

COMODO
Creating Trust Online®



Comodo cWatch Web Security

Software Version 4.10

Quick Start Guide

Guide Version 4.10.040119

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo cWatch Web Security - Quick Start Guide

- cWatch Web Security is a cloud-based security intelligence service that continuously monitors and protects websites against millions of attacks and threats.
- In addition to **website protection**, cWatch includes 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**
 - **DNS Configuration**
 - **SSL Configuration**
 - **Configure Malware Scans**
 - **Automatic Configuration**
 - **Manual Configuration**
 - **Configure CDN Settings**
 - **Configure WAF Policies**
 - **Add Trust Seal to Your Websites**
- **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 sites with licenses in the cWatch interface. See **Add Websites** for more details.

Available license types are:

- Basic
- WAF Starter
- Pro
- Premium

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

Feature/Service	Premium	Pro	WAF Starter	Basic
Malware Detection and Removal				
Malware removal by experts	Unlimited	Unlimited	One time	One time
Hack repair and restore				
Vulnerability repair and restore				
Traffic hijack recovery				
SEO/Search poisoning recovery				

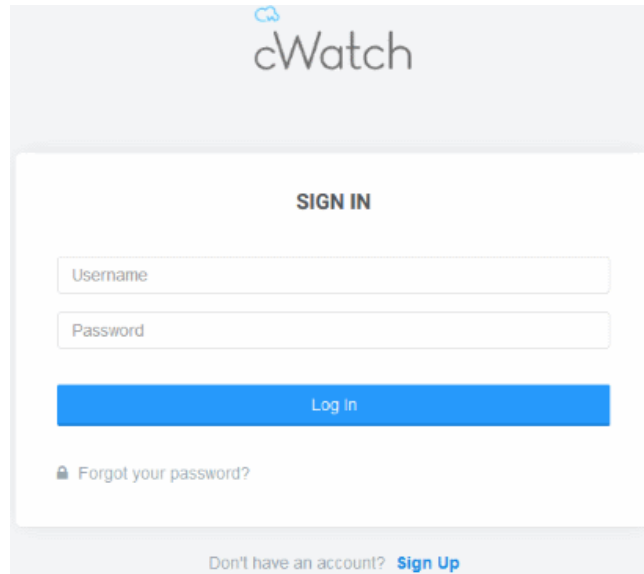
Automatic Malware Removal	✓	✓	✗	✗
Spam & Website Filtering	✓	✓	✗	✗
Malware Scan	Every 6 hours	Every 12 hours	Every 24 hours	Every 24 hours
Vulnerability (OWASP) Detection	Every 6 hours	Every 12 hours	Every 24 hours	Every 24 hours
Security Information and Event Management (SIEM)				
	✓	✓	✗	✗
24/7 Cyber-Security Operations Center (CSOC)				
	✓	✓	✓	✗
Dedicated analyst	✓	✓	✓	✗
Web Application Firewall (WAF)				
Custom WAF rules	✓	✗	✗	✗
Bot Protection	✓	✓	✓	✗
Scraping Protection	✓	✓	✓	✗
Content Delivery Network (CDN)				
Layer 7 DDoS Protection	✓	✓	✓	✓
Layer 3, 4, 5 & 6 DDoS Protection	✓	✓	✓	✓
Trust Seal	✓	✓	✓	✓

After completing a purchase:

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

Login to cWatch

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

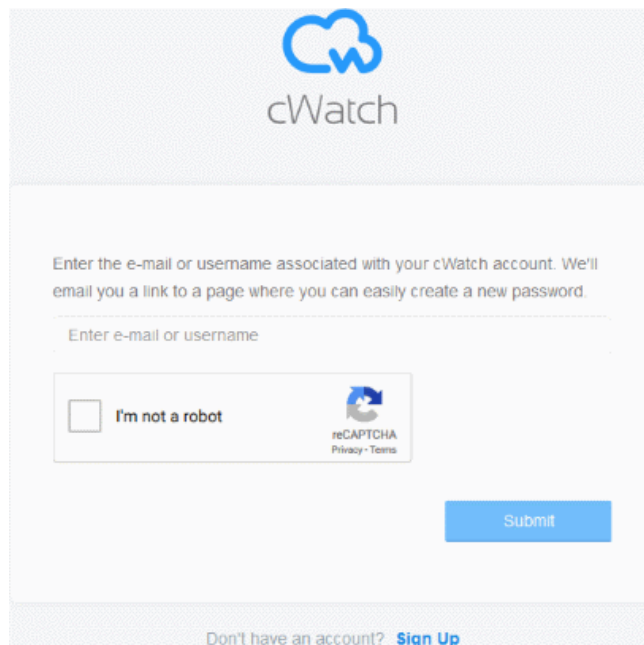


First time Login:

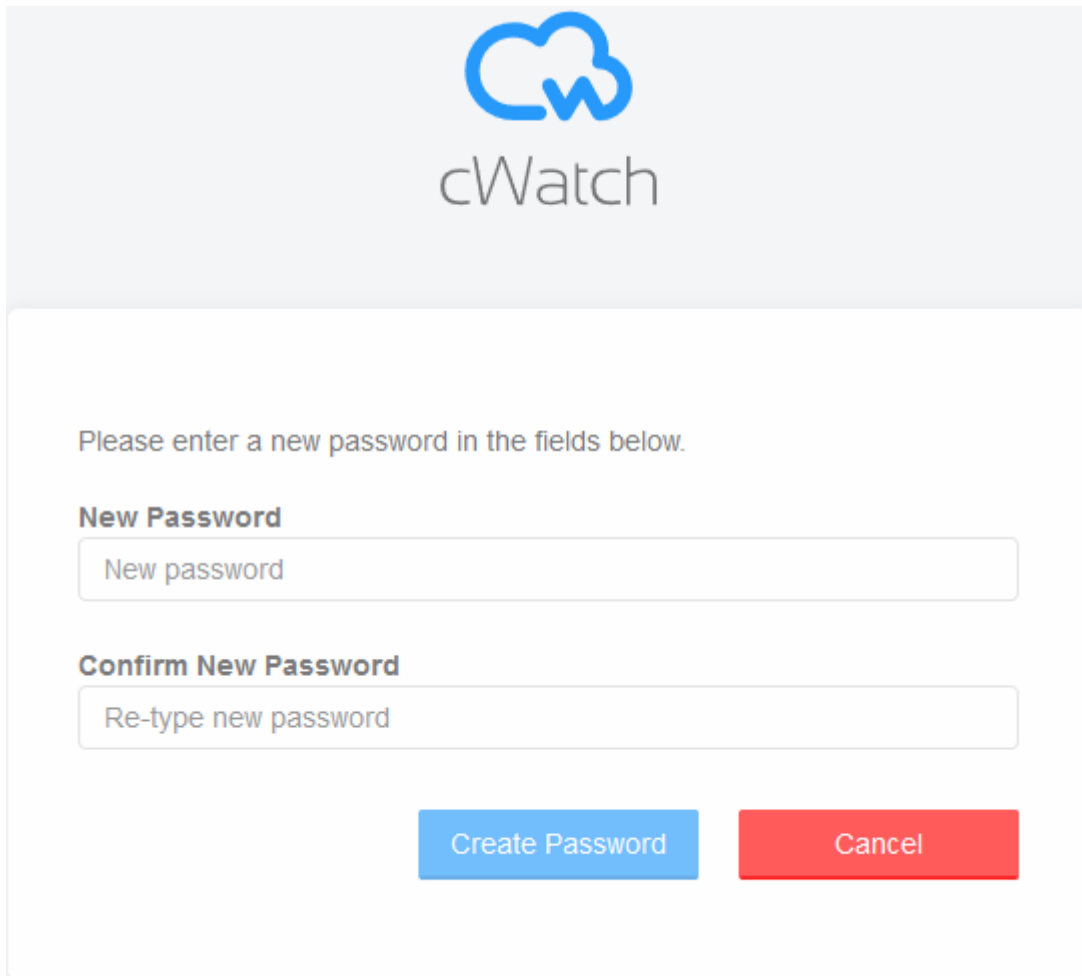
- Get your username and password from the cWatch confirmation email.
- After logging in, we strongly recommend you change your password for security reasons.

Lost Passwords

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

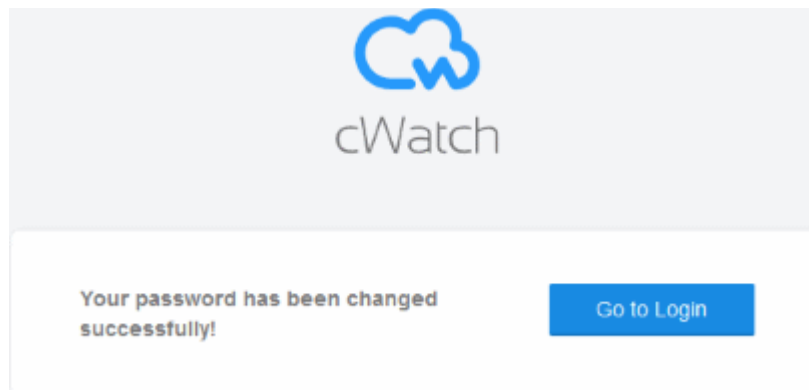


- You will receive a password reset mail.
- Click 'Reset Password' to open the password creation page.
- Enter a password and confirm it:



The screenshot shows the cWatch logo at the top. Below it, the text reads "Please enter a new password in the fields below." There are two input fields: "New Password" with the placeholder text "New password" and "Confirm New Password" with the placeholder text "Re-type new password". At the bottom, there are two buttons: "Create Password" (blue) and "Cancel" (red).

- Click 'Create Password'



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

Add Websites

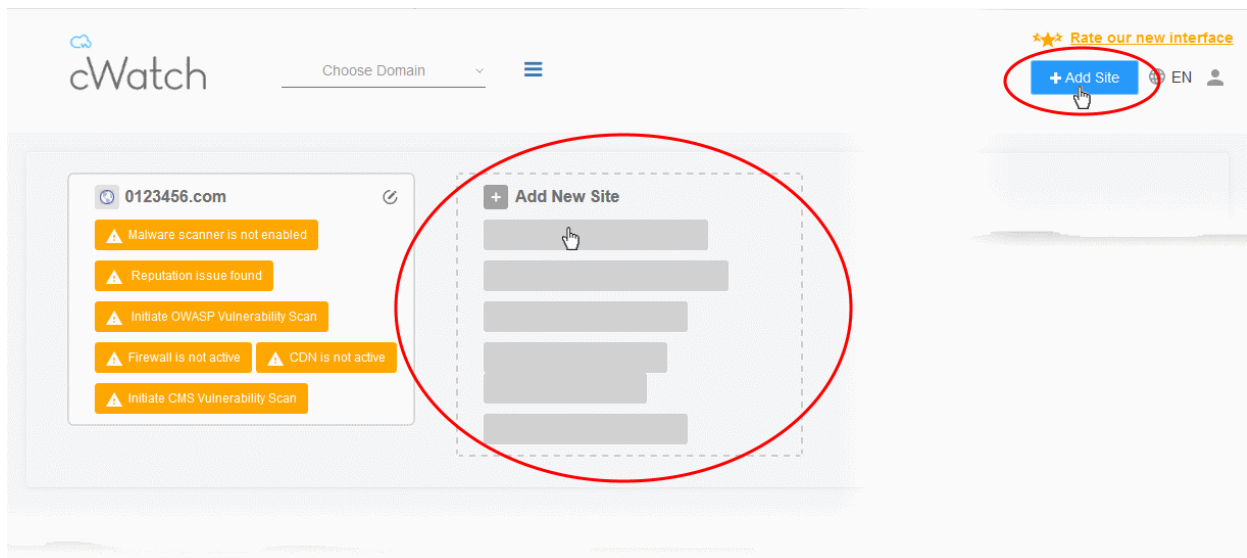
- You need to add websites to cWatch to enable protection and take advantage of the content delivery network (CDN).
- The number of domains you can add depends on the number of licenses you purchased. Each license covers one FQDN. You need separate licenses for sub-domains.
- Once added, you can configure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

Add a new domain

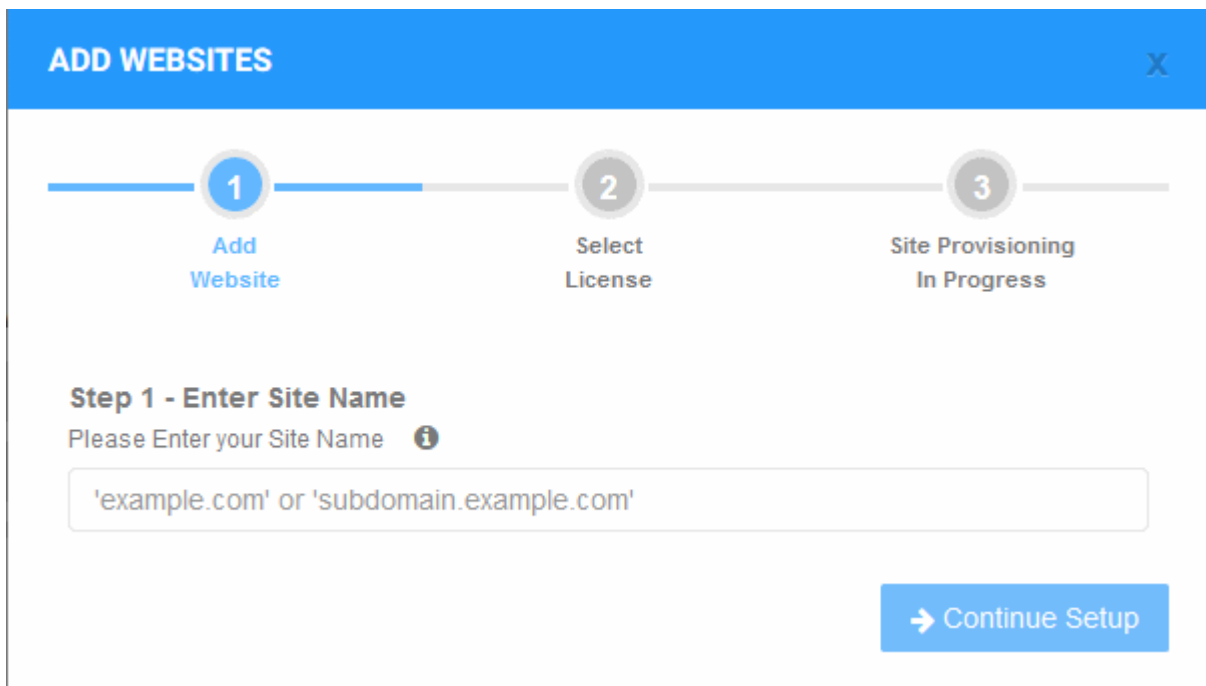
- Login to cWatch at <https://login.cwatch.comodo.com/login> with your Comodo account credentials.

The dashboard appears and shows enrolled websites as tiles.

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



The 'Add Websites' wizard starts:

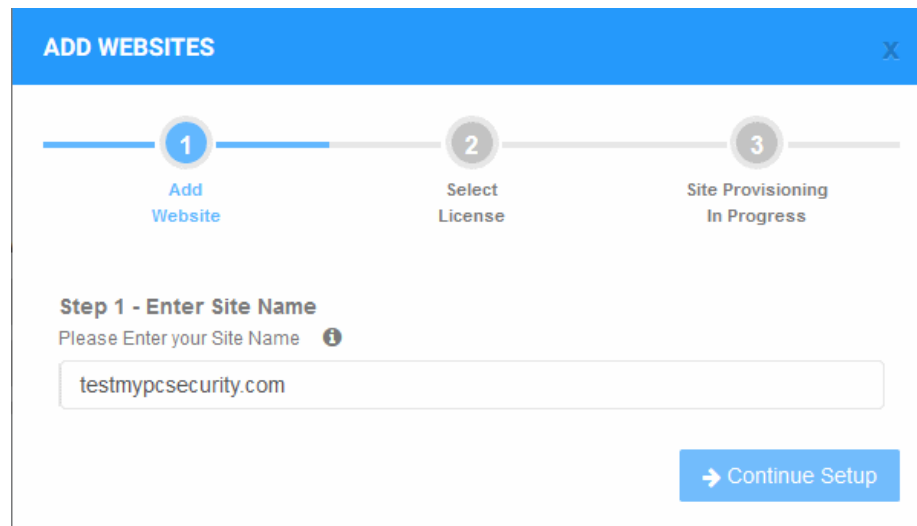


The wizard has three steps:

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

Step 1 - Register your website

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

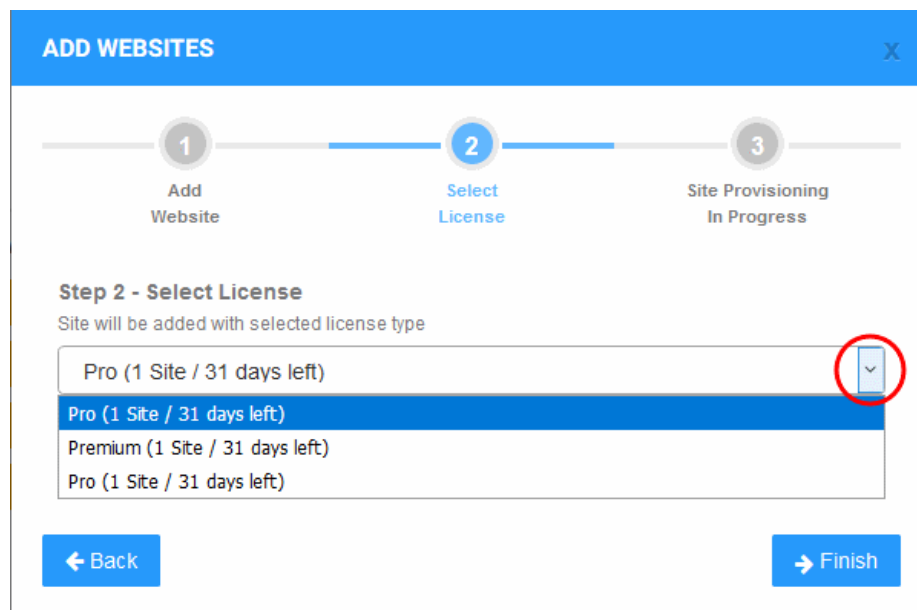


- Click 'Continue Setup' to move to the next step.

Step 2 - Select License

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

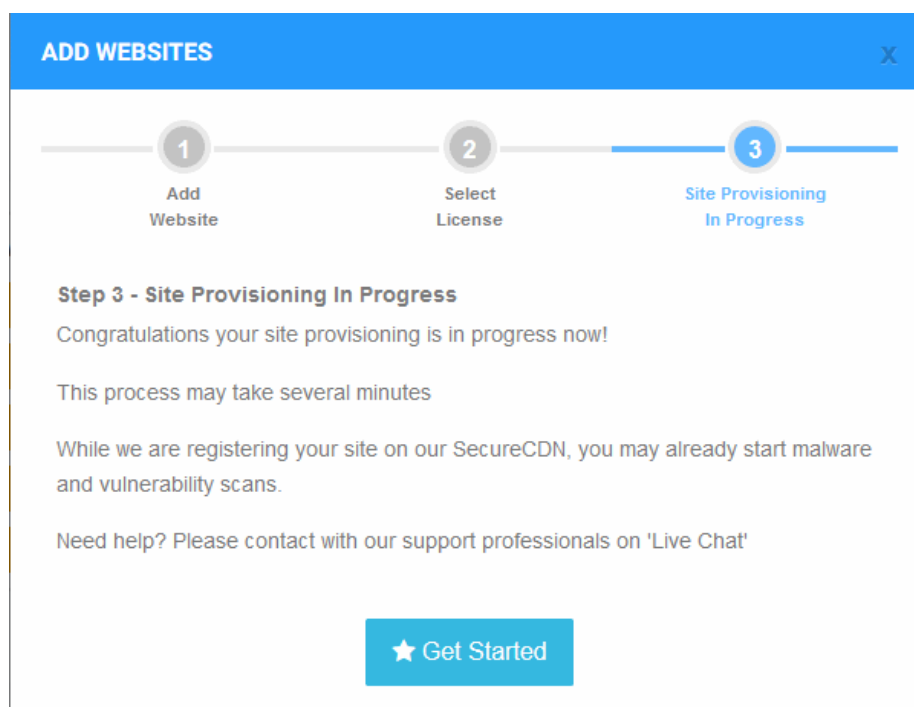
- cWatch features vary according to license type. Details are available [here](#).
- The drop-down lists all licenses that you have purchased.
- Choose the type of license you wish to associate with the domain:



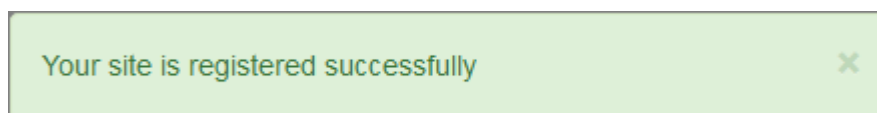
- Click 'Finish' to proceed.

Step 3 - Finalization

The final stage is for cWatch to provision your site:



You will see the following confirmation message when registration is complete:



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

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

Note:

- cWatch auto-generates a CNAME DNS record for the website you just 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 record:
 - Select a website in the drop-down at top-left of the dashboard
 - Select the 'DNS' tab (or click the hamburger button and select 'DNS')
 - The CNAME DNS record is shown under 'DNS'
- Your web host may be able to help you add the CNAME. Guidance is also available at <https://support.google.com/a/topic/1615038?hl=en>.

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

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 **DNS Configuration** 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 Scans](#) for more details.
- Configure the CDN in order to accelerate site loading times and improve security. See [Configure CDN Settings](#) for more details.
- Configure Web Application Firewall (WAF) settings. See [Configure WAF Policies](#) for more details.
- Configure your site's trust seal. See [Add Trust Seal to Your Websites](#) for more details.

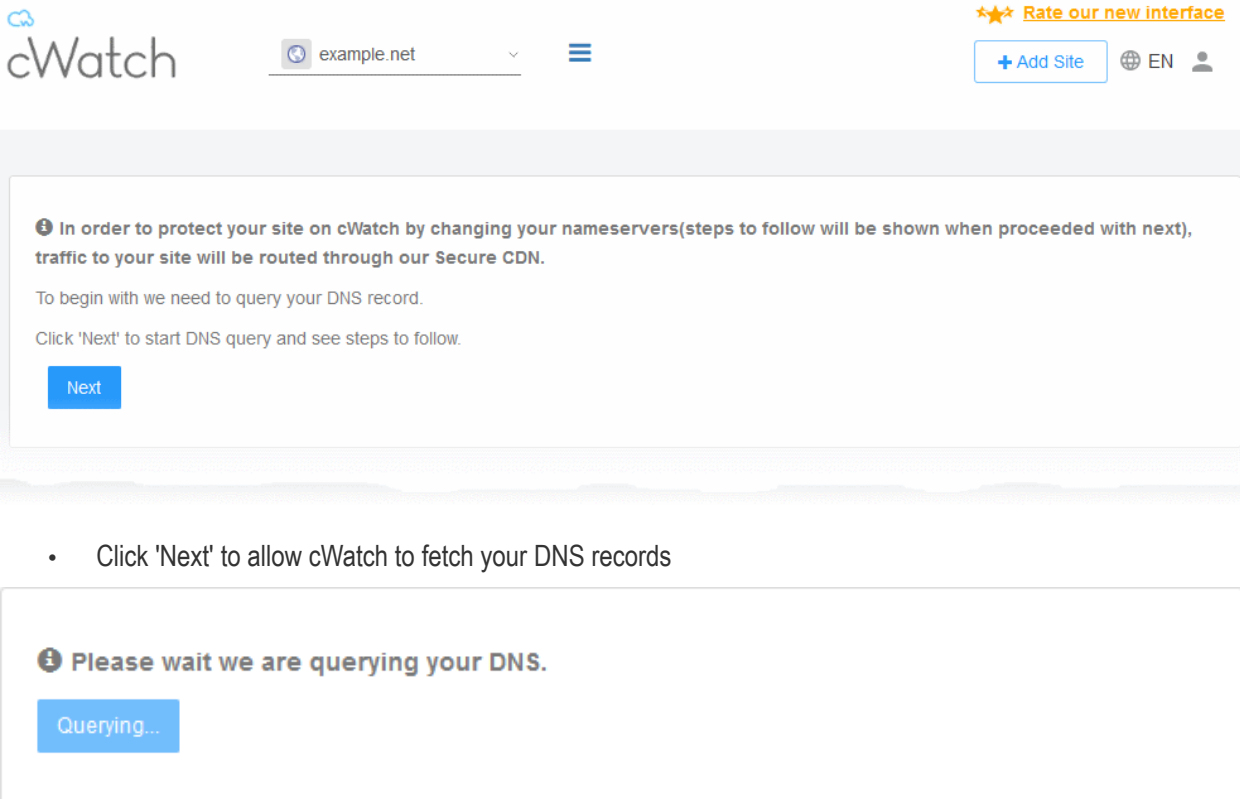
DNS Configuration

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

Configure DNS settings on your site

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'DNS' tab (or click the hamburger button and select 'DNS')

cWatch first queries your DNS servers to collect your existing records:



The screenshot shows the cWatch dashboard interface. At the top left is the cWatch logo. In the center, there is a dropdown menu with 'example.net' selected. To the right, there is a 'Rate our new interface' link with three stars, an 'Add Site' button, and language/user icons. The main content area contains a message box with the following text: 'In order to protect your site on cWatch by changing your nameservers(steps to follow will be shown when proceeded with next), traffic to your site will be routed through our Secure CDN. To begin with we need to query your DNS record. Click 'Next' to start DNS query and see steps to follow.' Below this message is a blue 'Next' button. Below the message box is a second message box with the text: 'Please wait we are querying your DNS.' Below this message is a blue 'Querying...' button.

- Click 'Next' to allow cWatch to fetch your DNS records

The DNS configuration page for the site will then load, complete with the site's name server (NS) details:

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

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

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

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

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

DNS Records

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

TYPE	NAME	VALUE	TTL	
A	<input type="text" value="Name"/>	<input type="text" value="IPv4 Address"/>	Automatic TTL	<input type="button" value="Add Record"/>
<input type="text" value="Search DNS Record"/>				
TYPE	NAME	VALUE	TTL	STATUS
TXT	@	"v=spf1 -all"	Automatic TTL	<input type="button" value="Deactivate"/>

- Go to your site's DNS management page and enter the new name servers.
- See <https://support.google.com/domains/answer/3290309?hl=en> if you need more help on name server changes.

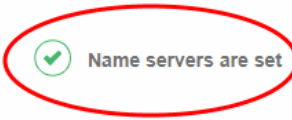
You can view whether the change was successful in the cWatch interface:

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

DNS Manage your Domain Name Server(DNS) settings.

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

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

TYPE	STATUS
ns1.dnsbycomodo.net	
ns2.dnsbycomodo.net	
ns3.dnsbycomodo.net	
ns4.dnsbycomodo.net	

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

Note:

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

SSL Configuration

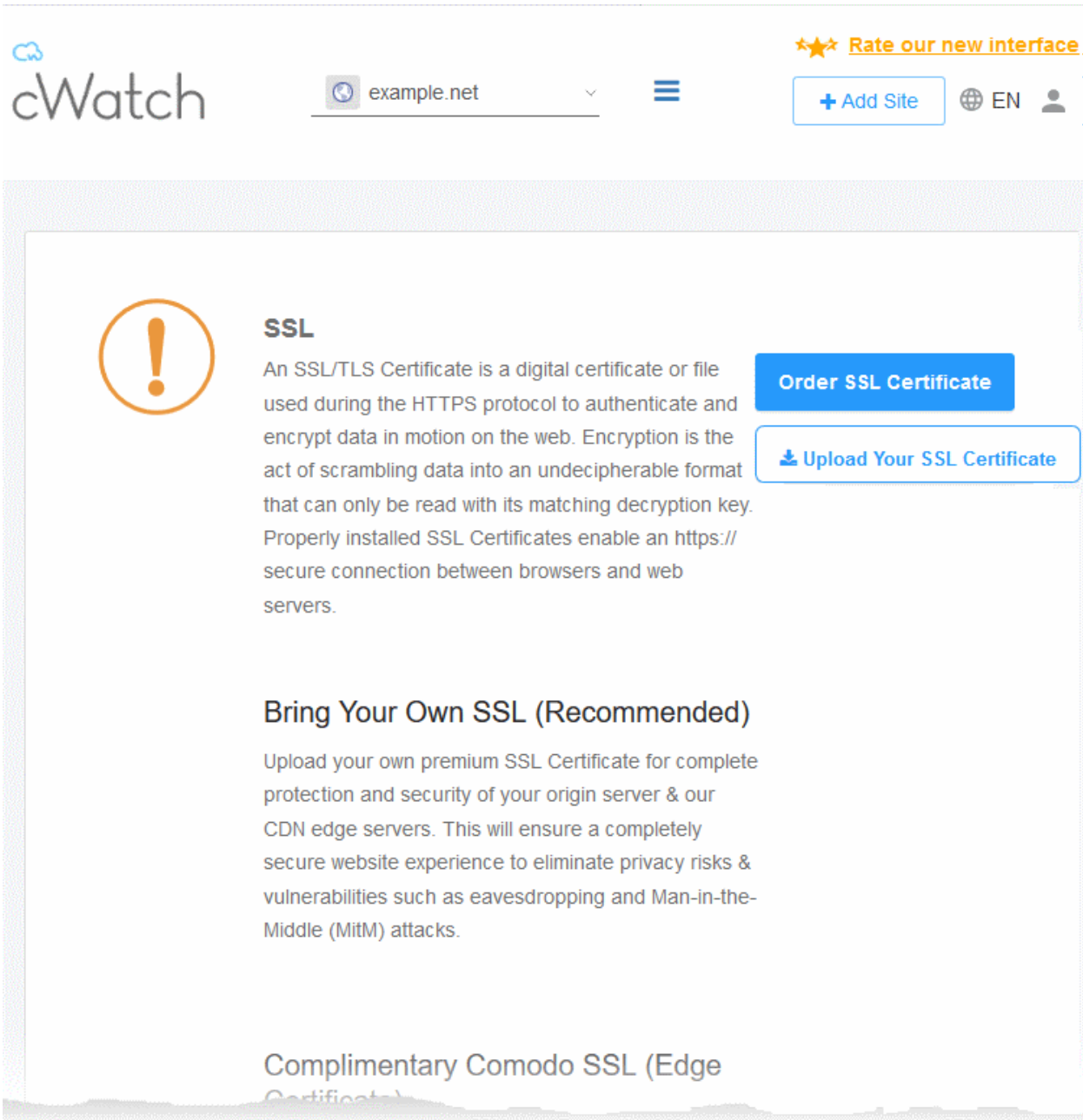
- Select a website from the drop-down at top-left and choose 'SSL'
- An SSL/TLS certificate is placed on a website to identify the domain owner, and to encrypt all data that passes between the site and a visitor's browser.
- Sites that use a SSL/TLS certificate have a URL that begins with HTTPS. For 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 site to the cWatch CDN edge servers. Recommended for most customers.
 - This will secure the traffic between your site (the origin server) and the cWatch CDN.
 - See [Upload your own SSL Certificate](#) to find out how to deploy your certificate
- **Complimentary Comodo SSL**
 - Get a free SSL from Comodo deployed on the CDN Edge servers.
 - You need to configure your site to use Comodo DNS in order to get the free SSL certificate. This can be done in two ways:
 - Change your domain's authoritative DNS servers to Comodo DNS
 - Enter DNS records explicitly
 - Help to configure DNS is available in the online help page - [Activate CDN for a Website](#).
 - See [Install Complimentary SSL Certificate](#) to find out how to deploy your free certificate

Upload your own SSL Certificate

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



SSL

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

[Order SSL Certificate](#)

[Upload Your SSL 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.

Complimentary Comodo SSL (Edge Certificate)

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

SSL

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

[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.

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

📘 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.

[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:

Upload Your Certificate - Form Parameters	
Parameter	Description
	<pre> -----BEGIN CERTIFICATE----- MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGE wJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA 1UECzMC VU4xFDASBgNVBAMTC0hlcm9uZyBZYW5nMB4XDTA1MDcxNTIxMTk0N1oXD TA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAGTA1BOMQswCQYDV QQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTA1VOMRQwEgYDVQQDEwtIZXJvb mcgWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBe wKE/B7j V14qeysl nr26xZUSVko36ZnhiaO/zbMOoRcKK9vEcgmTcLFuQTWDl3RA gMBAAGj gbEwga4wHQYDVR0OBByEFFXI70krXeQDxZgbaCQoR4jUDncEMH8GA1UdI wR4MHAA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMQswCQYDVQQGEwJDTjELM AkGA1UE CBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECzMCV U4xFDAS BgNVBAMTC0hlcm9uZyBZYW5nggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIh vcNAQEE BQADQQA/ugzBrjjK9jcWnDVfGHlk3icNRq0oV7Ri32z/ +HQX67aRfgZu7KWdI+Ju Wm7DCfrPNGVwFWUQOmsPue9rZBgO -----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.



SSL

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

[Order SSL 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.

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

[Uninstall](#)

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

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

Complimentary Comodo SSL (Edge Certificate)

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

**Option A -
Change your domain's
authoritative DNS**
[> Click for more details](#)

**Create CNAME record
pointed back to us**
[> Click for more details](#)

You have two options to enable the free certificate:

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

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

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

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

See **DNS Configuration** for more details.

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

Option A - Change your domain's authoritative DNS

[> Click for more details](#)

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 ours. Click 'Domain' tab to follow the instructions.

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

Create CNAME record pointed back to us

[> 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	www.example.net
Expiration date	Mar 24, 2020 (362 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'

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

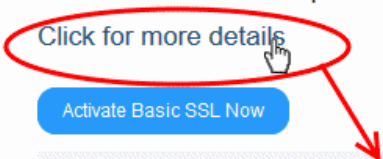

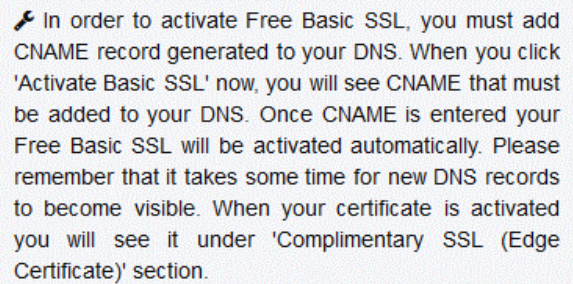
[Click for more details](#)

Option B

Create CNAME record pointed back to Comodo

[Click for more details](#)

[Activate Basic SSL Now](#)


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

- Click the 'Activate Basic SSL Now' button:


Option B

Create CNAME record pointed back to Comodo

[Click for more details](#)

Activating 

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

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

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

CNAME KEY:

`_32cba9664abf865b2fafcc9a13ce99d4`

CNAME VALUE:

`2b62240e2e92177963e113516c4bba0c.3a43f61c206dce84bb456d6ac4a41964.comodoca.com`

cWatch generates a CNAME record for domain control validation.

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

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

Complimentary Comodo SSL (Edge Certificate)

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

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

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.

Configure Malware Scans

- Click the website name > 'Settings' > 'Malware Scan'
- You need to upload the cWatch scanner file to your site in order to run malware scans.
- One done, cWatch will run scheduled scans on all files hosted on the website. You can also start manual scans from the 'Malware' page.

Upload the scanner file

- Select the website from the menu at top-left of the dashboard
- Click the 'Malware' tab (or click the hamburger button and select "Malware")
- Click 'Enable Scanner'

The screenshot shows the cWatch dashboard for the domain 'testmypcsecurity.com'. A notification at the top states 'Malware Scanner has not been activated.' and provides instructions to start a scan. A red circle highlights the 'Enable Scanner' button in the notification, with a red arrow pointing to the 'ENABLE SCANNER' modal window below. The modal window contains the following text and form elements:

ENABLE SCANNER [Close]

In order to enable malware detection, we need to connect to your site via FTP/sFTP and upload server side scan agent.

Please fill the form above and click 'Enable Scanner'.

Automatic
 Manual

Connection Type:

Hostname: 21

Username:

Password:

Site Directory:
e.g., /public_html/.

See the following sections for help with:

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

Automatic Configuration

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Malware' tab (or click the hamburger button and select "Malware")
- Click 'Enable Scanner'

ENABLE SCANNER
✕

In order to enable malware detection, we need to connect to your site via FTP/sFTP and upload server side scan agent.

Please fill the form above and click 'Enable Scanner'.

Automatic
 Manual

Connection Type: FTP

↕

e.g., /public_html/.

Cancel
Enable Scanner

- Choose 'Automatic' and enter your website information

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.

- Click 'Enable Scanner' to upload the file
- Note. Our technicians will also use these settings to access your site IF you request them to remove malware
- Once uploaded, automatic scans are enabled on your website.

Manual Configuration

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Malware' tab (or click the hamburger button and select "Malware")
- Click 'Enable Scanner'
- Select 'Manual' in the 'Enable Scanner' dialog


ENABLE SCANNER ✕

In order to enable malware detection, we need to connect to your site via FTP/sFTP and upload server side scan agent.

Please fill the form above and click 'Enable Scanner'.

Automatic

Manual

1.) Download this file. 

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

3.) Enter the URL that you uploaded the file at, then click 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 [DNS Configuration](#) for more information.
- You can also configure the DNS settings of the website from the 'CDN' > 'Settings' > 'Activation' page. See the online help page <https://help.comodo.com/topic-285-1-848-13908-Activate-CDN-for-a-Website.html>

if you need guidance on this.

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.

Configure CDN Settings

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'CDN' tab (or click the hamburger button and select 'Firewall')
- Click 'Settings' on the 'CDN' page
- Click the 'CDN' tab (if not already opened)

The screenshot shows the cWatch dashboard for 'example.net'. The 'Settings' page is active, with the 'CDN' tab selected. The 'Cache Settings' section includes:

- SET DEFAULT CACHE TIME:** 1 Day
- CACHE CONTROL HEADER:** 1 Day
- USE STALE:** Serve expired content
- QUERY STRING:** Treat as separate cacheable item

On the right side, there are two purge options:

- Purge Individual Files:** Includes a 'FILE PATH' input field and a 'Purge' button.
- Purge All Files:** Includes a description: 'Purging clears the site or file cache on the edge servers and gets rebuilt from the origin on the next request.' and a 'Purge' button.

Cache Settings

Cache Settings

(i) SET DEFAULT CACHE TIME

1 Day ▼

(i) CACHE CONTROL HEADER

1 Day ▼

(i) USE STALE

Serve expired content

(i) QUERY STRING

Treat as separate cacheable item

(i) IGNORE CACHE CONTROL

Ignore max age set by the origin

Update

Cache Settings - Table of Parameters	
Parameter	Description
Set Default Cache Time	<p>Define how long content fetched from your web servers should remain in the CDN cache. Cached content is used to accelerate site loading times for your visitors.</p> <p>The CDN will collect refreshed content from your site when this period expires.</p> <p>This setting is useful if your website's cache control headers (CCH) are not used or ignored by the browser on your visitors computer. See next row for more on this.</p>
Cache Control Header	<p>Defines how long cached content in the web browser can be reused without checking the web server for updates.</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 repeatedly from the server.</p>

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	Web-pages with a query string (e.g.'?q=something') will be cached as separate files. CDN updates the cached files whenever the original pages are updated.
Ignore Cache	Visitor's browsers use the value in 'Set default cache time' regardless of the time-to-live and header expiry settings of your pages.

- 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

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 blue '+' 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

Site Settings

i ORIGIN IP RESOLUTION

ORIGIN IP

i CUSTOM HOST HEADER

i ORIGIN PROTOCOL

Update

Site Settings	
Origin IP Resolution	<p>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.</p> <ul style="list-style-type: none"> 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	Enter the custom host header in this field if the host header for your site is different to the domain name.
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

Serve compressed files with GZip

ⓘ CONTENT DISPOSITION

Force files to download

ⓘ REMOVE COOKIES

Ignore cookies in requests

ⓘ PSEUDO STREAMING

Enable pseudo stream seeking

ⓘ ADD XFF HEADER

Add X-Forwarded-For HTTP Header

ⓘ ADD CORS HEADER

Allow Cross Origin Resource Sharing

ⓘ ENABLE WEBP

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	The CDN identifies the actual IP address of the client connecting to the website. This is used to render location based content, logging and more.
Add CORS Header - Allow Cross Origin Resource Sharing	Appends '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 Policies

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

Configure WAF settings

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Firewall' tab (or click the hamburger button and select 'Firewall')
- Click 'Settings' to open the 'WAF Settings' page

Firewall [Settings](#)

Custom WAF Rules Total 2 rules

← Settings

WAF SETTINGS

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

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

WAF POLICIES

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

WAF Settings

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

WAF SETTINGS

Our Web Application Firewall (WAF) blocks hacking attempts, such as SQL injections and XSS, and malicious 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

WAF Polices


- The 'WAF Policies' area shows a list of all WAF policies.
- Click the '+' symbol to view the constituent rules in a policy. You can enable / disable rules as required.

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

Enable / disable firewall rule(s)

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

NAME	STATUS
Application DDoS Protection	Active
+ User Agents	
 WAF & OWASP Top Threats	
SQL Injection	<input checked="" type="checkbox"/>
XSS Attack	<input checked="" type="checkbox"/>
Shellshock Attack	<input checked="" type="checkbox"/>
Remote File Inclusion	<input checked="" type="checkbox"/>
Wordpress	<input checked="" type="checkbox"/>
Invalid User Agent	<input type="checkbox"/>
Apache Struts Exploit	<input checked="" type="checkbox"/>
Local File Inclusion	<input checked="" type="checkbox"/>
Common Web Application Vulnerabilities	<input checked="" type="checkbox"/>
Web Shell Execution Attempt	<input checked="" type="checkbox"/>
Response Header Injection	<input checked="" type="checkbox"/>
Template for keren tests	<input type="checkbox"/>
+ CSRF Attacks	
+ IP Reputation	

- Use the check-boxes to enable or disable particular rules.
- Any changes will be deployed in approximately a minute.

Add Trust Seal to Your Websites

- Select a website from the drop-down at top-left and choose '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

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Trust Seal' tab (or click the hamburger button and select 'Trust Seal')

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

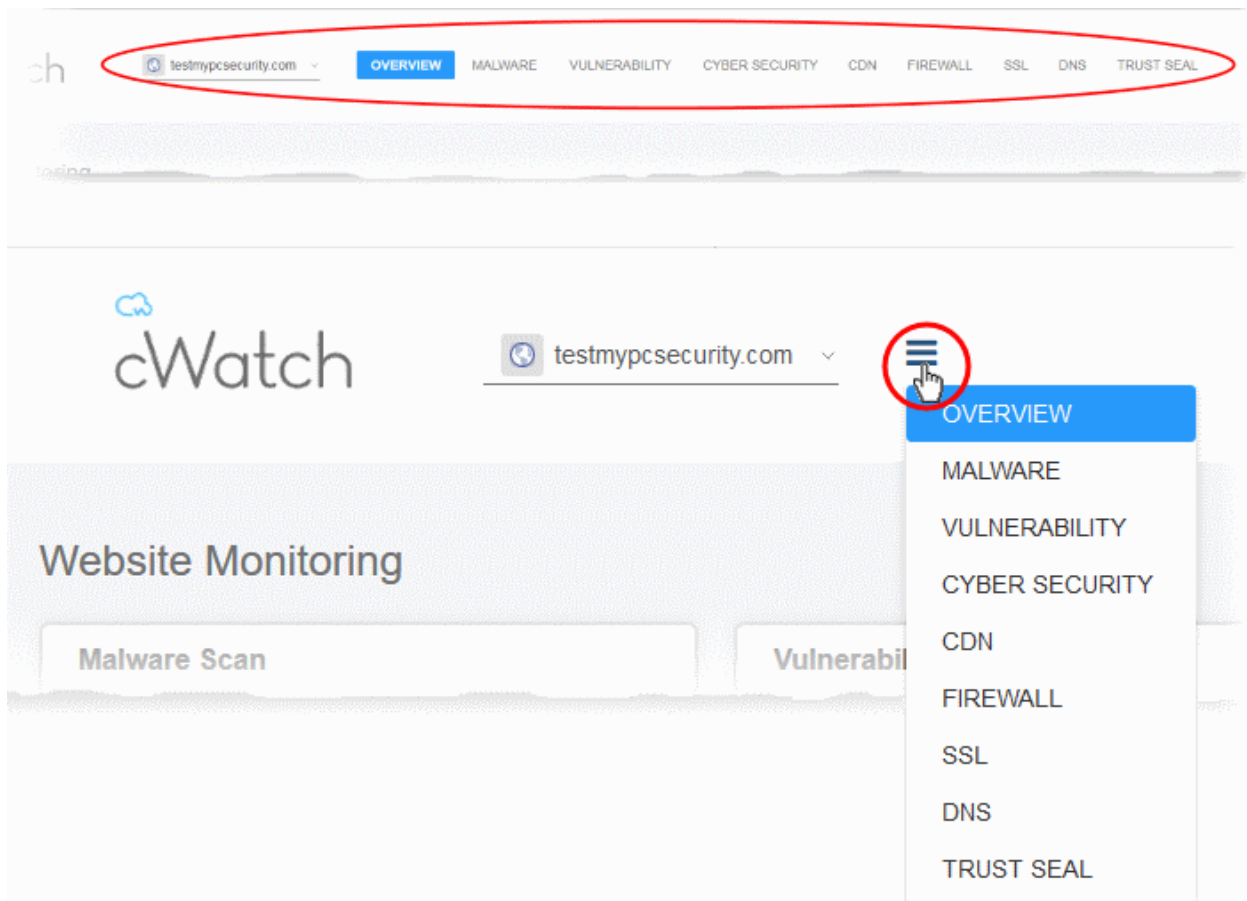
Here are some sample scenarios:

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

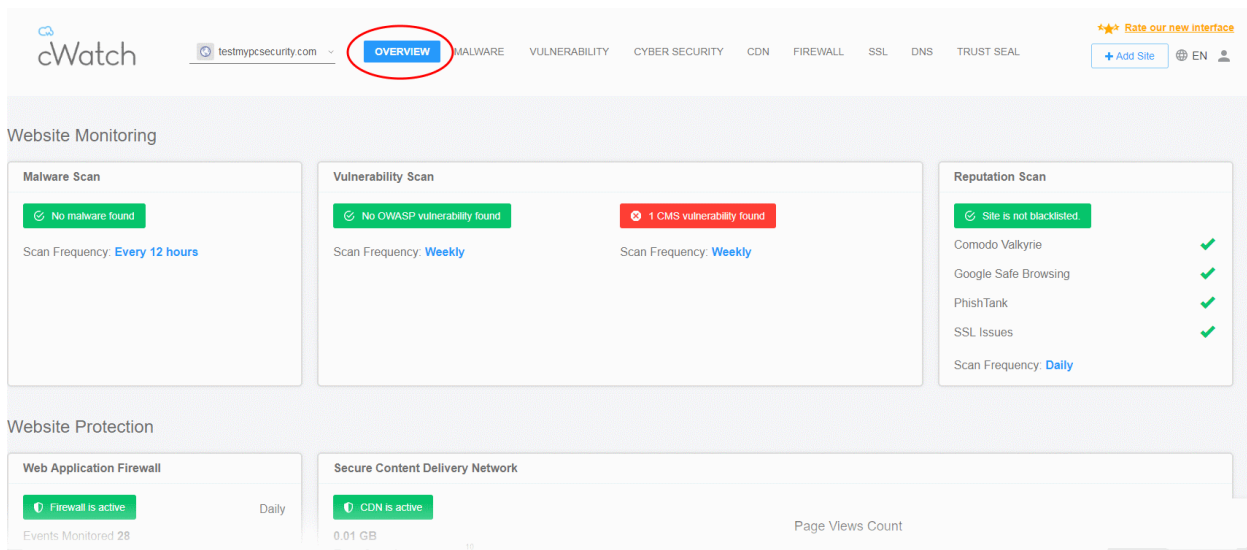
- No negative messaging is shown if your site fails a scan/appears on a blacklist. After a grace period, the seal will simply disappear, replaced by a transparent single-pixel image. The seal will reappear when the issues are fixed.
- Select the language which should be used in the trust seal
- Follow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

Use the cWatch Interface

- The cWatch dashboard contains an at-a-glance summary of security status of all domains that are protected and managed.
 - Click the 'cWatch' logo in the top-left corner to open the dashboard at any time
 - See <https://help.comodo.com/topic-285-1-848-11006-The-Dashboard.html>.
- The drop-down on the left lets you choose the domain you want to manage and to view threat statistics.
 - Links to all major areas of the interface are in the top menu. They may be collapsed into a hamburger menu if your browser window is not wide enough.



- The main display shows data for the selected item.



- **Overview** - Summary of monitored parameters, security status and CDN performance. See <https://help.comodo.com/topic-285-1-848-11010-Website-Overview.html> for more details.
- **Malware** - Activate malware scanner, run virus scans, view scan results and monitor malware cleanup progress. You need to upload our .php file to the server to enable malware scans. See <https://help.comodo.com/topic-285-1-848-11011-Malware-Scans.html> for more details.
- **Vulnerabilities:**
 - CMS vulnerability scans - Identify weaknesses in your content management system (CMS). You can also enable or disable automatic weekly scans.

The scanner supports the following types of CMS:

- WordPress
- Joomla
- Drupal
- ModX
- Typo3

You can run on-demand vulnerability/CMS scans on the site at anytime.

- OWASP top-ten threats - Scan your site for OWASP vulnerabilities and view results. You can also enable or disable automatic weekly scans.

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

- **Cyber Security** - Real-time analysis of attack patterns on your website 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** - Activate and configure CDN services and view details 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.html> to find out more.
- **Firewall** - Configure Web Application Firewall (WAF) policies for the domain and create your own custom Firewall rules. See <https://help.comodo.com/topic-285-1-848-13906-Firewall-Rules.html> for more information.
- **SSL** - Secure traffic between CDN edge servers and your website visitors. You can get a complimentary SSL certificate from Comodo. Alternatively, you can upload an existing certificate. See <https://help.comodo.com/topic-285-1-848-12464-SSL-Configuration.html> for more details.
- **DNS** - Configure DNS and nameservers in order to enable cWatch protection. See <https://help.comodo.com/topic-285-1-848-12463-DNS-Configuration.html> for more information.
- **Trust Seal** - Add a cWatch site seal on managed websites. There are two types of seals: 'Malware Free' and 'Protected'. See <https://help.comodo.com/topic-285-1-848-13683-Add-Trust-Seal-to-your-Websites.html> for more details.

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