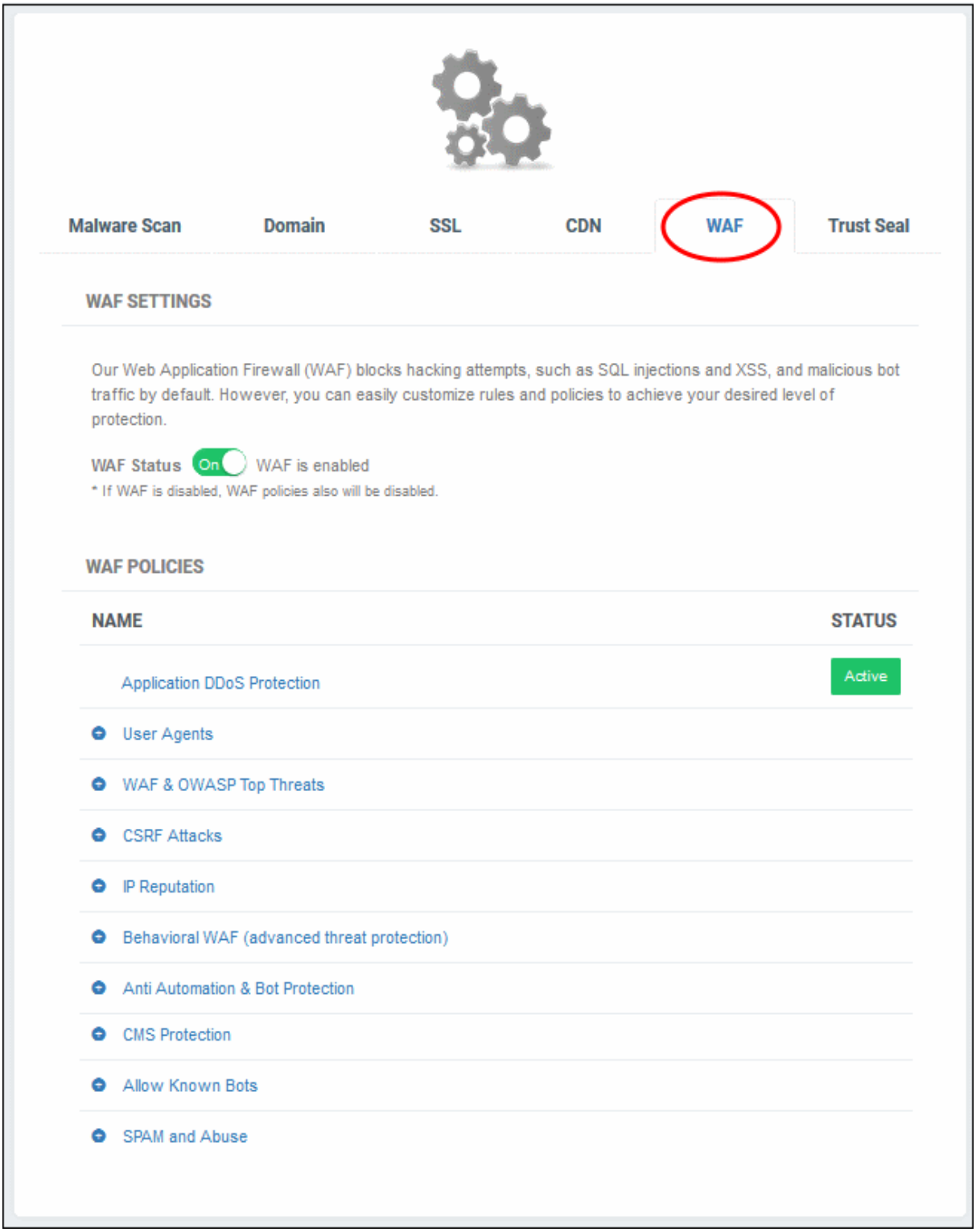
- Click the 'Settings' cog icon underneath your username
- Click 'Manage Settings' in the row of the site whose DNS settings you want to configure.
- Open the 'WAF' tab

OR

- Click on the website you wish to configure in the left–hand menu then choose 'Settings'
- Open the 'WAF' tab

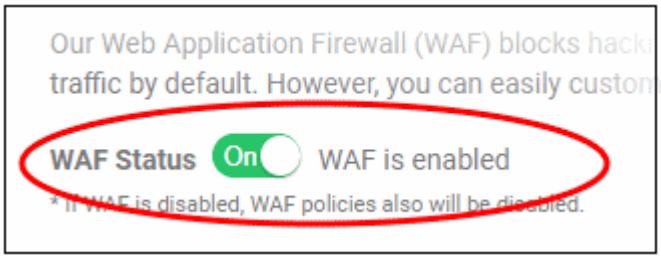
cWatch ships with built–in rules for the web application firewall (WAF) which provide the highest levels of protection for your website.

- Firewall tasks include preventing SQL injections, preventing bot traffic and more.
- There are several types of WAF policy, each with a set of constituent rules. You can enable or disable rules as required.



WAF Status

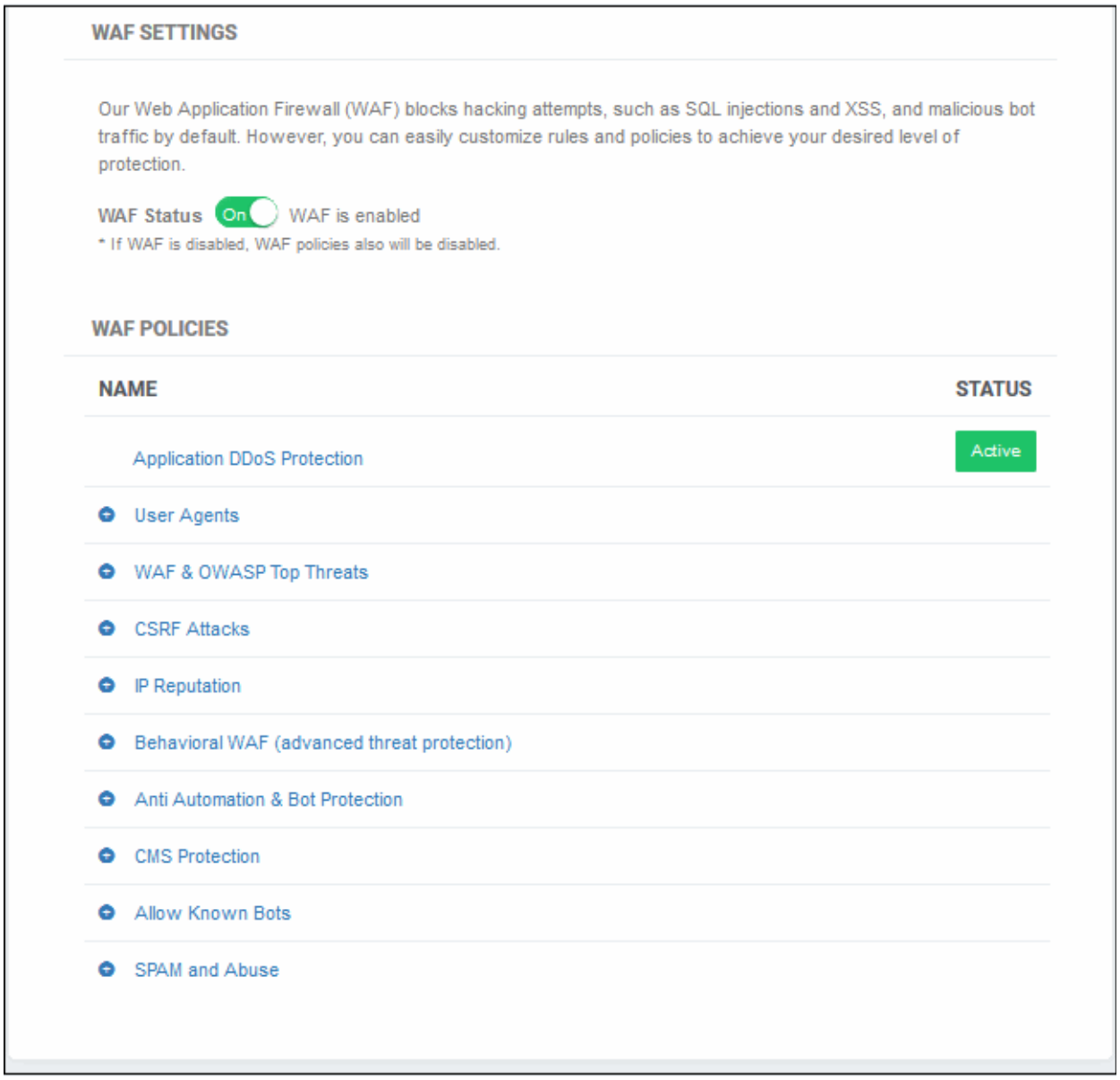
- Switch WAF protection on or off:



Note - if you disable WAF protection then no firewall policies are applied. Any custom firewall rules are also disabled.

WAF Polices

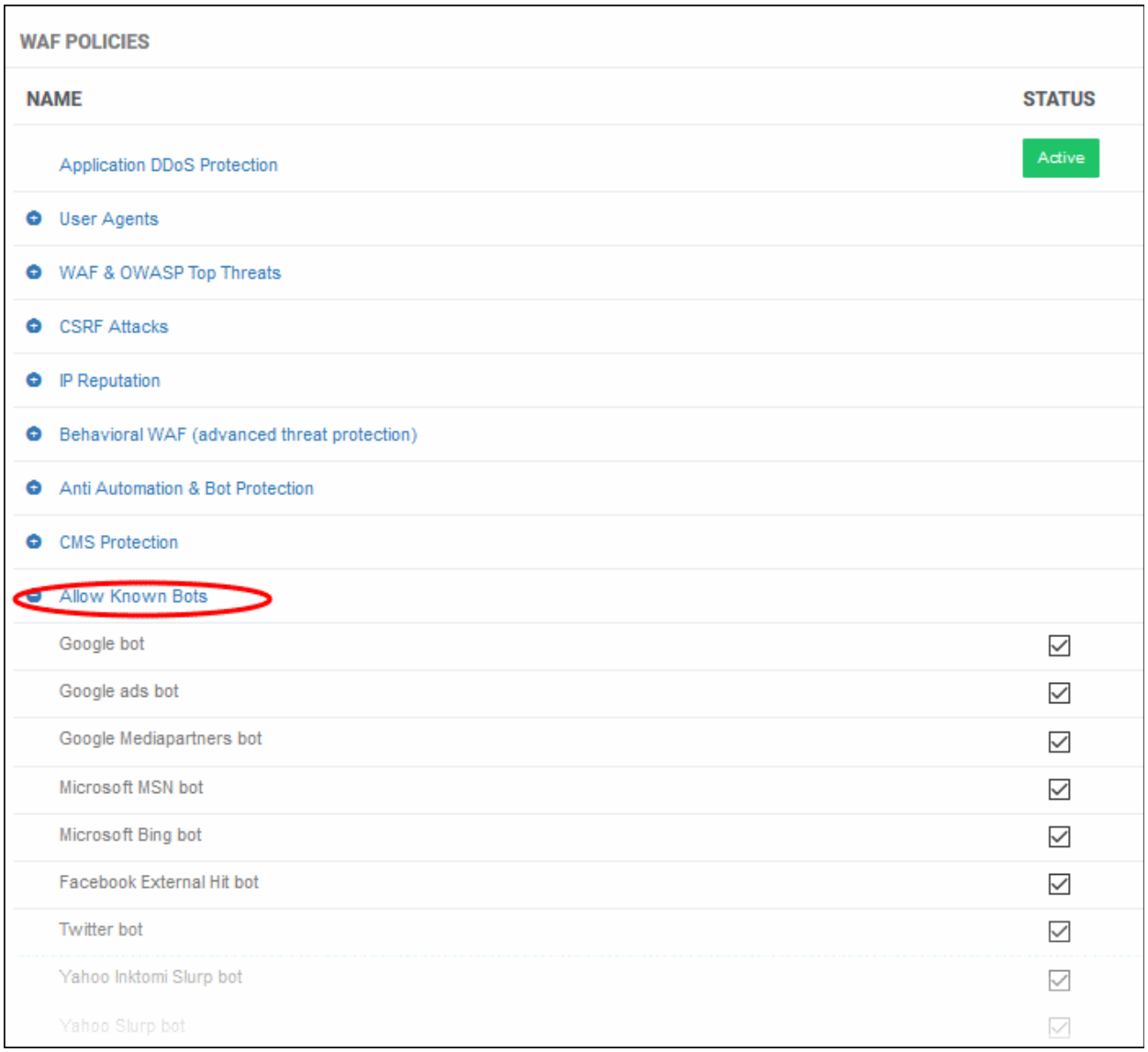
- This section lists all WAF policies and rules.
- Click the '+' symbol to view specific rules in a policy. You can enable / disable rules as required.



- **Name** – Label of the built-in WAF policy.
- **Status** – Whether or not the firewall is active. 'Passive' indicates the firewall is disabled.

To enable / disable firewall rule(s)

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



- Use the check-boxes to enable or disable particular rules.

Any changes will be deployed in approximately a minute.

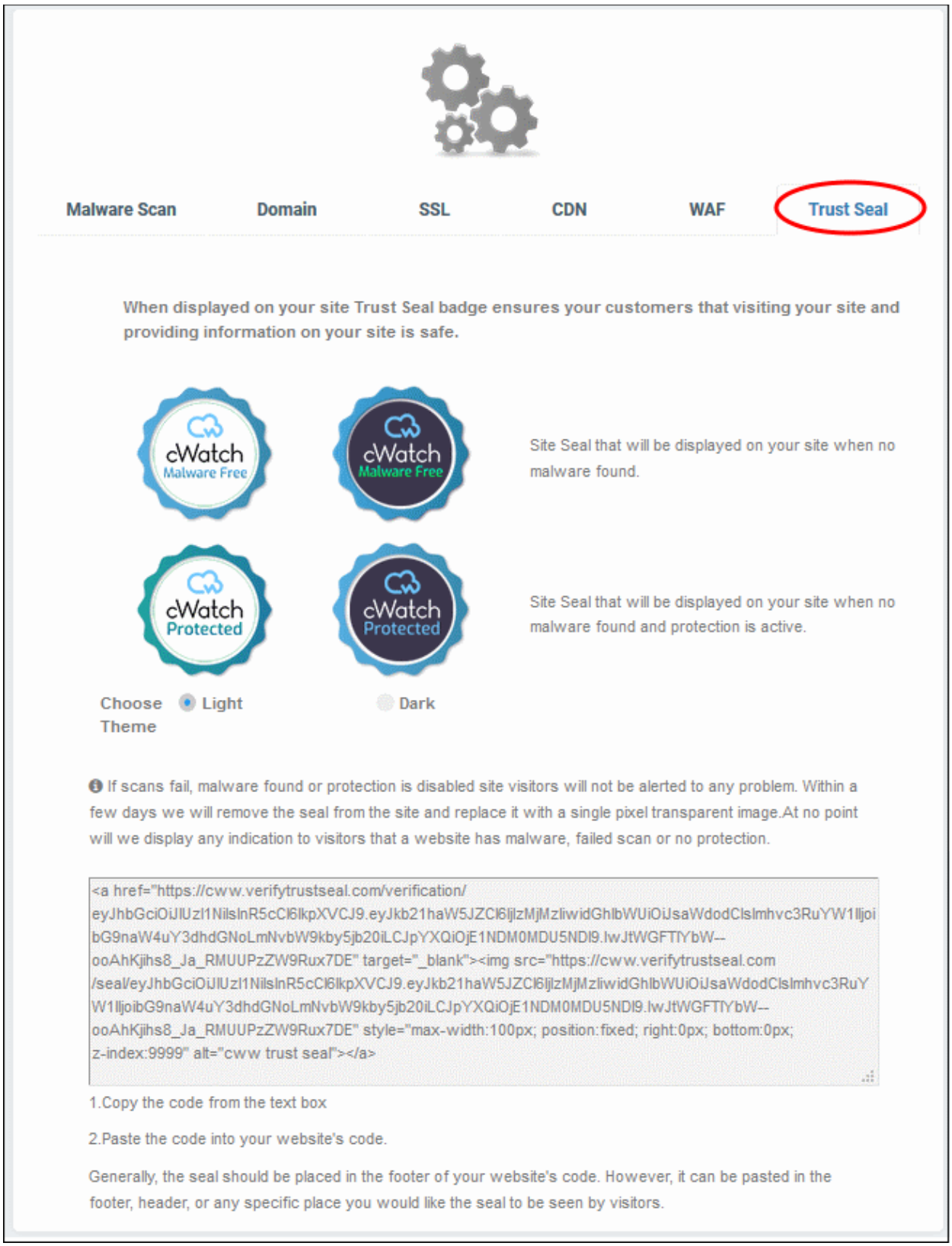
Configure Trust Seal

The trust seal proves to your visitors that your site is malware free and enjoys 24/7 protection by one of the leaders in online security. This helps build the trust you so often need to convert visitors into paying customers.

- Click the 'Settings' cog icon underneath your username
- Click 'Manage Settings' in the row of the site you want to configure
- Open the 'Trust Seal' tab

OR

- Click on the website you wish to configure in the left–hand menu then choose 'Settings'
- Open the 'Trust Seal' tab



- There are two types of seal – 'Malware Free' and 'Protected'. The type shown on your site depends on the following conditions:
  - '**Malware Free**' – Displayed if your site is not blacklisted and has no malware.
  - '**Protected**' – Displayed if your site is not blacklisted, has no malware and both CDN and Web Application Firewall (WAF) are active.

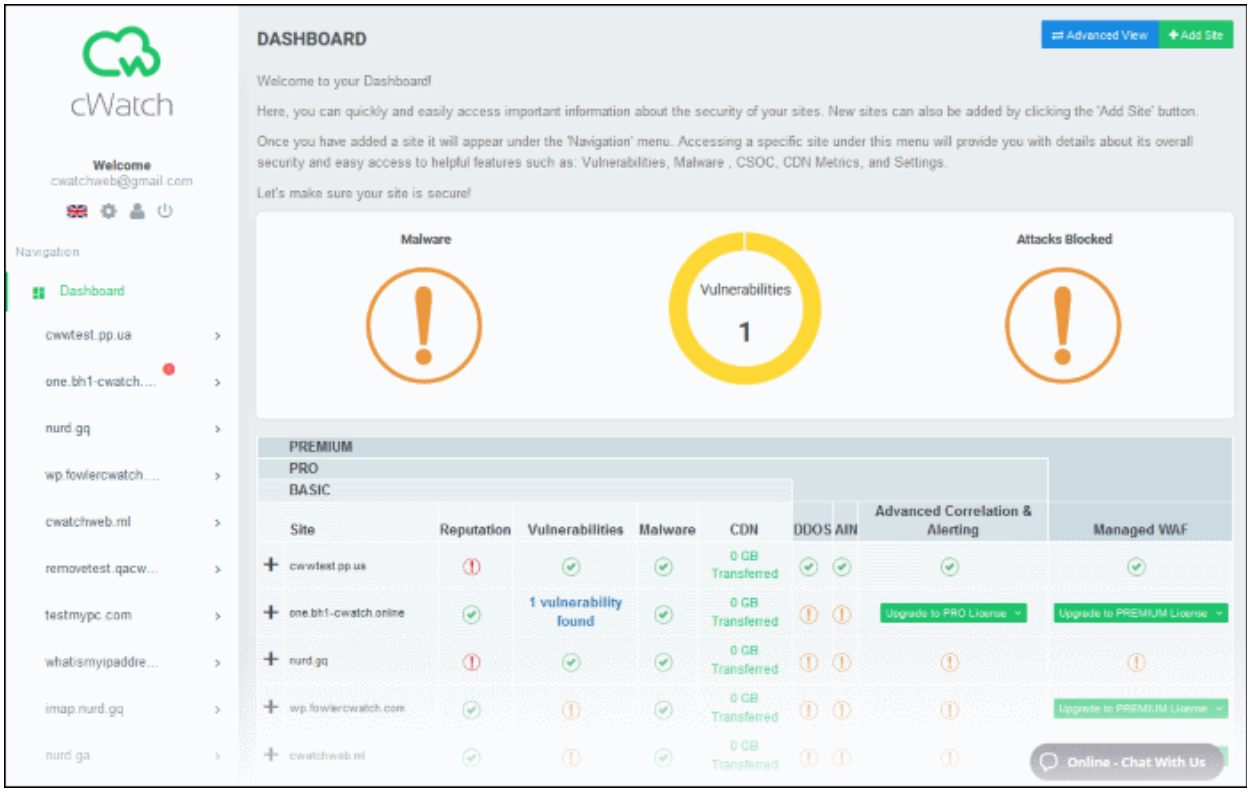
Here are some sample scenarios:

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 or 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.
- Follow the instructions in the settings page to add the seal code to your web pages.

Use the cWatch Interface

The menu on the left shows all sites you have added to cWatch. You can view threat statistics and configure the website by selecting the required option below the domain name. You can also change your profile information.



Left Menu

- **Dashboard** - Overall statistics on all websites that are protected and managed. See **https://help.comodo.com/topic-285-1-848-11006-The-Dashboard.html**

Domain Components

- Click on any domain name to open the following menu items:

- **Alert** - Shows all notifications about malware and vulnerabilities discovered on the website. See **https://help.comodo.com/topic-285-1-848-11493-View-Alerts.html** for more details.
- **Overview** - At-a-glance summary of security status and CDN performance. See **https://help.comodo.com/topic-285-1-848-11010-Website-Overview.html** for more details.
- **Vulnerabilities:**
  - Scan your site for OWASP top–ten threats. You can also enable or disable automatic weekly scans.
  - Run a WordPress scan to identify vulnerabilities in your WordPress site, plugins, themes and more.
  - You can run on–demand vulnerability/WordPress scans on the site at anytime. See **https://help.comodo.com/topic-285-1-848-11492-Comodo-Vulnerability-Scan-Results.html** for more details.
- **Malware Scans** - Run virus scans, view scan results and monitor malware cleanup progress. You need to upload our .php file to your server to enable malware scans. See **https://help.comodo.com/topic-285-1-848-11011-Malware-Scans.html** for more details.
- **COSC Results** - Shows a real-time analysis of attack patterns on your domain from the Comodo Security Operations Center. See **https://help.comodo.com/topic-285-1-848-11494-Cyber-Security-Operation-Center-Results.html** for more details.
- **CDN Metrics** - Shows data about your content delivery network traffic. This includes total usage, data throughput and the locations from which your traffic originated. See **https://help.comodo.com/topic-285-1-848-11495-Content-Delivery-Network-Metrics.html** to find out more.
- **Firewall Rules** – Define your own custom Web Application Firewall (WAF) rules according to your requirements. See **https://help.comodo.com/topic-285-1-848-12468-Configure-Firewall-Rules.html** for more information.
- **Settings** - Allows you to configure domain malware scanning, CDN coverage, FTP access and SSL certification. See **https://help.comodo.com/topic-285-1-848-11496-Website-Configuration.html** to find out more.

Main Settings – You can view and manage your domain settings and DNS. See **https://help.comodo.com/topic-285-1-848-11013-The-Settings-Interface.html** for more details.

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**