

COMODO
Creating Trust Online®



Comodo cWatch Web Security

Software Version 4.8

Quick Start Guide

Guide Version 4.8.013119

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**
- **Login to cWatch**
- **Add Websites**
- **Configure your websites**
 - **SSL Configuration**
 - **Domain Configuration Instructions**
 - **Configure Malware Scan**
 - **Configure Automatic Scan**
 - **Configure Manual Scans**
 - **Configure CDN Settings**
 - **Configure WAF Settings**
 - **Configure Trust Seal Settings**
- **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			
Malware removal by experts Hack repair and restore Vulnerability repair and restore Traffic hijack recovery SEO/Search poisoning recovery	Unlimited	Unlimited	One time

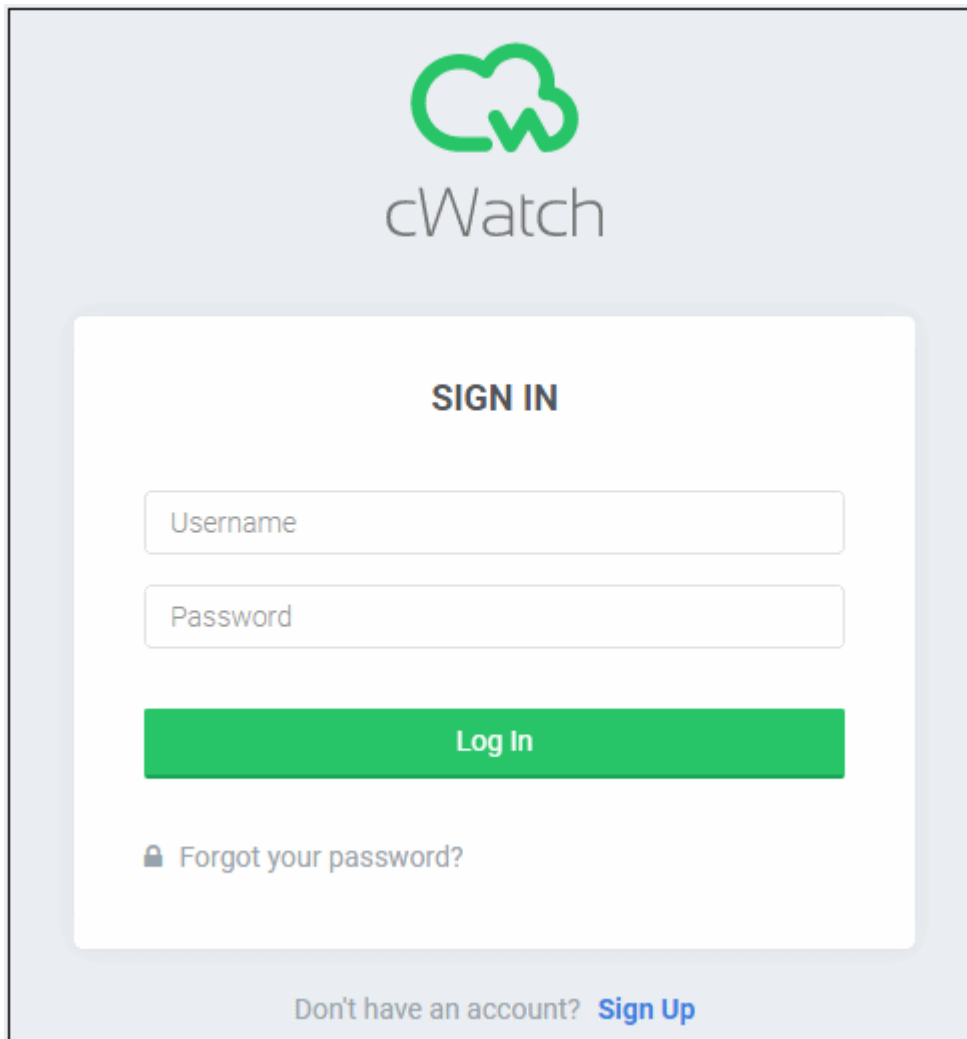
Automatic Malware Removal	✓	✓	✗
Spam & Website Filtering	✓	✓	✗
Malware Scan	Every 6 hours	Every 12 hours	Every 24 hours
Vulnerability (OWASP) Detection	Every 6 hours	Every 12 hours	Every 24 hours
Security Information and Event Management (SIEM)	✓	✓	✗
24/7 Cyber-Security Operations Center (CSOC)	✓	✓	✗
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 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:



SIGN IN

Username

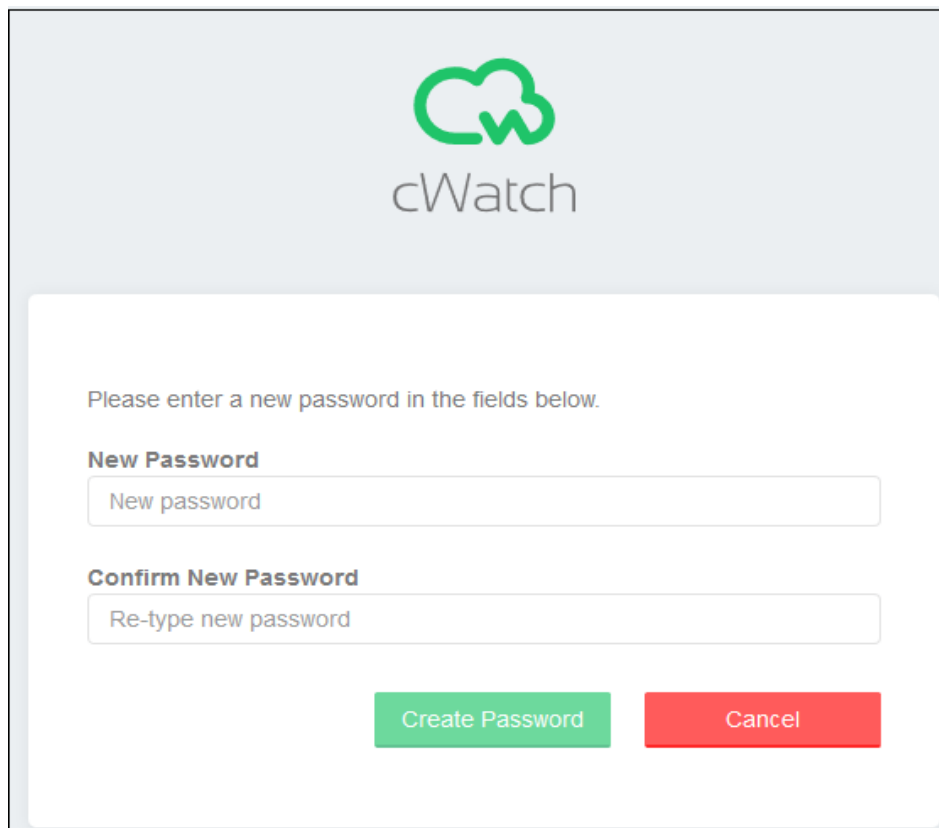
Password

Log In

🔒 [Forgot your password?](#)

Don't have an account? [Sign Up](#)

- 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':

The screenshot shows the cWatch logo at the top center. Below it, a white box contains the text "Please enter a new password in the fields below." followed by two input fields. The first field is labeled "New Password" and contains the placeholder text "New password". The second field is labeled "Confirm New Password" and contains the placeholder text "Re-type new password". At the bottom of the white box, there are two buttons: a green "Create Password" button and a red "Cancel" button.

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

Add Websites

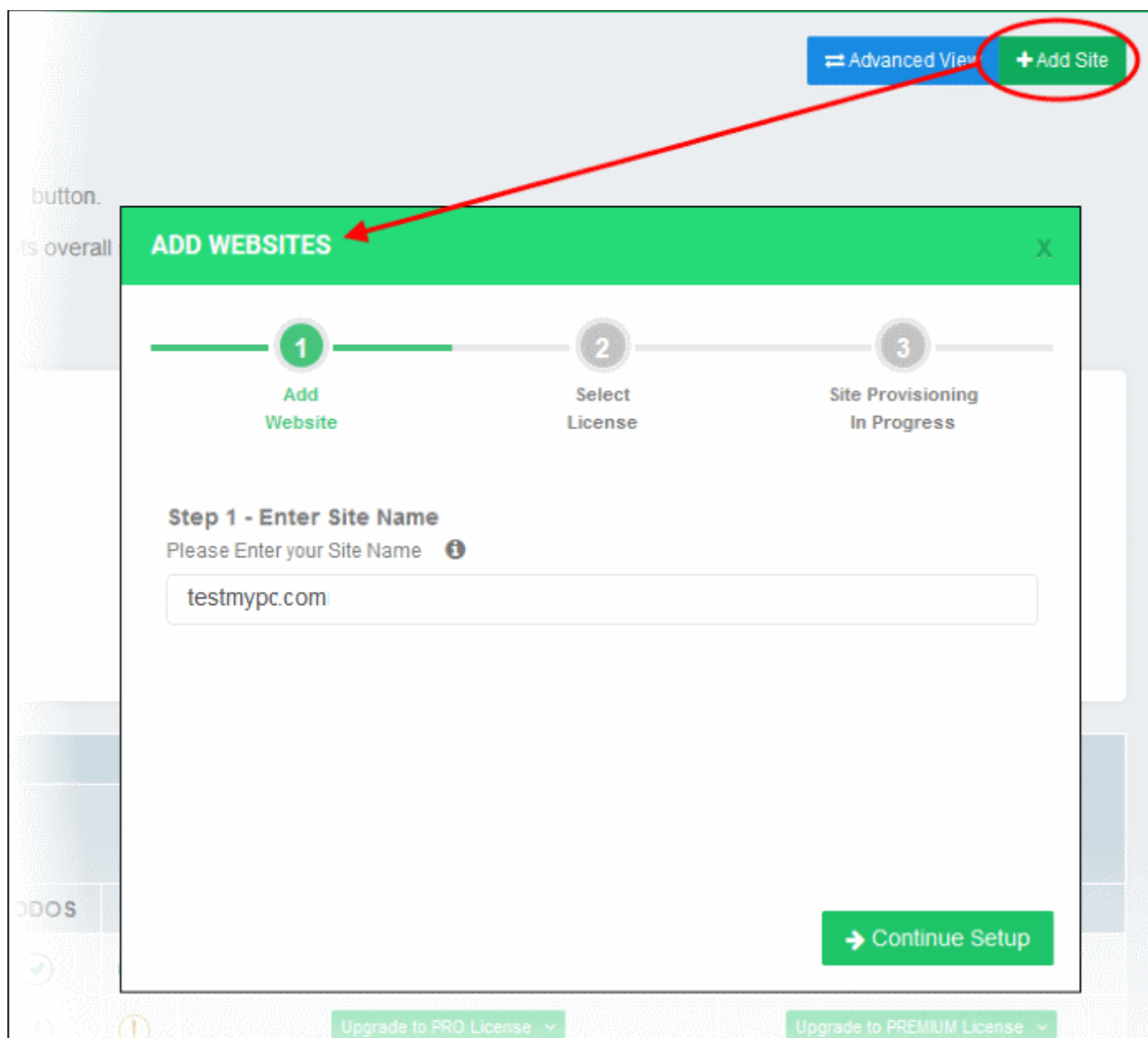
- You need to add websites to cWatch to enable protection and take advantage of the content delivery network (CDN).
- The number of domains you can add depends on number of licenses you purchased. Each license covers one domain.
- Once added, you can configure threat monitoring and CDN settings for each 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

ADD WEBSITES X

1 Add Website

2 Select License

3 Site Provisioning In Progress

Step 2 - Select License

Site will be added with selected license type

Basic (1 Site / Indefinite Usage) ▼

[Learn more](#)

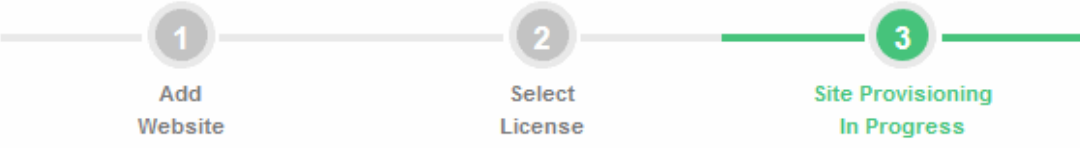
← Back → Finish

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>.

ADD WEBSITES X



1
Add Website

2
Select License

3
Site Provisioning In Progress

Step 3 - Site Provisioning In Progress

Congratulations your site provisioning is in progress now!

This process may take several minutes


On left menu you will see the status of your site's provisioning, by clicking on refresh button you can get the latest status.











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

[★ Get Started](#)

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

SETTINGS



SITE	LICENSE	SETTINGS	
cwvtest.pp.ua	Premium	Manage Settings Manage DNS	
one.bh1-cwatch.online	Basic	Manage Settings Manage DNS	
nurd.ga	Premium Trial	Manage Settings Manage DNS	
nurd.gq	Premium Trial	Manage Settings Manage DNS	
wp.fowlercwatch.com	Pro Trial	Manage Settings Manage DNS	
cwatchweb.ml	Pro Trial	Manage Settings Manage DNS	
cwatch.pp.ua	Premium Trial	Manage Settings Manage DNS	
removelest.qacww.cf	Pro Trial	Manage Settings Manage DNS	
testmypc.com	Pro Trial	 Provisioning Completed. Click here to get started with domain settings.	

- 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.

SETTINGS - TESTMYPC.COM

Malware Scan | Domain | SSL | CDN | WAF | Trust Seal

Malware Scanner has not been activated.

Scanner is not active for this site. In order to start scan and see results regarding the security of your site, you must enable the scanner.

We need to upload our malware monitoring file to your site via FTP/sFTP (this operation can also be done manually).

We will need FTP/sFTP access only once so no FTP/sFTP access is required after the upload is done.

[Activate Manually](#)

Fill the form to enable malware scanner for testmypc.com.

Connection Type:

Hostname:

Username:

Password:

Site Directory:

e.g., /public_html/.

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:

- 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.
- Upload or create an SSL certificate so https sessions can be protected. See [SSL Configuration](#) 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.

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).

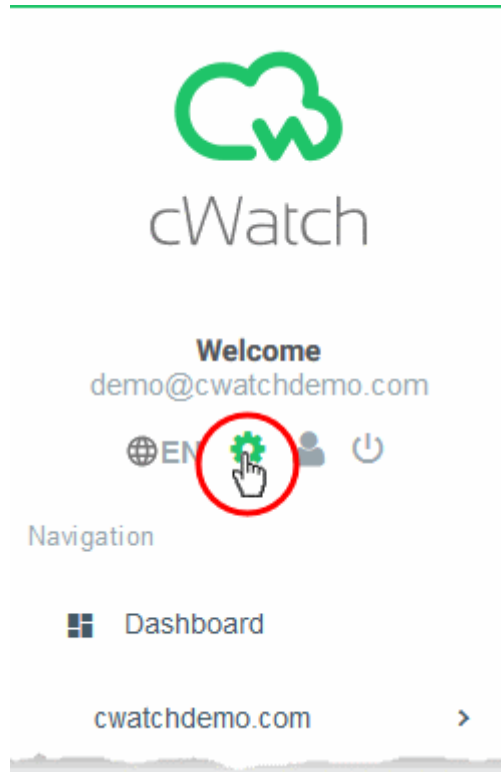
There are two ways this can be done:

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

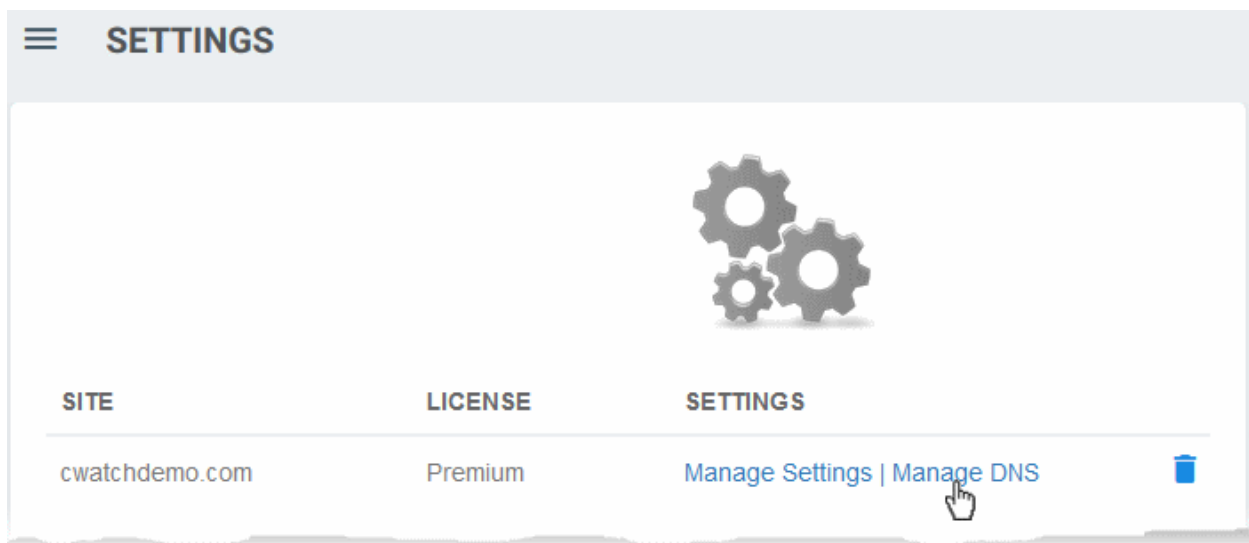
Option A – Change your domain's authoritative DNS servers to Comodo

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.

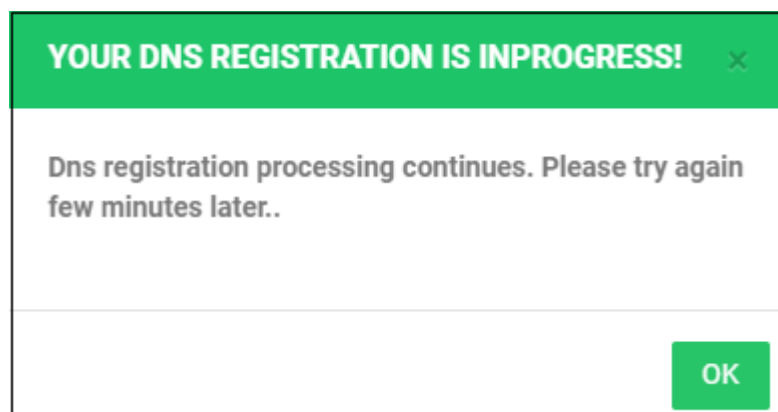
- Click the settings cog icon under your username



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



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



- Once complete, open the settings page again and click 'Manage DNS' in the row of the target website
- Nameserver details are shown as follows:

SETTINGS - DNS - *.YUMURTA.COM

DNS

Manage your Domain Name Server(DNS) settings.

To use cWatch Cyber Secure Content Delivery(CDN) Network and Web Application Firewall, you need to change your domain's authoritative DNS servers, which are also referred to as nameservers. For your reference, here are the Comodo's 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.

Not sure how to change nameservers? Try:
<https://support.google.com/domains/answer/3290309?hl=en>
 Still need a help? Please contact with our support professionals on 'Live Chat'

DNS Records
 A, AAAA, and CNAME records can have their traffic routed through the Comodo Cyber Secure CDN system. Add more records using the form below, and click the activate button next to the record to update traffic. [View Comodo Cyber Secure 1033](#)

TYPE	VALUE	STATUS
NS	ns1.dnsbycomodo.net	! Name servers are not set
NS	ns2.dnsbycomodo.net	

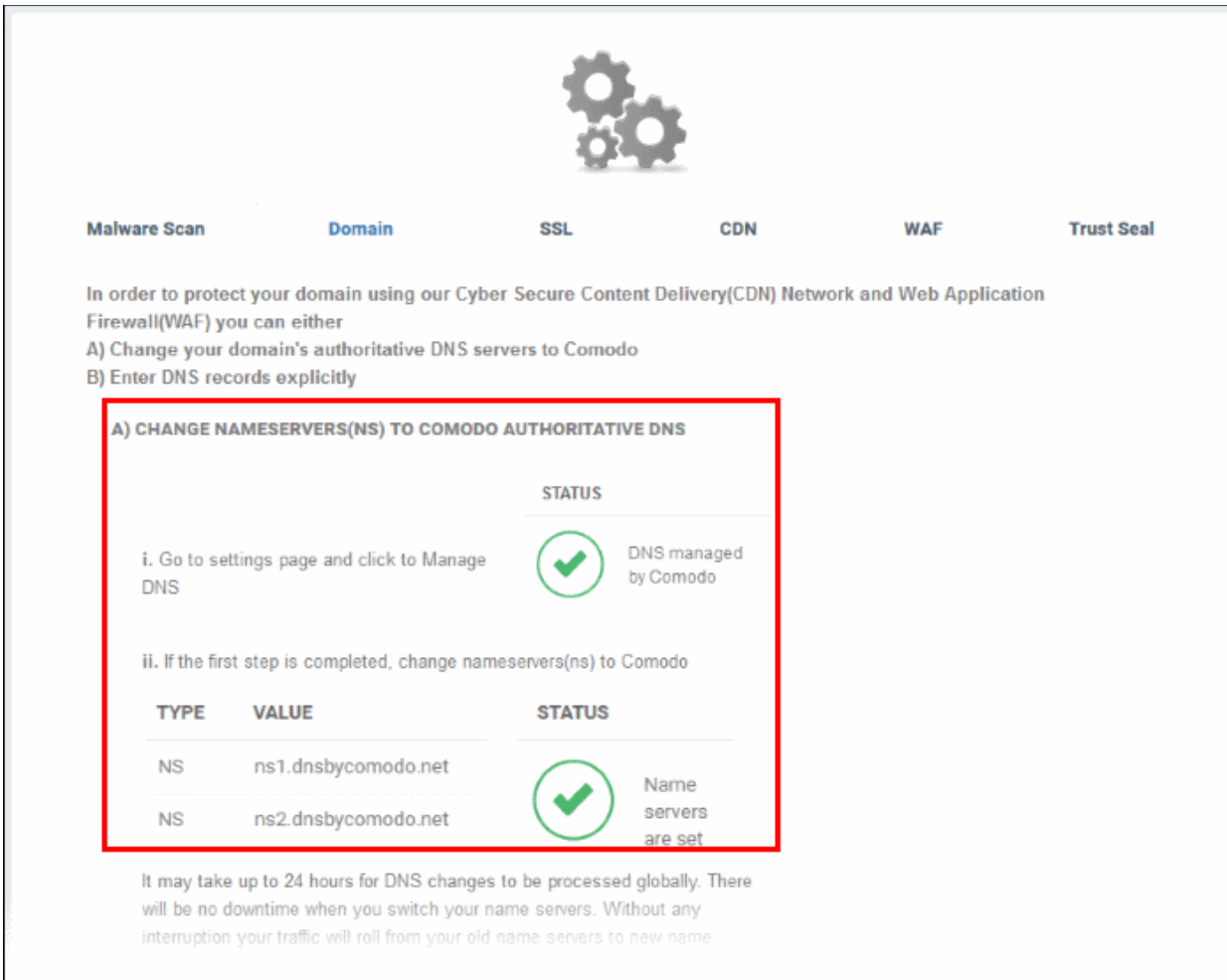
- Go to your website's DNS management page and enter the new nameservers
- See <https://support.google.com/domains/answer/3290309?hl=en> if you need more help changing nameservers
- Open the settings page and click 'Manage DNS' to view the nameserver update status:

your domain's nameservers you've

TYPE	VALUE	STATUS
NS	ns1.dnsbycomodo.net	✔ DNS managed by Comodo
NS	ns2.dnsbycomodo.net	

in your name at this switch your

- 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




The screenshot shows the 'Domain' tab in the Comodo cWatch interface. At the top, there are navigation tabs: Malware Scan, Domain (selected), SSL, CDN, WAF, and Trust Seal. Below the tabs, there is a heading: "In order to protect your domain using our Cyber Secure Content Delivery(CDN) Network and Web Application Firewall(WAF) you can either". Below this heading are two options: "A) Change your domain's authoritative DNS servers to Comodo" and "B) Enter DNS records explicitly".


Option A is highlighted with a red box and contains the following content:

A) CHANGE NAMESERVERS(NS) TO COMODO AUTHORITATIVE DNS

STATUS

i. Go to settings page and click to Manage DNS  DNS managed by Comodo

ii. If the first step is completed, change nameservers(ns) to Comodo

TYPE	VALUE	STATUS
NS	ns1.dnsbycomodo.net	 Name servers are set
NS	ns2.dnsbycomodo.net	

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

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.

In order to enter DNS records explicitly, you should first note the 'CNAME' and 'A' records from the cWatch interface. After adding a website, these details are auto-generated and available in the 'Settings' > 'Domain' tab.

- Click the settings icon above the navigation menu to open the main settings page and click 'Manage Settings' in the website row that you want to configure the DNS settings
- OR
- Click the website name in the left menu then 'Settings'
 - Select the 'Domain' tab and 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



- Note down the 'CNAME' and 'A' records
- Go to your website's DNS management page and enter the 'CNAME' and 'A' records
- If you need more help regarding adding 'CNAME' and 'A' records, visit <https://support.google.com/a/topic/1615038?hl=en>
- DNS propagation may take around 30 minutes depending on your hosting.
- Please note there will be no downtime on your site during these changes


Once the records have been updated successfully, you can view the status in the cWatch interface.

- Click the settings icon above the navigation menu to open the main settings page and click 'Manage Settings' in the website row that you want to configure the DNS settings
- OR
- Click the website name in the left menu then 'Settings'
 - Select the 'Domain' tab and scroll down to option 'B - Enter DNS Records Explicitly'

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

B) ENTER DNS RECORDS EXPLICITLY

TYPE	NAME	VALUE	STATUS
CNAME	subone	subonemycwatchcom1326-givkjgav4ntofwivqlm.stagingsecurecdn.com	✔ Configured.



- You can view the confirmation under the 'Status' column.

SSL Configuration

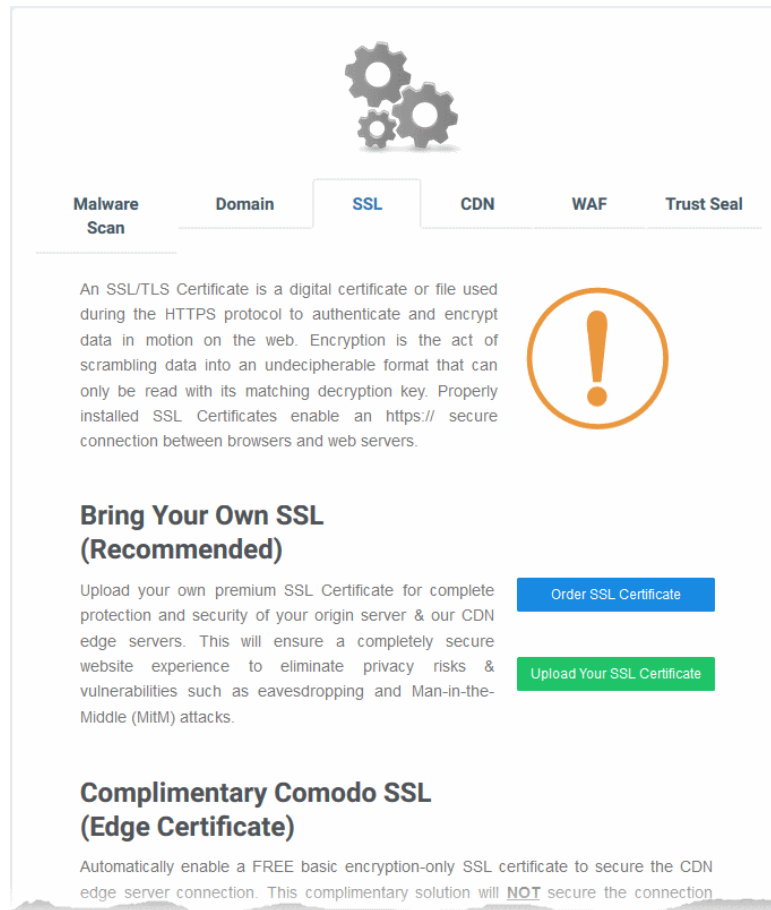
- An SSL/TLS certificate is placed on a website to identify the domain owner and encrypt all data that passes between the site and a visitor's browser.
- Sites that use a SSL/TLS certificate have a URL that begins with HTTPS. For example, <https://www.example.com>
- Comodo strongly recommends you use a certificate on your site.

There are two ways to deploy a certificate with cWatch Web:

- Bring your own SSL**
 - Upload the certificate used on your website to the cWatch CDN edge servers. Recommended for most customers.
 - This will secure 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
- Complimentary Comodo SSL**
 - Get a free SSL from Comodo deployed on CDN Edge servers
 - In order to obtain your free SSL certificate, you should have configured your website to use Comodo DNS. This can be done in two ways:
 - Change your domain's authoritative DNS servers to Comodo DNS
 - Enter DNS records explicitly
 - Guidance on DNS configuration is available in the previous section [Domain Configuration Instructions](#).
 - See [Install Complementary SSL Certificate](#) to find out how to deploy your free certificate

Upload your own SSL Certificate

- Click the cog icon above the navigation menu to open settings.
- Click 'Manage Settings' in the row of the website that you want to configure
- OR
- Click the website name on the left menu, then 'Settings'
- Select the 'SSL' tab in the 'Settings' page:



The screenshot shows the 'SSL' tab selected in a navigation menu. The main content area features a paragraph explaining SSL/TLS certificates, a warning icon, and two sections: 'Bring Your Own SSL (Recommended)' with 'Order SSL Certificate' and 'Upload Your SSL Certificate' buttons, and 'Complimentary Comodo SSL (Edge Certificate)' with a note that it is not secure.

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 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

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

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.

Order SSL Certificate

Upload Your SSL Certificate

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 SSL Certificate

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-----

	<pre> MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGEw JDTjEL MAkGA1UECBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1 UECxMC VU4xFDASBgNVBAMTC0hlcm9uZyZyZW5nMB4XDTA1MDcxNTIxMTk0N1oXDT A1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAGTA1BOMQswCQYDVQ QHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTA1VOMRQwEgYDVQQDEwtlZXJvbm cgWwFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBew KE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbMOoRcKK9vEcgmTcLFuQTWDl3Rag MBAAGj gbEwga4wHQYDVR0OBYYEFFXI70krXeQDxZgbaCQoR4jUDncEMH8GA1UdIw R4MHaA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMQswCQYDVQQGEwJDTjELMA kGA1UE CBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECxMCVU 4xFDAS BgNVBAMTC0hlcm9uZyZyZW5nggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvc NAQEE BQADQQA/ugzBrjjK9jcWnDVfGHlk3icNRq0oV7Ri32z/ +HX67aRfgZu7KWdI+Ju Wm7DCfrPNGVvFWUQOmsPue9rZBgO -----END CERTIFICATE----- </pre>
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.

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.

[Order SSL Certificate](#)

Domain	www.cwatchdemo.com
Expiration date	May 18, 2020 (479 days left)
Wildcard	No

[Uninstall](#)

Complimentary Comodo SSL

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 Complementary SSL Certificate

- Click the cog icon above the navigation menu to open settings.
 - Click 'Manage Settings' in the row of the website that you want to configure
- OR
- Click the website name on the left menu, then 'Settings'
 - Select the 'SSL' tab in the 'Settings' page:
 - Scroll down to 'Complimentary Comodo SSL (Edge Certificate)':

**Malware
Scan****Domain****SSL****CDN****WAF****Trust
Seal**

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



Middle (MitM) attacks.

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](#)

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

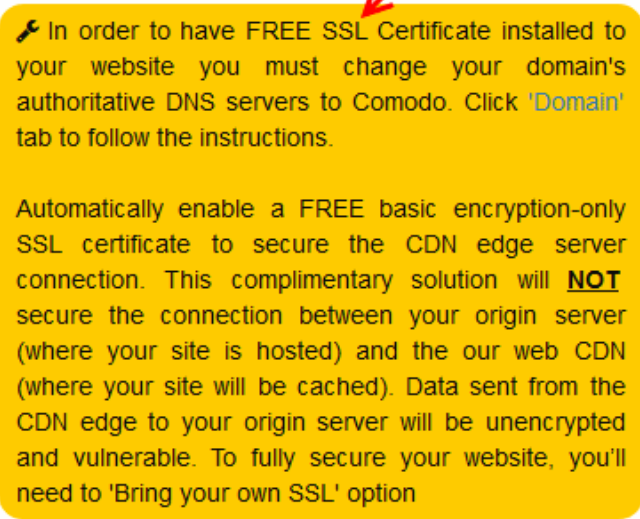
Option A - Change your domain's authoritative DNS servers to Comodo

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

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](#)

[Activate Basic SSL Now](#)

 In order to have FREE SSL Certificate installed to your website you must change your domain's authoritative DNS servers to Comodo. 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

Option B - Create CNAME record pointed back to Comodo > [Click for more details](#)

- 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.

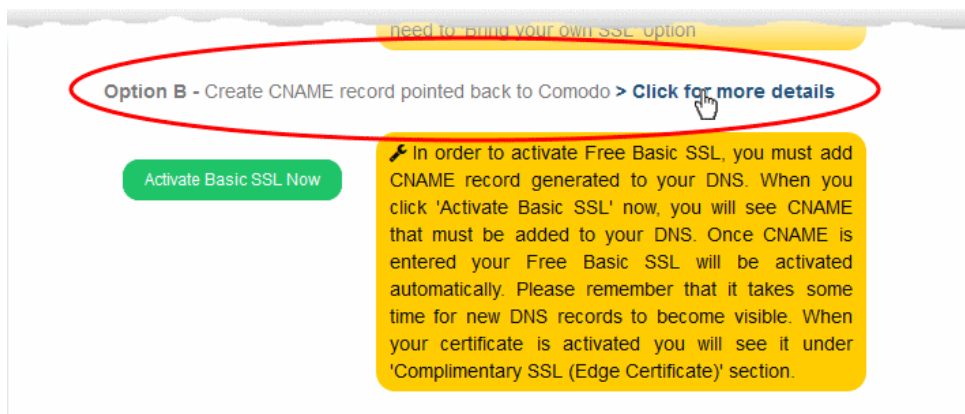
Domain	cwatchdemo.com
Expiration date	Jan 23, 2020 (365 days left)
Wildcard	No

[Uninstall](#)

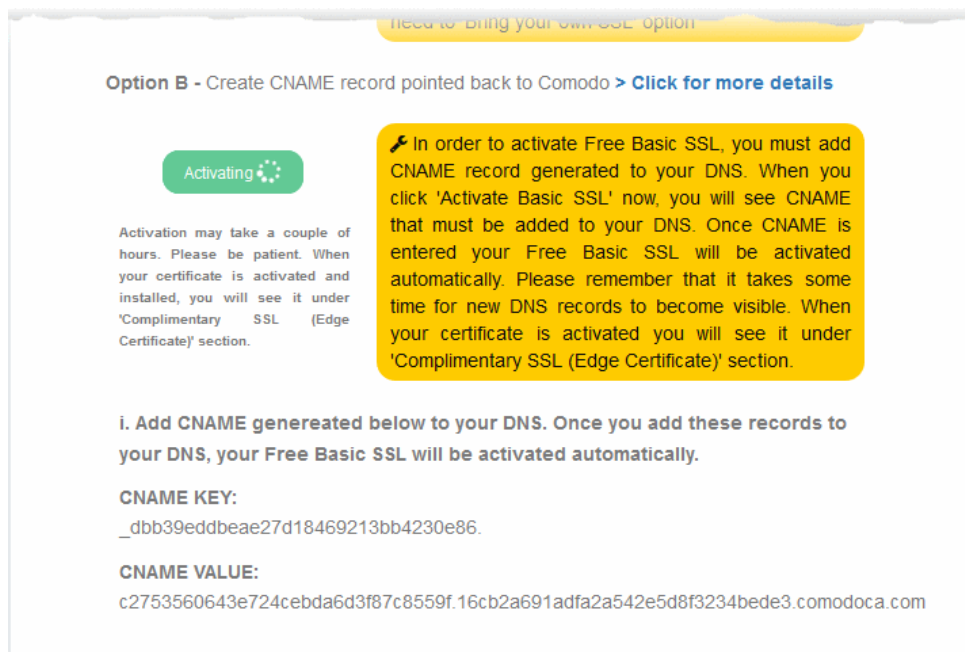
- The certificate is valid for one year and is set for auto-renewal.
- Note – This certificate encrypts the connection between the CDN servers, which host a copy of your site, and your website visitors.
- It does not encrypt the traffic between your web-server and the CDN edge servers.
- You need to 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'



- Click the 'Activate Basic SSL Now' button:



cWatch generates a CNAME record for domain control validation.

- Make a note of the CNAME KEY and CNAME VALUE records
- Go to your site's DNS management page and enter the new CNAME key and CNAME records
 - See <https://support.google.com/domains/answer/3290309?hl=en> if you need more help on this.
- 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 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	cwatchdemo.com
Expiration date	Jan 23, 2020 (365 days left)
Wildcard	No

Uninstall

- 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.

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

B) ENTER DNS RECORDS EXPLICITLY

TYPE	NAME	VALUE	STATUS
CNAME	subone	subonemycwatchcom1326-givkjgav4ntofwivqlm.stagingsecurecdn.com	 Configured.

Configure Malware Scans

- Click the website name > 'Settings' > 'Malware Scan'
- You need to upload a file to your site to activate malware scans.
- You have the option to automatically remove the malware at the end of every scan.
- You can have cWatch upload the file for you, or you can manually upload the file.

The screenshot shows the cWatch interface for 'cwatchdemo.com'. The left sidebar contains a navigation menu with 'Settings' highlighted. The main content area shows the 'Malware Scan' tab selected, with a message indicating that the scanner is not activated. The message includes instructions on how to enable the scanner via FTP/sFTP and provides a link to 'Activate Manually'.

See following sections for detailed guidance on:

- **Automatic configuration**
- **Manual Configuration**

Automatic Configuration

You can have cWatch upload the malware activation file to your site as follows:

- Click a website name on the left and choose 'Settings'
- Open the 'Malware Scan' tab
- Connection Type - select 'FTP' or 'sFTP'. sFTP = encrypted connection
- Specify your web server hostname and login details
- Specify the location to which you want to upload the file. This must be publicly accessible.
- Click 'Enable Scanner' to upload the file

Malware Scan Domain SSL CDN WAF Trust Seal

Malware Scanner has not been activated.

Scanner is not active for this site. In order to start scan and see results regarding the security of your site, you must enable the scanner.

We need to upload our malware monitoring file to your site via FTP/sFTP (this operation can also be done manually).

We need to upload our malware monitoring file to your site via FTP/sFTP (this operation can also be done manually).

We will need FTP/sFTP access only once so no FTP/sFTP access is required after the upload is done.

[Activate Manually](#)

Fill the form to enable malware scanner for 012345.com.

Connection Type:

Hostname: Port:

Username:

Password:

Site Directory:

e.g., /public_html/

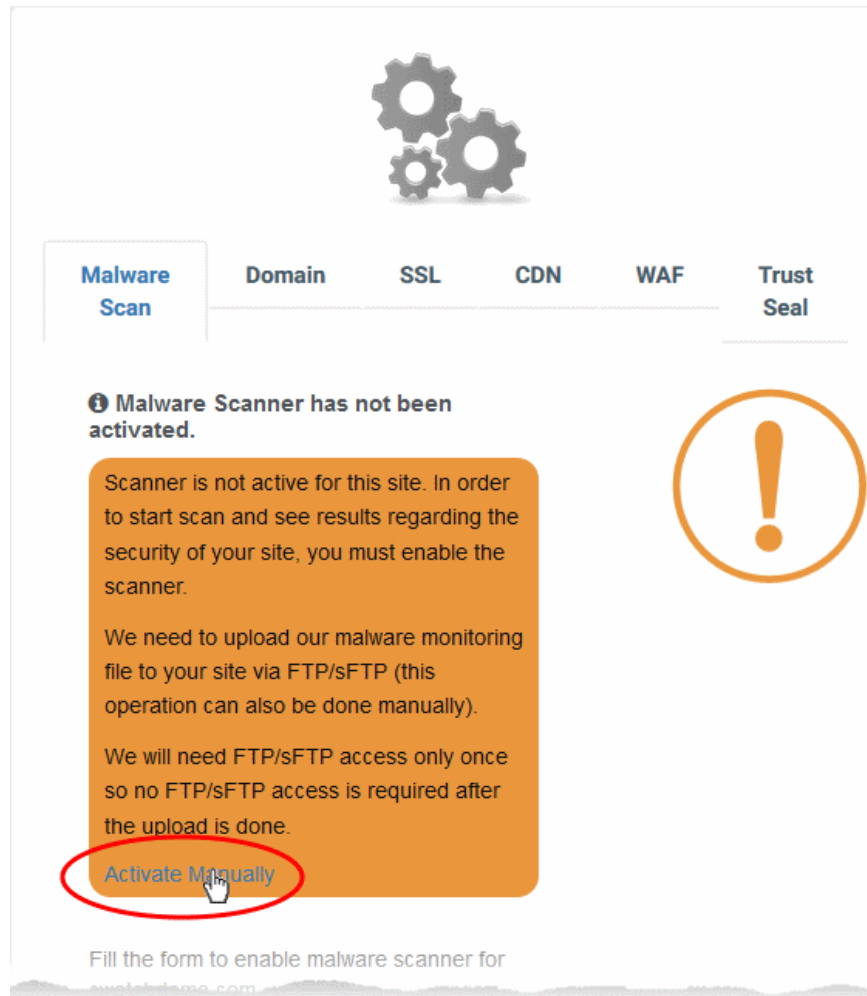
[Enable Scanner](#)

FTP / s/FTP Settings - Table of Parameters	
Parameter	Description
Hostname	IP or hostname of your web-server
Port	By default, FTP/sFTP connections use port 21. Change this setting if your web-server uses a different port for FTP/sFTP connections.
Username/ Password	Login credentials to your web-server.
Site Directory	Location to which cWatch should upload the file. This must be publicly accessible.

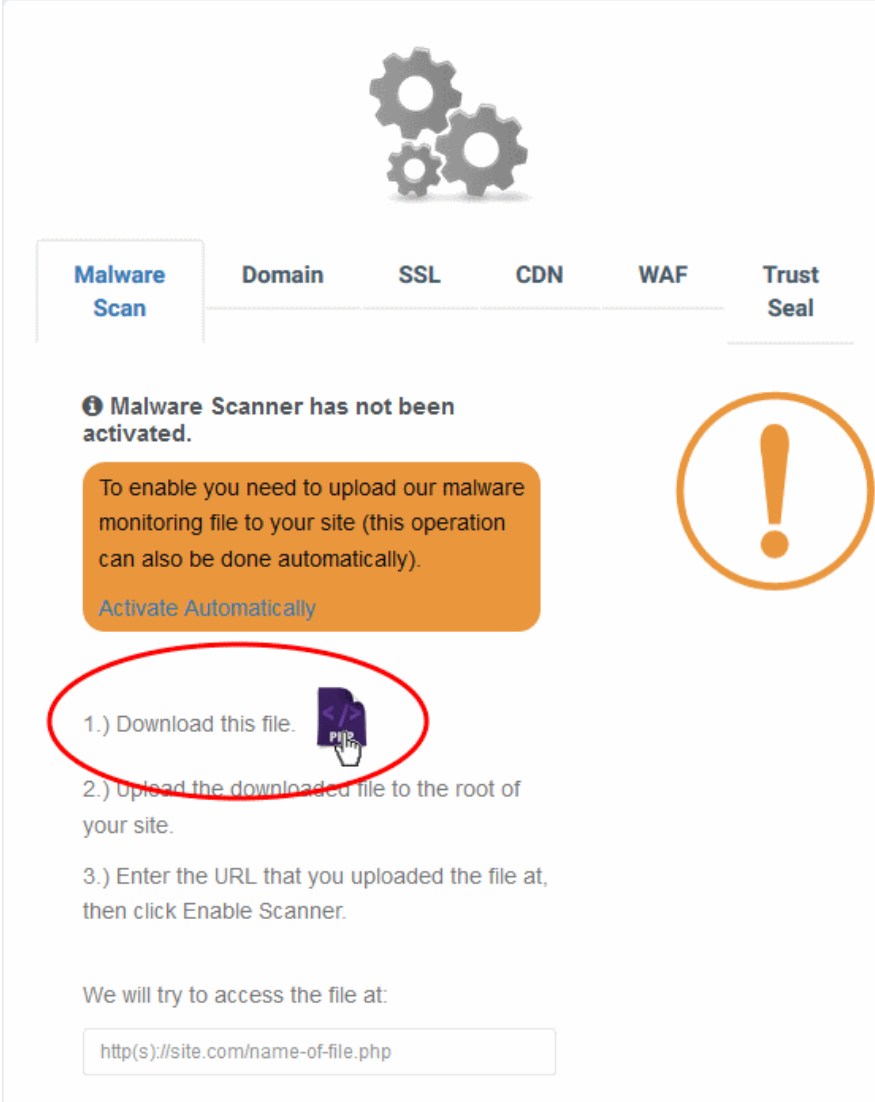
- Note. Our technicians will also use these settings to access your site IF you request them to remove malware.

Manual Configuration

- 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:




Malware Scan Domain SSL CDN WAF Trust Seal

Malware Scanner has not been activated.

To enable you need to upload our malware monitoring file to your site (this operation can also be done automatically).

[Activate Automatically](#)

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 Enable Scanner.

We will try to access the file at:

- 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

The screenshot shows the 'CDN' settings page. At the top, there are navigation tabs: Malware Scan, Domain, SSL, **CDN** (highlighted with a red circle), WAF, and Trust Seal. Below the tabs, there is a 'CACHE SETTINGS' section with the following options:

- Set Default Cache Time:** 1 Day
- Cache Control Header:** 1 Day
- Use Stale:** Serve expired content
- Query String:** Treat as separate cacheable item
- Ignore Cache Control:** Ignore max age set by the origin

At the bottom right of the cache settings, there is a green button labeled 'Update Cache Settings'. Below this, there are two sections: 'PURGE INDIVIDUAL FILES' and 'PURGE ALL FILES'. The 'PURGE INDIVIDUAL FILES' section has a 'File Path' input field. The 'PURGE ALL FILES' section has a description: 'Purging clears the site or file cache on the website. This is useful if you want to clear the cache for a specific file or the entire site.' There is a 'Purge' button below the description.

Cache Settings

Cache Settings - Table of Parameters	
Parameter	Description
Set Default Cache Time	<p>Define how long content fetched from your web servers by the CDN should remain in the CDN cache.</p> <p>This is useful if your website's cache control headers (CCH) are not used or ignored by the browser on your visitors computer.</p> <p>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</p>

	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: <ul style="list-style-type: none"> • 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 INDIVIDUAL FILES

File Path +

Purge

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

SITE SETTINGS

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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Click 'Purge'

Site Settings

Origin IP Resolution On

Origin IP

Custom Host Header

Origin Protocol

Update

- **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

Gzip Compression	<input type="checkbox"/> Serve compressed files with GZip
Content Disposition	<input type="checkbox"/> Force files to download
Remove Cookies	<input type="checkbox"/> Ignore cookies in requests
Pseudo Streaming	<input type="checkbox"/> Enable pseudo stream seeking
Add XFF Header	<input checked="" type="checkbox"/> Add X-Forwarded-For HTTP Header
Add CORS Header	<input type="checkbox"/> Allow Cross Origin Resource Sharing
Enable WebP	<input type="checkbox"/> Allow separate caching for WebP files

Update

Edge Settings - Table of Parameters

Parameter	Description
Gzip Compression – Server compressed files with GZip	Reduces the size of files for faster network transfers. Optimizes bandwidth usage and increases transfer speeds to browsers.

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.

Malware Scan **Domain** **SSL** **CDN** **WAF** **Trust Seal**

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 **On** 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 Status

- Switch WAF protection on or off:

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

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.

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	

- **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:

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	
Google bot	<input checked="" type="checkbox"/>
Google ads bot	<input checked="" type="checkbox"/>
Google Mediapartners bot	<input checked="" type="checkbox"/>
Microsoft MSN bot	<input checked="" type="checkbox"/>
Microsoft Bing bot	<input checked="" type="checkbox"/>
Facebook External Hit bot	<input checked="" type="checkbox"/>
Twitter bot	<input checked="" type="checkbox"/>
Yahoo Inktomi Slurp bot	<input checked="" type="checkbox"/>
Yahoo Slurp bot	<input checked="" type="checkbox"/>

- 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 website visitors into paying customers.
- The site seal is available in multiple languages

Add the trust seal to your website

- Click the cog icon above the navigation menu to open settings.
- Click 'Manage Settings' in the row of the website that you want to configure
- OR
- Click the website name on the left menu, then 'Settings'
- Select the 'Trust Seal' tab:

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.

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.

The screenshot shows the cWatch dashboard. On the left is a navigation menu with options: Dashboard, cwatchdemo.com, Overview, Vulnerabilities, Malware, Cyber Security, CDN Metrics, Firewall Rules, and Settings. The main dashboard area includes a welcome message, a 'Welcome' section with user email and language settings, and three circular gauges for Malware (3), Vulnerabilities (1), and Attacks Blocked (indicated by an exclamation mark). Below these is a table of managed sites:

Site	DDOS	AIN	Advanced Alerts	Managed WAF
+ cwvtest.pp.ua	✓	✓	✓	✓
+ one.bh1-cwatch.online	!	!	Upgrade to PRO License	Upgrade to PREMIUM License
+ testmypc.com	!	!	Upgrade to PRO License	Upgrade to PREMIUM License
+ whatismyipaddress.com	!	!	Upgrade to PRO License	Upgrade to PREMIUM License

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:
- **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 content management system (CMS) scan to identify vulnerabilities in your CMS core site, plugins, themes and more.
 - The following CMS types are supported:
 - WordPress
 - Joomla
 - Drupal
 - ModX
 - Typo3
 - 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-Scans.html> for more details.
 - **Malware** - 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.
 - **Cyber Security** - 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](https://www.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