

**COMODO**  
Creating Trust Online®



# Comodo

## cWatch Web Security

Software Version 4.8

# Website Administrator Guide

Guide Version 4.8.012819

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

## Table of Contents

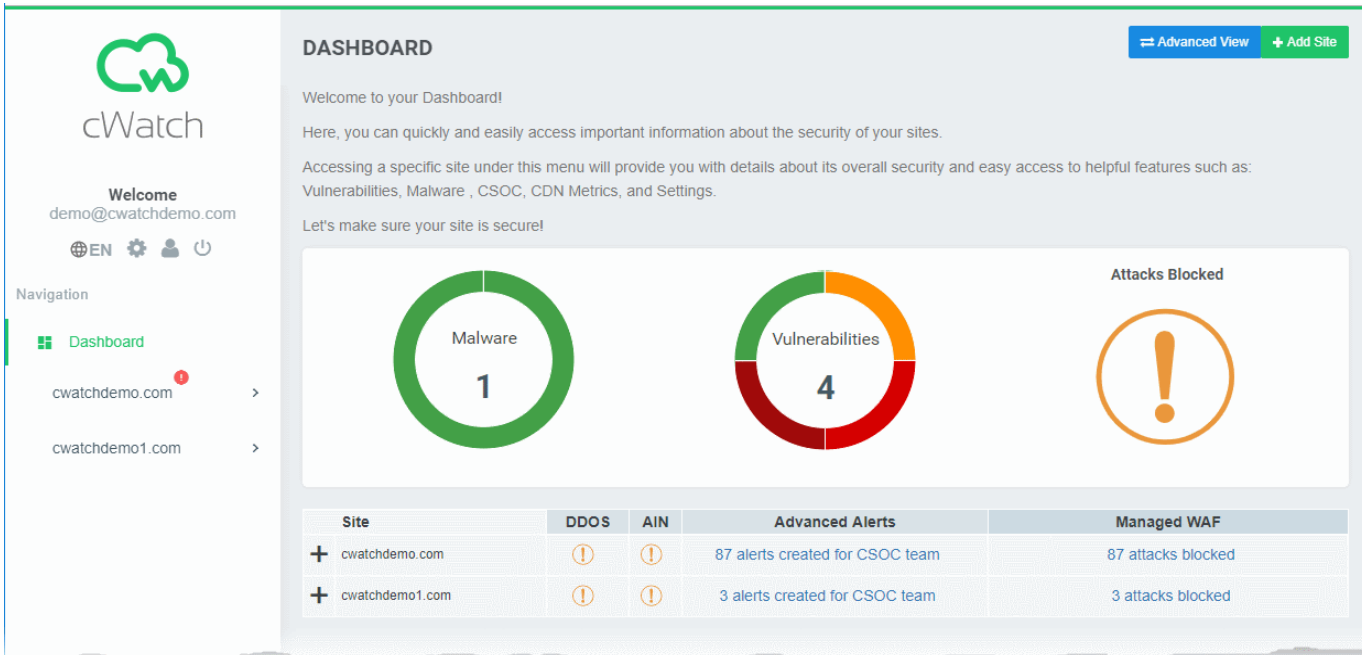
1 Introduction to Comodo cWatch Web Security.....	3
1.1 Purchase a License.....	4
1.2 License Types.....	19
1.3 Login to the Admin Console.....	19
1.4 Add Websites.....	22
2 The Main Interface.....	29
3 The Dashboard.....	31
4 Website Data and Settings.....	36
4.1 Website Overview.....	36
4.2 Comodo Vulnerability Scans .....	40
4.2.1 CMS Vulnerability Scans.....	41
4.2.2 OWASP Top 10 Vulnerability Scans.....	47
4.3 Malware Scans.....	54
4.4 Cyber Security Operation Center Results.....	64
4.4.1 WAF Statistics.....	65
4.4.2 WAF Events.....	69
4.5 Content Delivery Network Metrics.....	72
4.6 Configure Firewall Rules.....	78
4.7 Website Configuration.....	81
4.7.1 Configure Malware Scan Settings.....	83
4.7.1.1 Automatic configuration .....	83
4.7.1.2 Manual Configuration.....	85
4.7.2 Domain Configuration Instructions .....	86
4.7.3 SSL Configuration .....	91
4.7.4 Configure CDN Settings.....	99
4.7.5 Configure WAF Settings .....	103
4.7.6 Configure Trust Seal .....	106
5 The Settings Interface.....	108
6 Upgrade Licenses for Domains.....	117
7 Manage Your Profile.....	120
8 Get Support.....	123
About Comodo Security Solutions.....	126

# 1 Introduction to Comodo cWatch Web Security

cWatch Web Security is a security intelligence service which protects networks and web applications from a wide ranges of threats.

- cWatch runs regular malware scans on your domains and automatically removes any malware. The Content Delivery Network (CDN) service accelerates site performance by delivering your web content from the data center closest to your visitor.
- The service constantly logs events on your domains to identify new attack vectors. These logs allow the Comodo Cyber-Security Operations Center (CSOC) to dynamically create and apply firewall rules to combat the latest threats.
- The console dashboard instantly tells you about the health of your sites, including any attacks and security related incidents. You can have threat notifications sent to your email.
- The web application firewall provides military grade defense against hacker, SQL injections, bot traffic and more. You can also create your own custom firewall rules.
- You can run regular weekly scans for the top 10 OWASP threats and for known CMS vulnerabilities.

cWatch Web Security is available in three different service levels. More details are available in [License Types](#).



**DASHBOARD** Advanced View Add Site

Welcome to your Dashboard!

Here, you can quickly and easily access important information about the security of your sites.

Accessing a specific site under this menu will provide you with details about its overall security and easy access to helpful features such as: Vulnerabilities, Malware, CSOC, CDN Metrics, and Settings.

Let's make sure your site is secure!

Malware

1

Vulnerabilities

4

Attacks Blocked

!

Site	DDOS	AIN	Advanced Alerts	Managed WAF
+ cwatchdemo.com	!	!	87 alerts created for CSOC team	87 attacks blocked
+ cwatchdemo1.com	!	!	3 alerts created for CSOC team	3 attacks blocked

This guide explains how to purchase cWatch licenses, how to set up the service, and how to use the management console.

## Guide Structure:

- **Introduction to Comodo cWatch Web Security**
  - **Purchase a License**
  - **License Types**
  - **Log-in to the Administrative Console**
  - **Add Websites**

- **The Main Interface**
- **The Dashboard**
- **Website Data and Settings**
  - **Website Overview**
  - **Comodo Vulnerability Scans**
  - **Malware Scans**
  - **Cyber Security Operation Center Results**
  - **Content Delivery Network Metrics**
  - **Configure Firewall Rules**
  - **Website Configuration**
    - **Configure Malware Scan Settings**
    - **SSL Configuration**
    - **Configure CDN Settings**
    - **Configure WAF Settings**
    - **Configure Trust Seal**
- **The Settings Interface**
- **Upgrade Licenses for Domains**
- **Manage Your Profile**
- **Get Support**

## 1.1 Purchase a License

Three types of cWatch license are available:

- Basic
- Pro
- Premium

For more details on the services offered with each, see **License Types**.

- You can purchase licenses at <https://cwatch.comodo.com/plans.php>, or from the cWatch management console after logging in at <https://login.cwatch.comodo.com/login>.
- Licenses are charged per-website. Sub-domains are not covered if you buy a license for a primary domain like example.com. Each sub-domain must be purchased as a separate license.
- You can add multiple license types to your account if you wish to implement different protection levels on different websites.
- You can associate websites with licenses in the cWatch interface. See **Add Websites** for more details.

### Purchase a license

- Choose a license type at <https://cwatch.comodo.com/plans.php>. See **License Types** for more details about the features of each license.

## Best Website Security Solution

<p><b>Premium</b></p> <p>→ On Demand Analysts ←</p> <p><b>\$24.90</b> mo</p> <p>- Full Service -</p> <p><b>per domain</b></p> <p>—</p> <p>Scan every 4 hrs</p> <p>Expert security tuning</p> <p>Unlimited Malware Removal</p> <p>⌵</p> <p><b>DO IT ALL NOW</b></p>	<p><small>Most Popular</small></p> <p><b>Pro</b></p> <p>→ Complete Protection ←</p> <p><b>\$9.90</b> mo</p> <p>- Best Seller -</p> <p><b>per domain</b></p> <p>—</p> <p>Scan every 6 hrs</p> <p>Unlimited Malware Removal</p> <p>⌵</p> <p><b>PROTECT NOW</b></p>	<p><b>Basic</b></p> <p>→ +1x Malware Removal ←</p> <p><b>FREE</b></p> <p>- No credit card required -</p> <p><b>per domain</b></p> <p>—</p> <p>Scan Manually</p> <p>Upgrade anytime for protection</p> <p>⌵</p> <p><b>FREE TRIAL</b></p>
--	--	---

- Alternatively, visit <https://cwatch.comodo.com>, click 'Products' > 'Fix & Protect Now'

You will be taken to license configuration page:



**ADD SECURITY TO YOUR WEBSITE**

Website

DOMAIN.COM

**CONTINUE**

Own Multiple Domains?

**SHOP MULTIPLE LICENSES**

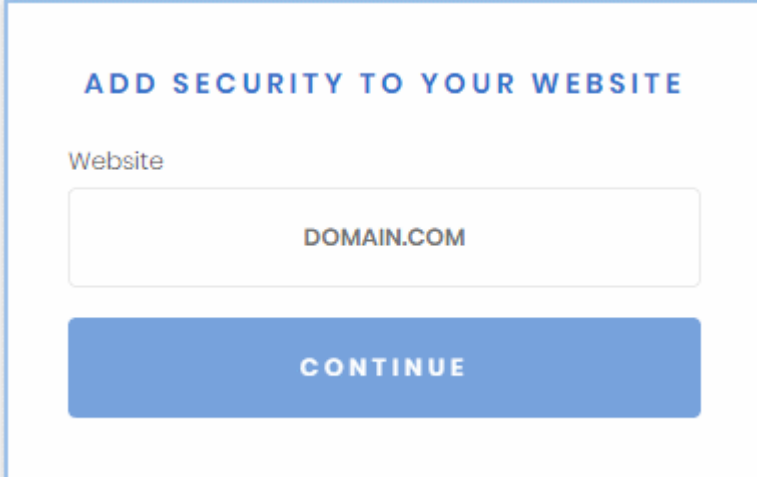
- Choose whether you want single domain license or multi-domain license.
  - Purchase single domain license** - Enter your domain name and click 'Continue' to purchase a

single domain license. See [Purchase single domain license](#) for more details.

- [Purchase multi-domain licenses](#) - Click 'Shop Multiple Licenses' to purchase licenses for multiple websites. See [Purchase multi-domain licenses](#) for more details.

### Purchase single domain license

#### Step 1 - Enter your domain name



**ADD SECURITY TO YOUR WEBSITE**

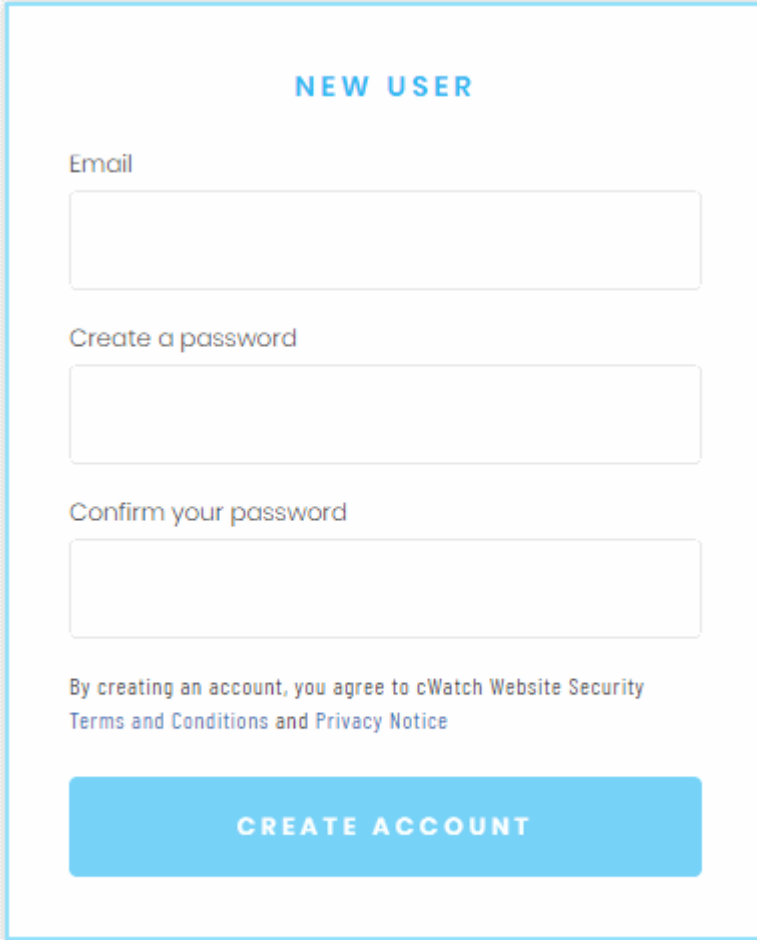
Website

DOMAIN.COM

**CONTINUE**

- Type your website (without 'www.') in the Website field and click continue

#### Step 2 - Enter your Comodo account Information



**NEW USER**

Email

Create a password

Confirm your password

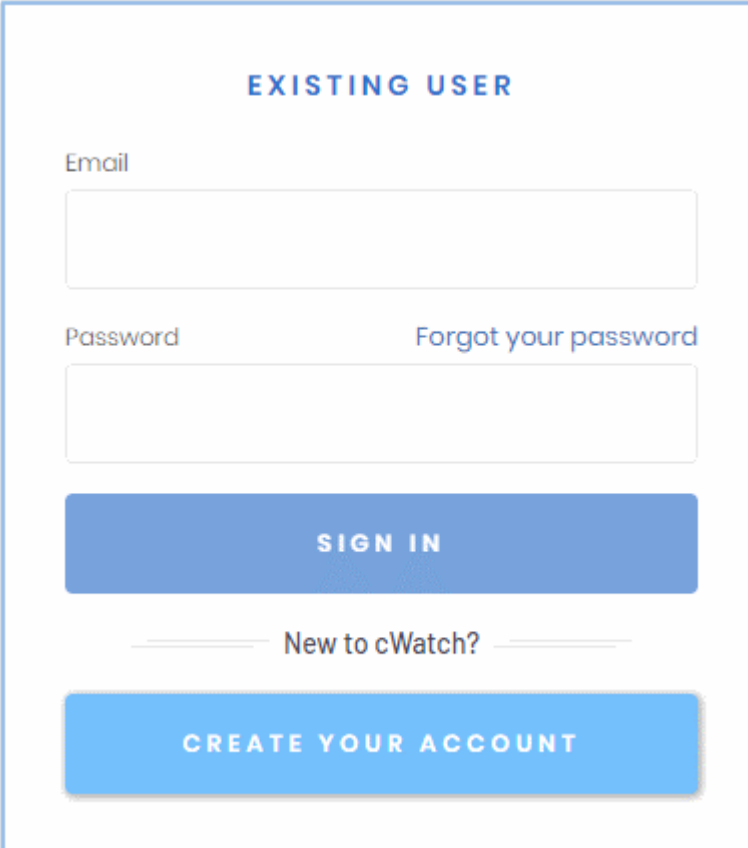
By creating an account, you agree to [cWatch Website Security Terms and Conditions](#) and [Privacy Notice](#)

**CREATE ACCOUNT**

Already have an account? [Sign in](#)

- If you don't have a Comodo account, enter your email address and a password to create a new account

- If you already have a Comodo account, click 'Sign in'



The screenshot shows a login form titled "EXISTING USER". It contains two input fields: "Email" and "Password". To the right of the "Password" field is a link that says "Forgot your password". Below the input fields is a dark blue button labeled "SIGN IN". Underneath the button is the text "New to cWatch?" with horizontal lines on either side. At the bottom of the form is a light blue button labeled "CREATE YOUR ACCOUNT".

- Enter your username and password and click 'Sign-in'

### Step 3 - Select License Type



	Basic	Pro	Premium
	Free account	Free 30 days	
Malware detection and removal	1x	✓	✓
Security information and event mgmt.	✗	✓	✓
24/7 Cybersecurity ops analysts	✗	✗	✓
Managed web application firewall	✗	✓	✓
Content delivery network	✗	✓	✓
24/7 Live technical support	✗	✓	✓
30 day free trial available	✗	✓	✓
No Credit Card Req.		\$9.90 - per month -	\$24.90 - per month -

## Confirm Website Security License

Every website has its own unique domain name which requires its own unique security license. We can begin repairing your website and add real-time detection to prevent future cyberattacks based website's security license.

### Review your order

1 Pro License  
Subtotal: \$9.9 per month

### Total

**\$9.9** monthly recurring payment

Cancel before MM/DD/YYYY as we offer our customers 30 day money back guarantee.

**PROCEED TO CHECKOUT**



- Select the license type for the domain. See **License Types** for more details about the features of each license.
- Click 'Proceed to Checkout'

## Step 4 - Enter Payment Details



**PAYMENT PROFILE**

Cardholder Name

Card Number

Expiration

Security Code

Currency

**BILLING INFO**

Address

Country

State

City

Postal Code

## Pay Annually to Immediately Save \$ 18.90 Now

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

### Annually Monthly

#### Review your order

1 Pro License

#### Subtotal

**\$ 9.9** end of year cost with monthly recurring payments

#### Savings

**\$ 0** discount with annual one time payment

#### Total

**\$ 9.9** month recurring payment

Cancel before MM/DD/YYYY as we offer our customers 30 day money back guarantee.

**SUBMIT PAYMENT**





- Payment Profile - Enter your card details for recurring payments for auto-renewal of license.
- Billing Info - Enter your billing address
- Choose the period of license. The available options are 'Annually' or 'Monthly'.
- Click 'Submit Payment'

## Step 5 - Activate License



- Click 'Activate cWatch' to start protecting your website

## Your Payment Successfully Processed Online.

Your order summary for purchasing cWatch Website Security licenses monthly recurring basis are listed below.

### Review your order

1 Pro License

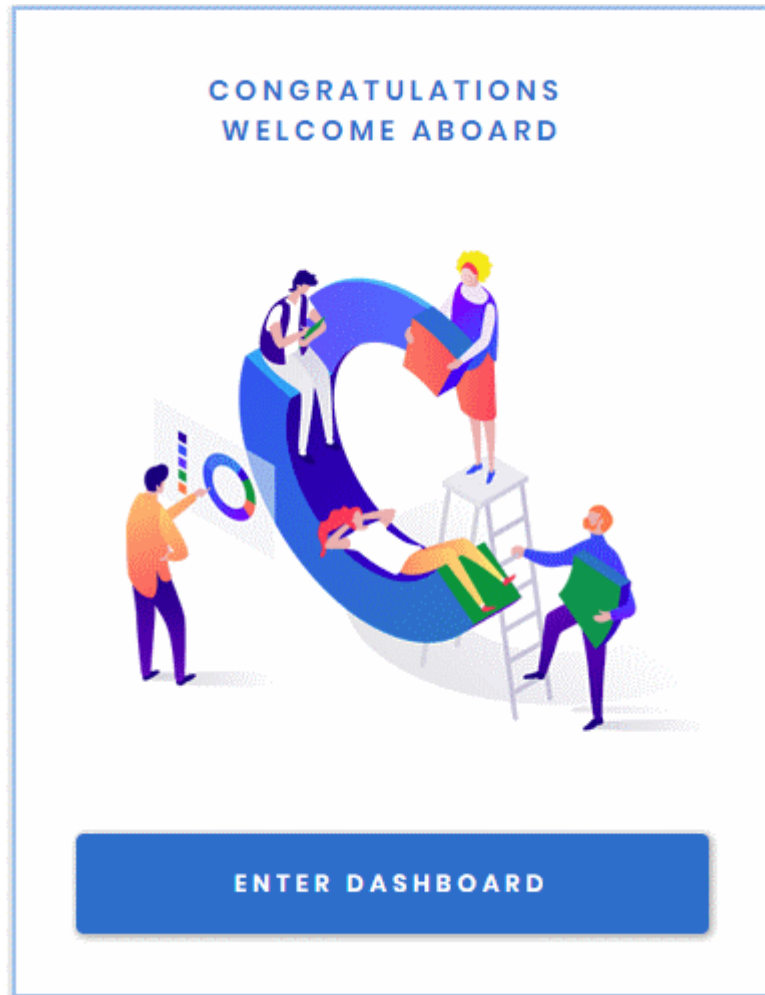
### Total

**\$ 9.9** monthly recurring payment

*Cancel before MM/DD/YYYY as we offer our customers 30 day money back guarantee.*

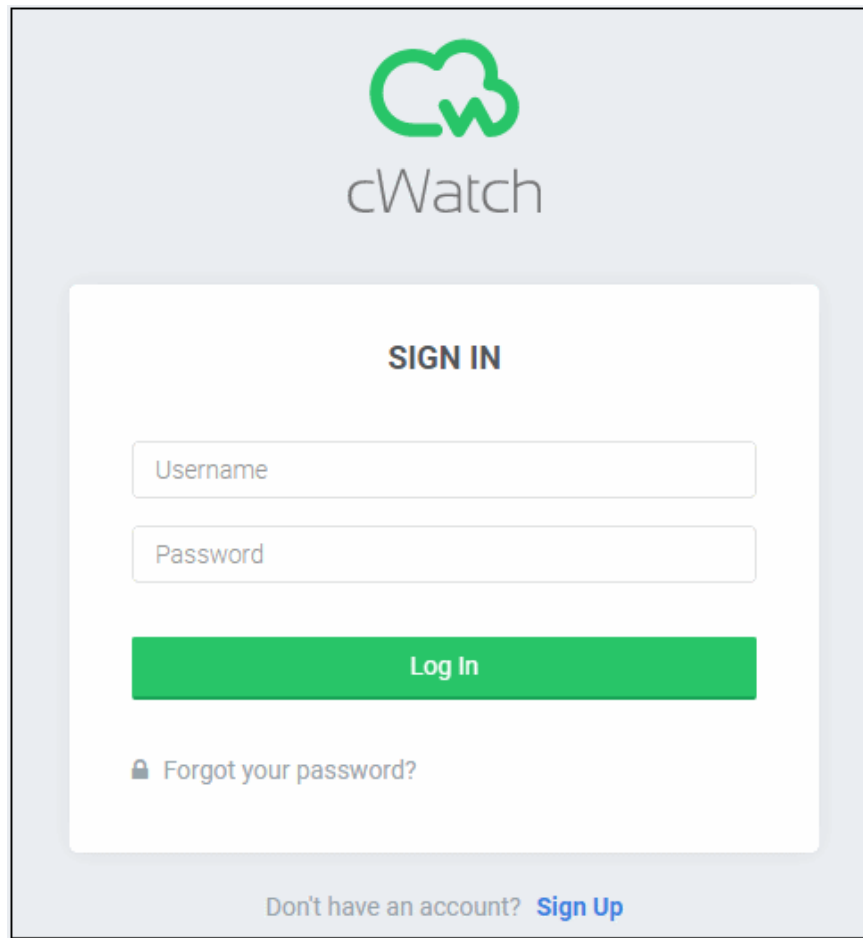
[Download your invoice »](#)






Your license is now activated.

- Click 'Enter Dashboard' to login to cWatch




  
cWatch

**SIGN IN**

Username

Password

**Log In**

 [Forgot your password?](#)

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

- Use your Comodo account username and password to login to cWatch.
- You have to read and accept to the 'Terms and Conditions' on your first login.

## TERMS AND CONDITIONS

**CWATCH WEB SECURITY END USER LICENSE AND  
SUBSCRIBER AGREEMENT****THIS AGREEMENT CONTAINS A BINDING ARBITRATION  
CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY  
BEFORE ACCEPTING THE TERMS AND CONDITIONS.**

IMPORTANT—PLEASE READ THESE TERMS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING THE SERVICES. BY USING, APPLYING FOR, OR ACCEPTING THE ACCOUNT OR SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT CLICK "I ACCEPT" AND DO NOT APPLY FOR, ACCEPT, OR USE THE SERVICES.

This End User License and Subscriber Agreement (this "Agreement") constitutes the final binding agreement between the company that you represent ("Subscriber") and either:

Comodo Security Solutions, Inc., with its principal place of business at 1255 Broad Street, Suite 100, Clifton, New Jersey 07013, United States, or

If you are located in the European Economic Area, Comodo Security Solutions, Ltd., which has its principal place of business at Third Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford Manchester M5 3EQ, United Kingdom, is the entity responsible for any data or information that is processed or controlled and associated with this product and services.

- Click the 'Add Site' button at top-right to get started
- See [Add Websites](#) for more help with adding and configuring websites.

**Purchase multi-domain license****Step 1 - Select Licenses**



BEST SELLER

## PRO

WEBSITE SECURITY LICENSES

QTY:

1

\$99.90 PER MONTH

Unlimited Malware Removal  
6 Hr Auto Site Scanning

## PREMIUM

WEBSITE SECURITY LICENSES

QTY:

1

\$249.00 PER MONTH

Unlimited Malware Removal  
4 Hr Auto Site Scanning  
Expert Security Tuning

### Shop Website Security Licenses

Every website has its own unique domain name which requires its own unique security license. We can begin repairing your website and add real-time detection to prevent future cyberattacks based website's security license.

Review your order

1 Pro License

\$99.90 per license  
\$99.90 per year

1 Premium License

\$249.00 per license  
\$249.00 per year

Total

**\$348.90** annually recurring payment

*Cancel before MM/DD/YYYY as we offer our customers 30 day money back guarantee.*

PROCEED TO CHECKOUT



- Enter the number of licenses you want in 'Pro' and/or 'Premium' types.
- One license covers one website or a sub domain
- Click 'Proceed to Checkout'

### Step 2 - Enter your Comodo account Information

### EXISTING USER

Email

Password Forgot your password

SIGN IN

————— New to cWatch? —————

CREATE YOUR ACCOUNT

- If you already have a Comodo account, enter your username and password and click 'Sign-in'
- If you don't have a Comodo account, Click 'Create Your Account' enter your email address and a password to create a new account

### NEW USER

Email

Create a password

Confirm your password

By creating an account, you agree to [cWatch Website Security Terms and Conditions](#) and [Privacy Notice](#)

**CREATE ACCOUNT**

Already have an account? [Sign in](#)

### Step 3 - Enter Payment Details



**PAYMENT PROFILE**

Cardholder Name

Card Number

Expiration

Security Code

Currency

**BILLING INFO**

Address

Country

State

City

Postal Code

### Pay Annually to Immediately Save \$68.70

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

#### Annually Monthly

Review your order

**1 Pro Licenses**  
Subtotal: \$99.90 per year  
Total: \$99.90 one time payment

**1 Premium Licenses**  
Subtotal: \$249.00 per year  
Total: \$249.00 one time payment

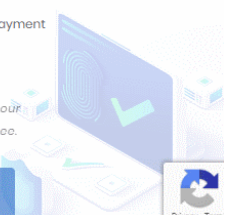
**Subtotal**  
**\$348.90** per year

**Savings**  
\$68.70 discount with annual one time payment

**Total**  
**\$348.90** year recurring payment

*Cancel before MM/DD/YYYY as we offer our customers 30 day money back guarantee.*

**SUBMIT PAYMENT**



- Payment Profile - Enter your card details for recurring payments for auto-renewal of licenses.
- Billing Info - Enter your billing address
- Choose the period of license. The available options are 'Annually' or 'Monthly'.
- Click 'Submit Payment'

## Step 4 - Activate License



- Click 'Activate cWatch' to start protecting your website

## Your Payment Successfully Processed Online.

Your order summary for purchasing cWatch Website Security licenses monthly recurring basis are listed below.

### Review your order

#### 1 Pro Licenses

Subtotal: \$99.90 per year  
Total: \$99.90 one time payment

#### 1 Premium Licenses

Subtotal: \$249.00 per year  
Total: \$249.00 one time payment

### Subtotal

**\$348.90** per year

### Savings

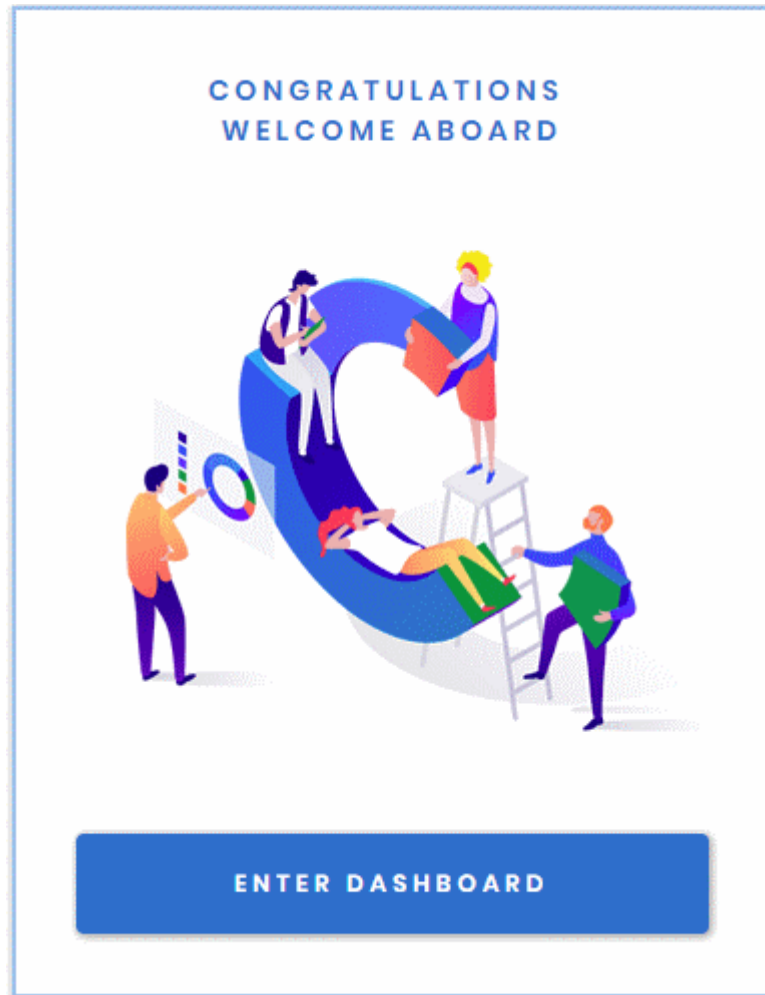
\$68.70 discount with annual one time payment

### Total

**\$348.90** year recurring payment

[Download you invoice »](#)

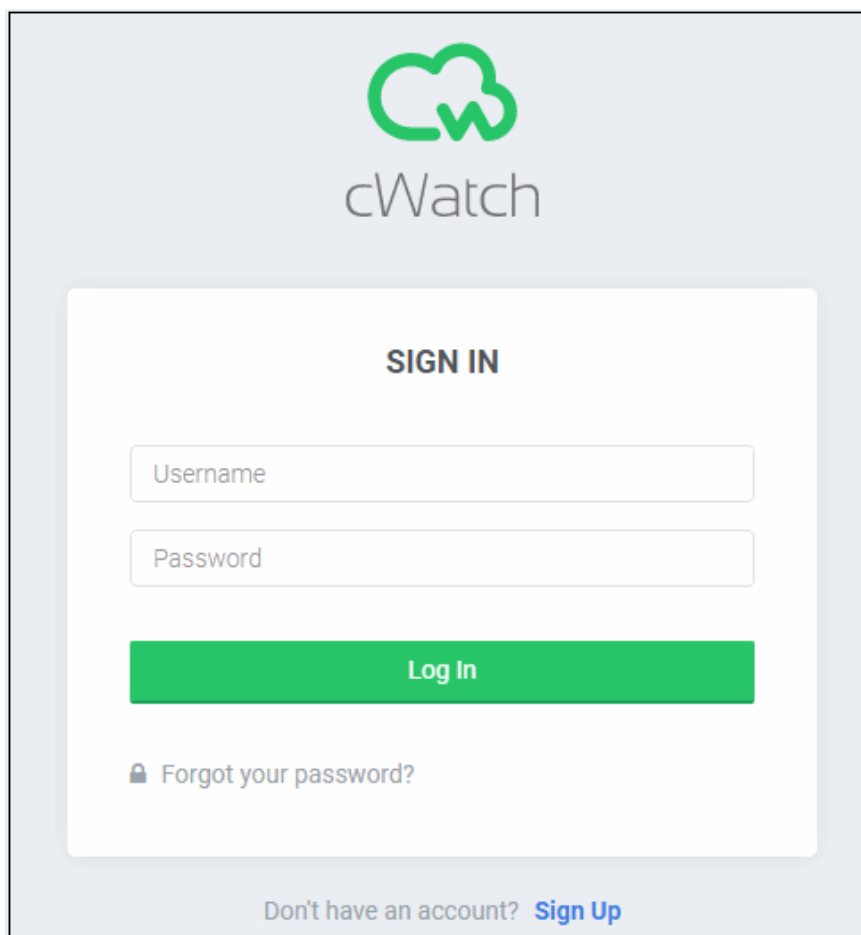





Your license is now activated.

- Click 'Enter Dashboard' to login to cWatch






  
cWatch

**SIGN IN**

Username

Password

**Log In**

 [Forgot your password?](#)

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

- Use your Comodo account username and password to login to cWatch.
- You have to read and accept to the 'Terms and Conditions' on your first login.

## TERMS AND CONDITIONS

**CWATCH WEB SECURITY END USER LICENSE AND  
SUBSCRIBER AGREEMENT****THIS AGREEMENT CONTAINS A BINDING ARBITRATION  
CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY  
BEFORE ACCEPTING THE TERMS AND CONDITIONS.**

IMPORTANT—PLEASE READ THESE TERMS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING THE SERVICES. BY USING, APPLYING FOR, OR ACCEPTING THE ACCOUNT OR SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT CLICK "I ACCEPT" AND DO NOT APPLY FOR, ACCEPT, OR USE THE SERVICES.

This End User License and Subscriber Agreement (this "Agreement") constitutes the final binding agreement between the company that you represent ("Subscriber") and either:

Comodo Security Solutions, Inc., with its principal place of business at 1255 Broad Street, Suite 100, Clifton, New Jersey 07013, United States, or

If you are located in the European Economic Area, Comodo Security Solutions, Ltd., which has its principal place of business at Third Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford Manchester M5 3EQ, United Kingdom, is the entity responsible for any data or information that is processed or controlled and associated with this product and services.

- Click the 'Add Site' button at top-right to get started
- See [Add Websites](#) for more help with adding and configuring websites.

## 1.2 License Types

cWatch offers different levels of monitoring, protection and content-delivery service depending on the type of license.

The three license types are:

- Basic
- Pro
- Premium

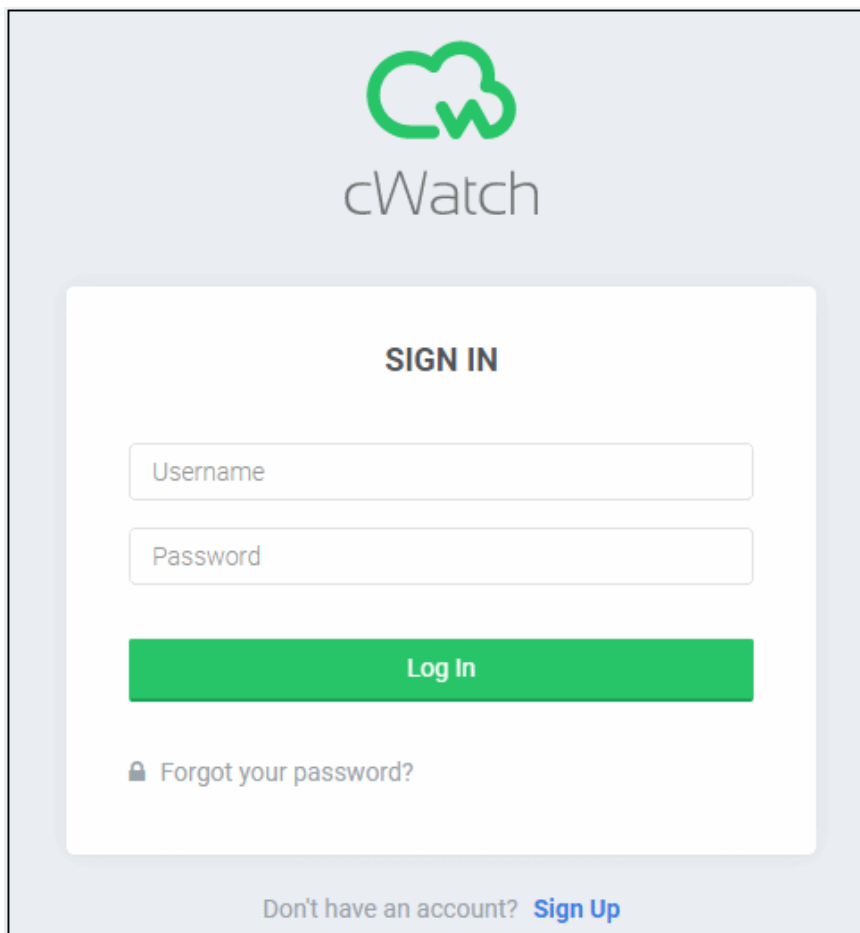
For help to associate websites with licenses, see [Add Websites](#).


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

Feature/Service	Premium	Pro	Basic
<b>Malware Detection and Removal</b>			
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
<b>Security Information and Event Management (SIEM)</b>			
	✓	✓	✗
<b>24/7 Cyber-Security Operations Center (CSOC)</b>			
	✓	✓	✗
Dedicated analyst	✓	✓	✗
<b>Web Application Firewall (WAF)</b>			
Custom WAF rules	✓	✗	✗
Bot Protection	✓	✓	✗
Scraping Protection	✓	✓	✗
<b>Content Delivery Network (CDN)</b>			
Layer 7 DDoS Protection	✓	✓	✓
Layer 3, 4, 5 & 6 DDoS Protection	✓	✓	✓
Trust Seal	✓	✓	✓

## 1.3 Login to the Admin Console

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




  
cWatch

**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 for security.
  - Click 'Forgot your password?' to reset your password.
  - Enter your mail address and click 'Submit' on confirmation screen:

  
cWatch

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

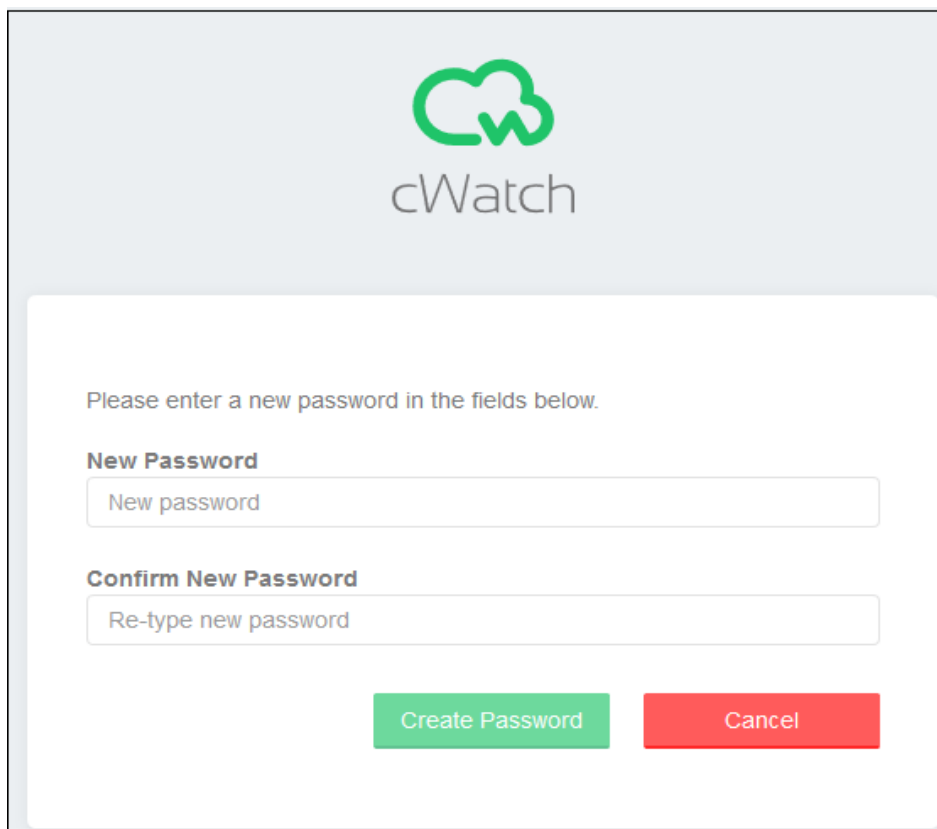
I'm not a robot
 
  
reCAPTCHA  
Privacy - Terms

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

- You will receive a password reset mail:

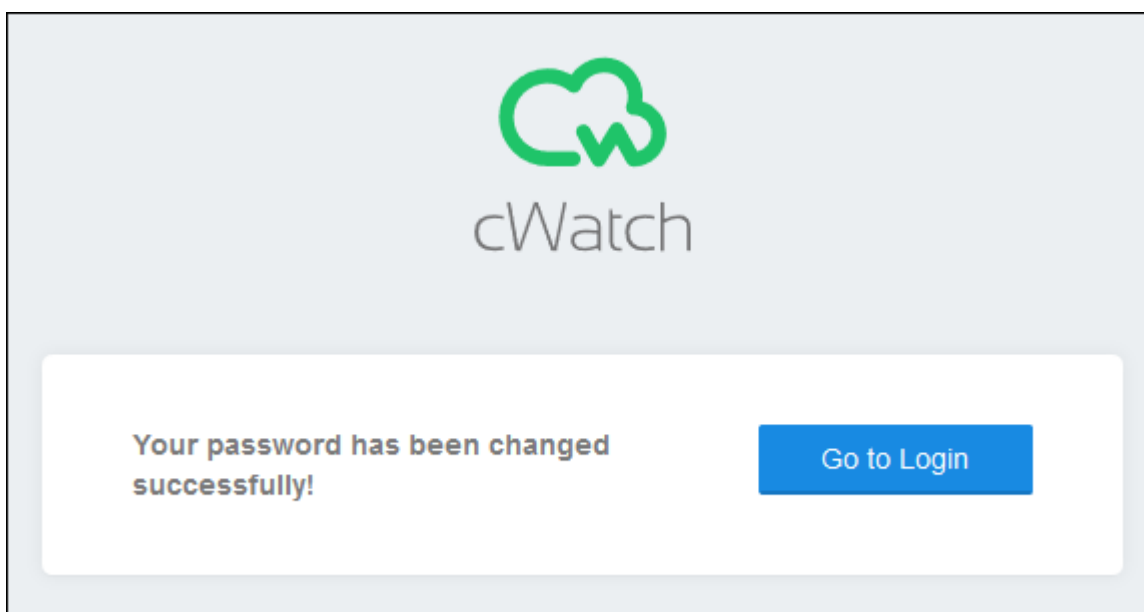


- Click 'Reset Password'. You are taken to the cWatch password reset page.
- Enter and confirm your new password:



The screenshot shows the cWatch password reset interface. At the top, there is a green logo consisting of a cloud with a 'w' inside, and the text 'cWatch' below it. Below the logo, a white box contains the text 'Please enter a new password in the fields below.' There are two input fields: the first is labeled 'New Password' and contains the placeholder text 'New password'; the second 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 'Create Password'



The screenshot shows the cWatch password change success message. At the top, there is a green logo consisting of a cloud with a 'w' inside, and the text 'cWatch' below it. Below the logo, a white box contains the text 'Your password has been changed successfully!' and a blue 'Go to Login' button.

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

## 1.4 Add Websites

- You need to add websites to cWatch to enable protection and to take advantage of the content delivery network (CDN).
- The number of sites you can add depends on your license. See [Purchase a License](#) for details about

license types.

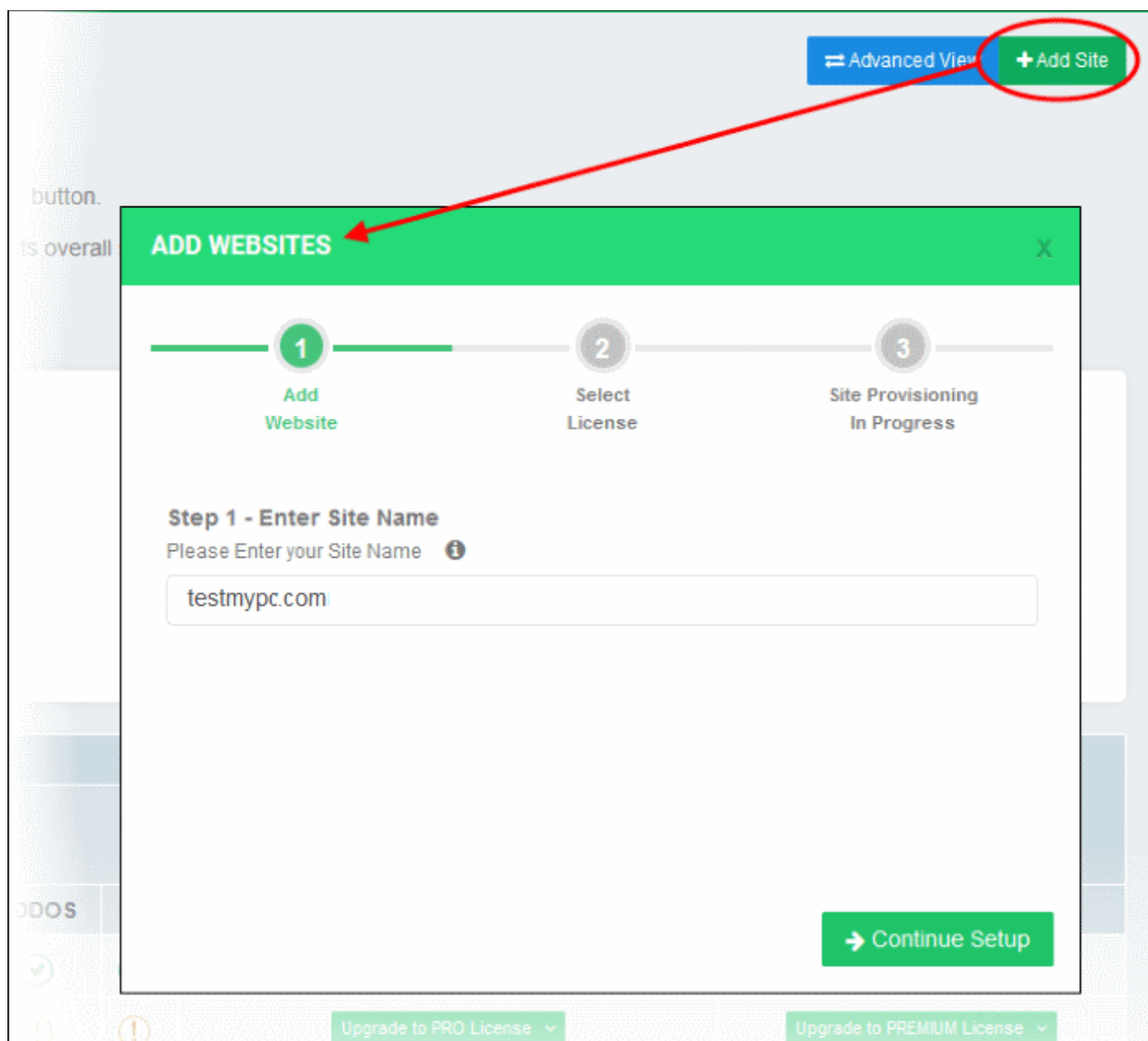
- Once added, you can configure threat monitoring and CDN settings for each site. See **Website Configuration** for more details.

### Add a new domain

- Login to cWatch at <https://login.cwatch.comodo.com/login> with your username and password.

The dashboard will appear by default

- Click 'Add Site' at top-right to start the 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 name of the website you want to register. Do not include 'www' at the start.
- Click 'Continue Setup' to move to the next step.

## ADD WEBSITES X

1  
Add Website

2  
Select License

3  
Site Provisioning In Progress

### Step 1 - Enter Site Name

Please Enter your Site Name i

→ Continue Setup

### Step 2 - Select License

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

- cWatch features vary according to license type. See [License Types](#) for more details. Alternatively, click 'Learn more' in the 'Select License' screen.
- The drop-down menu lets you select from all licenses you have purchased.
- Choose the type of license you wish to associate with the domain you entered in step 1
- Click 'Finish' to proceed
- See [Purchase a License](#) if you need help to buy more licenses



## 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 stage is for cWatch to provision your site:

## 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](#)











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

Your site is registered successfully X


- The next step is to configure cWatch protection on the site.
- Click 'Get Started' to open the cWatch 'Settings' page
- Click the 'here' in the site row to setup protection (highlighted in red box):

**SETTINGS**



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

- See **Website Configuration** for help to configure malware scans, CDN, firewall rules and more.




**Welcome**  
cwatchweb@gmail.com

Navigation

- Dashboard
- cwvtest.pp.ua
- one.bh1-cwatch.o...
- nurd.ga
- nurd.gq
- wp.fowlercwatch...
- cwatchweb.ml
- cwatch.pp.ua
- removetest.qacw...
- testmypc.com
- Alert
- Overview
- Vulnerabilities

**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:  Port:

Username:

Password:

Site Directory:

[Enable Scanner](#)

**Important Note:**

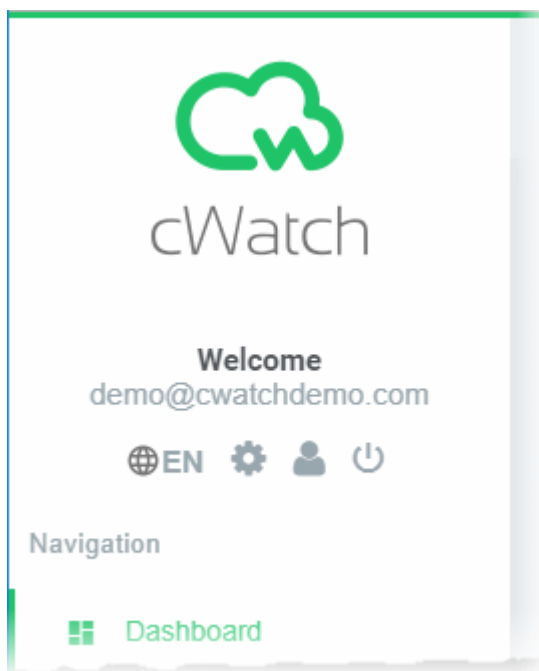
- cWatch generates a CNAME DNS record for the website you just enrolled
- You need to add this record to the DNS entry for your domain to route your site traffic through the CDN.
- To view the CNAME details:
  - Click the website name in the main menu on the left
  - Click '**Settings**' > '**Domain**'
- Your web host may be able to help you add the CNAME. Guidance is also available at <https://support.google.com/a/topic/1615038?hl=en>.


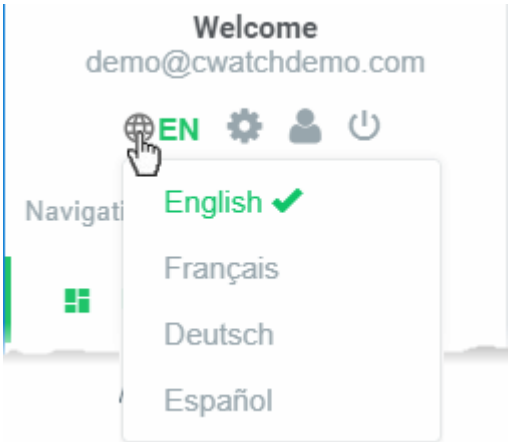



**Tip:** You can skip this step for now and can add the CNAME entry to the DNS records later. See **Domain Configuration Instructions** for more details.

- Repeat the process to add more websites.

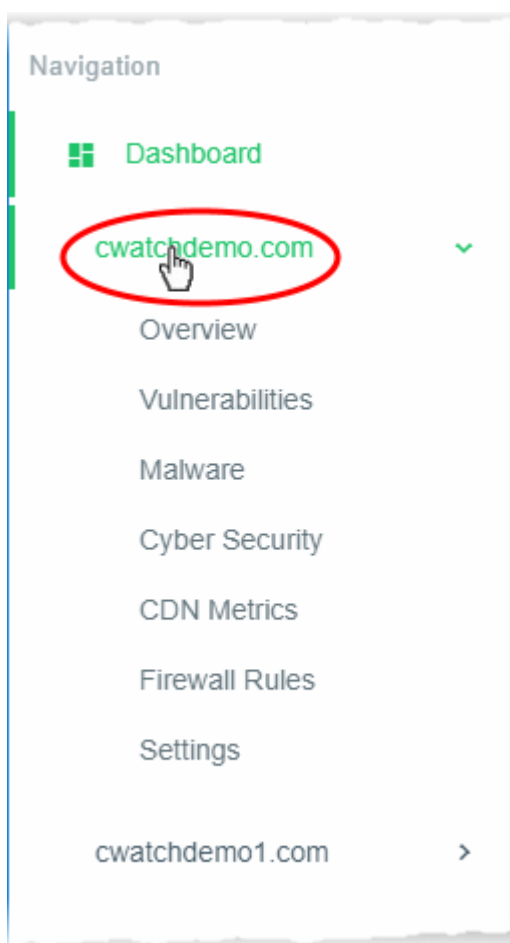
## 2 The Main Interface

- The cWatch dashboard contains an at-a-glance summary of the security of your monitored websites.
- Links to all major areas of the interface are on the left. The main display shows data for the selected item.
- Language selection, settings, profile options and logout are underneath your username:



 EN	<p>Shows the current interface language.</p> <ul style="list-style-type: none"> <li>• Click the globe icon to view and change interface language (Default = English)</li> </ul> 
	<p>Lists all domains which you have added to cWatch.</p> <ul style="list-style-type: none"> <li>• Manage Settings - configure malware scans, FTP, CDN and more. See <b>The Settings Interface</b> for more details.</li> <li>• Manage DNS - Add DNS records in order to route traffic through the content delivery network. See <b>Manage DNS Settings</b> for more details.</li> </ul>
	<p>Your profile. Change your contact details, alert settings and password. See <b>Manage Your Profile</b> for more details.</p>
	<p>Logout of cWatch.</p>

The left-hand menu contains a link to the dashboard and shows all domains added to your account. Click a domain name to reveal domain options:



- **Dashboard** - Overall statistics on all domains that are protected and managed.
- Click a domain name to open the following menu items:
  - **Overview** - Summary of security status and CDN performance. See **Website Overview** for more details.
  - **Vulnerabilities**
    - OWASP top-ten threats - Scan your site for OWASP vulnerabilities. You can also enable or disable automatic weekly scans.
    - CMS vulnerability scans - Identify weaknesses in your content management system (CMS). 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.
    - See **Comodo Vulnerability Scans** for more details.
  - **Malware** - 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 **Malware Scans** for more details.
  - **COSC** - Real-time analysis of attack patterns on your website from the Comodo Security Operations Center. See **Cyber Security Operation Center Results** for more details.
  - **CDN Metrics** - Data about your content delivery network traffic. This includes total usage, data throughput and the locations from which your traffic originated. See **Content Delivery Network Metrics** to find out more.
  - **Firewall Rules** - Create your own custom Firewall rule. See **Configure Firewall Rules** for more information.
  - **Settings** - View and configure cWatch protection settings for your website. See **Website Configuration** to learn more.

### Help and Support:

The footer contains copyright information, terms and conditions and support links.

2019 © Comodo Group, Inc. 2019. All rights reserved. All trademarks displayed on this web site are the exclusive property of the respective holders.

Terms and  
Conditions

Help

Online - Chat With Us

- Click the 'Terms and Conditions' link to view the cWatch EULA.
- Click 'Help' to view the cWatch guide at <https://help.comodo.com/topic-285-1-848-11000-Introduction-to-Comodo-cWatch-Web-Security.html>.
- Click the 'Chat with us' button for instant support from technicians at Comodo. See **Get Support** for more details.

## 3 The Dashboard

The dashboard shows a top-level summary of the security of all protected websites on your account. This allows you to quickly identify issues and effectively track the risks associated with your sites. Further details on each domain are listed underneath the main graphics.

- Click 'Dashboard' on the left to open the dashboard.
- Click 'Simple View' or 'Advanced View' at top-right to change the level of detail shown.

**DASHBOARD** Advanced View + Add Site

Welcome to your Dashboard!

Here, you can quickly and easily access important information about the security of your sites.

Accessing a specific site under this menu will provide you with details about its overall security and easy access to helpful features such as: Vulnerabilities, Malware, CSOC, CDN Metrics, and Settings.

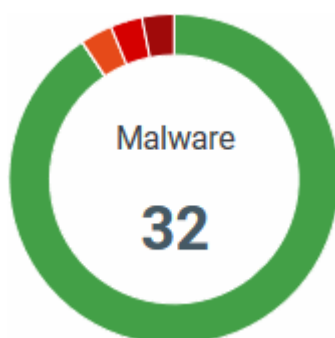
Let's make sure your site is secure!

**Malware**  
1

**Vulnerabilities**  
4

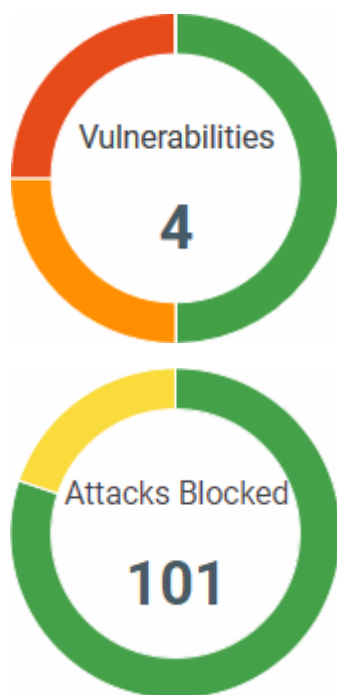
**Attacks Blocked**

Site	DDOS	AIN	Advanced Alerts	Managed WAF
+ cwatchdemo.com	!	!	87 alerts created for CSOC team	87 attacks blocked
+ cwatchdemo1.com	!	!	3 alerts created for CSOC team	3 attacks blocked



**Malware** - The total number of active malware found on all your sites.

- Place your mouse over a sector to view the malware found on a site as a percentage of overall.
- Click a sector to view the 'Malware Scans' page for that website.
  - The scans page also lets you request manual threat removal by technicians at Comodo
- See **Malware Scans** for more info.



**Vulnerabilities** - The total number of active vulnerabilities on all your sites.

- Place your mouse over a sector to view the vulnerabilities found on a site as a percentage of overall.
- Click a sector to open the 'Vulnerabilities' page for that website.
  - The vulnerabilities page provides detailed information on the detected threats and help to fix them. You can also request manual threat removal by specialists at Comodo.
- See [Comodo Vulnerability Scan Results](#) for more details.

**Attacks Blocked** - The number of attacks prevented by the Web Application Firewall (WAF) on all your sites.

- Green check-mark - No attacks detected so far
- Yellow exclamation mark - WAF is not enabled for your sites. To enable, select a site on the left, then click 'Settings' > 'WAF'
- Place your mouse over a sector to view the quantity of attacks blocked on a particular domain as a percentage of overall attacks.
- Click on a sector to view the attack details page for that website. See [Cyber Security Operation Center Results](#) for more info.

There are two ways to view the dashboard:

- [Simple View](#)
- [Advanced View](#)

### Simple View

View general info above every domain, including license type, license expiry date, and most recent scans.



Site	License Type	Expiration Date	Last Vulnerability Scan	Last Malware Scan
+ 0300tv.com	BASIC	29 December 2018 05:30	02 February 2018 13:13	-
admin.yetanothersite.us	ENTERPRISE TRIAL - yetanothersite.us	Expired <a href="#">Put A License Into Use</a>	-	-
ali.com	PREMIUM	Expired <a href="#">Put A License Into Use</a>	-	-
+ comodo.com	PREMIUM	09 June 2020 05:30	-	-
+ comodo1.com	PRO	11 April 2018 05:30	-	-
+ comodo8.com	PREMIUM	12 April 2018 05:30	-	-
+ cuzdan.com	BASIC	29 December 2018 05:30	-	-
+ despacito.com	ENTERPRISE - despacito.com	10 October 2020 05:30	-	-
+ dragon.comodo.com	BASIC	29 December 2018 05:30	-	-
ftp.0300tv.com	PREMIUM	Expired <a href="#">Put A License Into Use</a>	-	-
+ grey.com	PRO	11 April 2018 05:30	-	-
+ hola.com	BASIC	29 December 2018 05:30	17 January 2018 17:35	-
+ hurriyet.com	BASIC	06 November 2019 05:30	-	-
+ kali.com	BASIC	21 March 2118 05:30	-	-
+ kul.com	PRO	11 April 2018 05:30	-	-
+ kula.com	PRO	11 April 2018 05:30	-	-
mail.yetanothersite.us	PREMIUM	Expired <a href="#">Put A License Into Use</a>	-	-
+ one.comodo.com	PRO	11 April 2018 05:30	16 January 2018 13:26	-
phptravels.net	PREMIUM TRIAL	Expired <a href="#">Put A License Into Use</a>	-	-
+ rni.com	BASIC	21 March 2118 05:30	-	-

Dashboard - Simple View	
Column Header	Description
Site	Name of the website. <ul style="list-style-type: none"> <li>Click the '+' icon beside a site name to view a summary of the site's security status. Security features are arranged by license type. See '<a href="#">View Security Status of a Website</a>' for more details</li> </ul>
License Type	The type of license on the domain. See <a href="#">License Types</a> for more details on the features of each license.
Expiration Date	The last day of license validity. The expiry date is not shown for licenses with auto-renewal enabled.
Last Vulnerability Scan	Date and time of the most recent vulnerability scan on the site. <ul style="list-style-type: none"> <li>You can set up regular weekly scans to find the top 10 Open Web Application Security Project (OWASP) vulnerabilities</li> <li>You can also run scans for specific vulnerabilities in your WordPress websites, or run on-demand scans as required.</li> </ul>

	<ul style="list-style-type: none"> <li>Scan results are shown in the 'Vulnerabilities' page for the site (click the domain name on the left and select 'Vulnerabilities' from the menu).</li> </ul> <p>See <b>Comodo Vulnerability Scan Results</b> for more details.</p>
Last Malware Scan	<p>Date and time of the most recent virus scan on the site.</p> <ul style="list-style-type: none"> <li>cWatch scans all files on websites enabled for malware scanning.</li> <li>You can set a schedule for these scans and can also run on-demand scans when required.</li> <li>The results of the scans are displayed in the 'Malware' page. See <b>Malware Scans</b> for more details.</li> </ul>

## View Security Status of a Website

- Click the '+' icon beside a website name to open its security status details pane.

Each tile shows the security status of features covered by the various license types. The number of tiles you see depends on the website's active license type.

License Type	Tiles Displayed
Basic	Basic
Pro	Basic and Pro
Premium	Basic, Pro and Premium

## Advanced View

'Advanced View' shows different levels of statistics based on your license type. The higher the license type you have, the more security components you will see.

For example:

- 'Basic' license - Shows details about security components covered by the basic license type.
- 'Pro' license - Shows details about components covered by both basic and pro licenses.
- 'Premium' license - Shows details about components covered by basic, pro and premium licenses.

Site	DDOS	AIN	Advanced Alerts	Managed WAF
+ cwatchdemo.com	✓	✓	Upgrade to PRO License	Upgrade to PREMIUM License
+ cwatchdemo1.com	!	!	!	!
+ cwatchdemo2.com	!	!	!	!
+ cwatchdemo3.com	!	!	!	!

Similar to the 'Simple' view, you can view more information on each site by clicking the plus symbol beside the domain name.

Site	DDOS	AIN	Advanced Alerts	Managed WAF
+ cwatchdemo.com	✓	✓	Upgrade to PRO License	Upgrade to PREMIUM License
▼ cwatchdemo1.com	!	!	!	!

License Type: **PREMIUM**

Last Malware Scan Date: --

Last Vulnerability Scan Date: --

**BASIC**

- Reputation !
- Vulnerabilities !
- Malware !
- CDN !
- DDOS !
- AIN !

**PRO**

- Advanced Alerts !

**PREMIUM**

- Managed WAF !

+ cwatchdemo2.com	!	!	!	!
-------------------	---	---	---	---

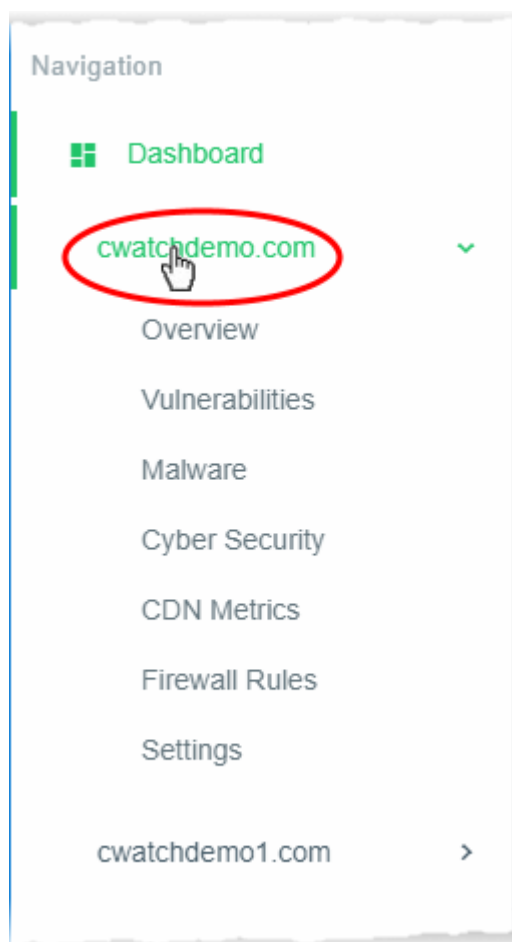
## Add Site

Allows you to add a new domain to your website. See [Add Websites](#) for more details.

## 4 Website Data and Settings

- cWatch displays panoramic data about all events on your website.
- These include attacks monitored and blocked, the results of malware and vulnerability scans, and incidents which were logged because they triggered a correlation rule.

Click a website on the left to open the following options:



**Overview** - Summary of security status and CDN performance. See [Website Overview](#) for more details.

- Vulnerabilities
  - **OWASP top-ten threats** - Scan your site for OWASP vulnerabilities. You can also enable or disable automatic weekly scans.
  - **CMS vulnerability scans** - Identify weaknesses in your content management system (CMS).

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.

See [Comodo Vulnerability Scans](#) for more.

**Malware** - 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 [Malware Scans](#) for more details.

**COSC** - Real-time analysis of attack patterns on your website from the Comodo Security Operations Center. See [Cyber Security Operation Center Results](#) for more details.

**CDN Metrics** - Data about your content delivery network traffic. This includes total usage, data throughput and the locations from which your traffic originated. See [Content Delivery Network Metrics](#) to find out more.

**Firewall Rules** - Create your own custom Firewall rule. See [Configure Firewall Rules](#) for more information.

**Settings** - View and configure cWatch protection settings for your website. See [Website Configuration](#) to learn more.

### 4.1 Website Overview

- Select a website on the left and choose 'Overview'
- The overview page shows a summary of security, traffic and visitor activity on your sites.
- Each tile on the page shows important information from a specific cWatch module.

- The tiles also contain shortcuts to view more detailed results and execute remedial actions if appropriate.

## Open the overview page

- Select a website on the left
- Click 'Overview' from the menu items

- Tiles are broken down into the following categories:
  - **Cyber Security Operation Center**
  - **Malware Scan**
  - **Vulnerabilities**
  - **Content Delivery Network**




## Cyber Security Operation Center

- Shows key information from cWatch security modules. Click a tile to see more detailed results.
- The number of tiles you see depends on your cWatch license.

- **Web Application Firewall** - Number of incidents detected by the firewall, and the number of attacks prevented. You can configure these items in your web application firewall rules.
- **Malware Analysis & Removal** - Results of the most recent manual or scheduled antivirus scan.





- **Reputation** - The trustworthiness of the site according to key security indicators.
  - Comodo Valkyrie - Comodo Valkyrie is a threat analysis platform that provides verdicts on the trust level of websites. A check-mark indicates that your site is not blacklisted by Valkyrie.
  - Google Safe Browsing and Phishtank - These are long-established blacklists of dangerous websites. A check-mark indicates that your site is not on their blacklist.
  - SSL issues - The TLS certificate on the site is misconfigured, invalid, or uses out-dated protocols.
- **Virtual Patching** - The result of the most recent vulnerability scan.
  - The tile shows the number of currently active OWASP vulnerabilities. These need to be mitigated.
  - Click the link at the bottom of the tile to view the vulnerabilities.
    - Then click on a vulnerability category to view all files affected by that attack type.
    - The file list page also has instructions to help you fix the vulnerability.
    - See **OWASP Top 10 Vulnerability Scans** for more help with this interface.
  - You can also create web application firewall rules to address the issues.
    - See **Configure Firewall Rules** for help to create custom WAF rules.

The icons at the bottom of the tiles show the threat level in that category. Click the verdict to open the corresponding module and view more detailed results.



-  - The website is safe. No actions need be taken at this point.
  - Click the icon to view a history of actions by the module
-  - The website is at risk.
  - Click the icon to open the corresponding module page. You can start a scan or submit a request for Comodo to remove the malware. See '**Malware Scans**' for more information.
-  - The security component has not been configured or the website has not yet been scanned.
  - Click the icon to configure the component or initiate a scan.


## Malware Scan

- Shows the numbers of malicious items found during the last scan on the site. Categories include:
  - 'Trojware & Backdoor'
  - 'Potentially Unwanted Application'
  - 'Defacement & Exploit'
  - 'Others'.

MALWARE SCAN			
TROJWARE & BACKDOOR	POTENTIALLY UNWANTED APPLICATION	DEFACEMENT & EXPLOIT	OTHERS
Last Scan <b>21 November 2018</b>	Last Scan <b>21 November 2018</b>	Last Scan <b>21 November 2018</b>	Last Scan <b>21 November 2018</b>
Malware Found <b>7</b>	Malware Found <b>0</b>	Malware Found <b>0</b>	Malware Found <b>0</b>
Has malware 	No malware found 	No malware found 	No malware found 

Click the verdict at the bottom of a tile to view more information.





-  - No malware detected. No actions need be taken at this point.
-  - Malware found on the site.

-  - The site has not yet been scanned.




See '[Malware Scans](#)' for additional help with this.

### Vulnerabilities

- cWatch scans your sites for the top 10 OWASP threats and for WordPress vulnerabilities. These tiles show the results of the most recent scan.
- The number of threats found in each category is shown in a separate tile.
  - Note - cWatch automatically blocks any OWASP threats it finds.

VULNERABILITIES			
<b>INJECTION</b> Last Scan <b>21 September 2018</b> Threat Count <b>0</b> No vulnerability found 	<b>XSS</b> Last Scan <b>21 September 2018</b> Threat Count <b>0</b> No vulnerability found 	<b>WEAK AUTHENTICATION</b> Last Scan <b>21 September 2018</b> Threat Count <b>0</b> No vulnerability found 	<b>SECURITY MISCONFIGURATION</b> Last Scan <b>21 September 2018</b> Threat Count <b>3</b> Has vulnerability 


Click the verdict at the bottom of a tile to view more information. See '[Comodo Vulnerability Scans](#)' for additional information.

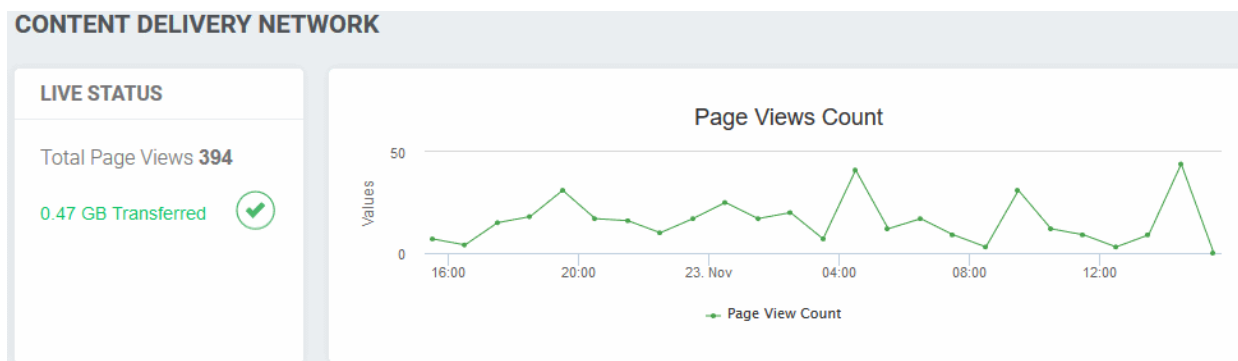
-  - The scan found no vulnerabilities. No actions need to be taken at this point.
-  - The site has vulnerabilities.
-  - The site has not yet been scanned.

### Content Delivery Network

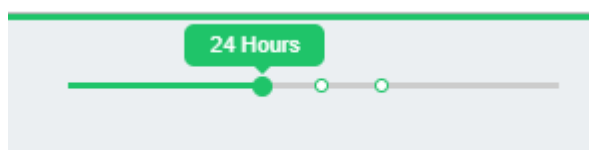
- Shows live data about your CDN usage and the number of times your pages were viewed.

**Note:** The CDN statistics are shown only for websites configured to use the CDN service.

- You need to add a CNAME to your site's DNS record to use the CDN. This record is auto-generated by cWatch.
- Click 'Settings' > 'CDN Settings' to view the CNAME record for your site. See [Configure CDN Settings](#) for more details
- If you haven't configured the CNAME then no data is shown here. Click the yellow information icon  to start the configuration process.
- See [Content Delivery Network Metrics](#) for more details about CDN statistics.



- Use the slider at top-right to change the time-period of the statistics:



#### Live Status:

- Shows the total number of times your pages were viewed by visitors, and the total amount of traffic used. Use the time period slider to see traffic and views for a specific date range.

## 4.2 Comodo Vulnerability Scans

- Click on a website in the left-hand menu and select 'Vulnerabilities'

CWatch can perform two types of vulnerability scan:

- Content management system (CMS) vulnerabilities
- OWASP Top Ten threats

### CMS Vulnerabilities

- A scan that searches for vulnerabilities in your content management system (CMS).
- The following CMS types are supported:
  - WordPress
  - Joomla
  - Drupal
  - ModX
  - Typo3
- Scanned items include core site, current CMS version, plugins, themes and more.
- The 'CMS Scan' pane shows results from the last scan and lets you:
  - Run on-demand scans your website
  - Schedule a weekly scan
- You can view details about each vulnerability and read guidance on how to fix them.
- You can also view reports from last ten CMS vulnerability scans.

### OWASP Top Ten Threats

cWatch periodically scans your sites for the top-ten vulnerabilities published by the Open Web Application Security Project (OWASP). It automatically blocks any of these threats that it discovers.



- The 'OWASP Top 10 Scan' pane shows results from the last scan and lets you:
  - Run on-demand scans your website
  - Schedule a weekly scan
- The scan results show the number of threats in each OWASP category that were blocked by cWatch. You can view descriptions on each vulnerability category
- You can also view scan reports for the last ten scans.

**Background.** OWASP is an online community that audits critical domain security issues and publishes the ten most widespread vulnerability categories. These categories help admins protect websites against the most serious security flaws. cWatch checks whether your registered domains are vulnerable to the tests in the OWASP top ten and allows you to take remedial actions on those that fail.

See the sections below if you need more help with each type of scan:

- **CMS Vulnerability Scans**
- **OWASP Top 10 Vulnerability Scans**

### 4.2.1 CMS Vulnerability Scans

- Click on a website in the left-hand menu and select 'Vulnerabilities'
- The content management system (CMS) scanner inspects your core site, plugins and themes to identify vulnerabilities in your current version.
- It also provides help to update your CMS and resolve any vulnerabilities. The scanner supports the following types of CMS:
  - WordPress
  - Joomla
  - Drupal
  - ModX
  - Typo3

You can run CMS scans on-demand and/or schedule weekly scans on your website. You can also view the results from the last ten scans.

#### Run CMS scans and view results

- Click on a registered domain on the left
- Choose 'Vulnerabilities' from the sub-menu:

The screenshot displays the 'Vulnerabilities - cwatchdemo.com' dashboard. On the left, the navigation menu includes 'Dashboard', 'cwatchdemo.com', 'Overview', 'Vulnerabilities', 'Malware', 'Cyber Security', 'CDN Metrics', and 'Firewall Rules'. The main area features a 'CMS Scan' section with a 'Daily Scan Allowed:10' indicator and a 'Start Scan' button. A 'LAST SCAN' summary box on the right provides details for the most recent scan: 'WordPress' CMS, scan date '05-10-2018 - 22:41 pm', version '1.2', and status 'Vulnerable'. It also includes a 'View Full Report' link and an 'Enable Weekly Scan' toggle.

The 'Last Scan' area on the right shows the results of the most recent scan, including the type of CMS scanned.

- **Scan Date** - Date and time at which the last scan was run.
- **Version** - The version of CMS that was scanned. This is the CMS version that your site runs on.
- **Status** - Whether the website has vulnerabilities or not.
  - Not Vulnerable - No weaknesses detected.
  - Vulnerable - Security threats found. Click on the row to view more details and fix advice.
  - Failed - Scan did not run for some reason.
  - 'CMS not found' - Shown if the site doesn't use a supported CMS, or because cWatch couldn't detect the CMS type for other reasons.
- Click the 'Refresh' icon on the top-right to reload the results of the latest scan.

The pane lets you:

- **Run an on-demand scan**
- **Configure Scheduled Scans**
- **View detailed results of the last scan**
- **View the results of previous scans**

### Start an on-demand CMS scan

You can manually start a CMS scan at anytime:

- Click on website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Click 'Start Scan' in the 'CMS Scan' pane:

**CMS Scan** ⓘ **Daily Scan Allowed:10**

Content Management System Scan is an online security scanner to detect CMS vulnerabilities. We keep your CMS core site, plugins and themes up-to-date as soon as the scan is completed. We provide you information about what vulnerabilities are in the current version of your site. Our solutions aim to protect you against attackers who might want you penetrate your website.

Click 'Start Scan' to start the CMS Scan. After this first scan, your CMS Scan will be scheduled on a weekly basis so you always know if your site is safe.

View Scan History ⓘ

**Start Scan**

Successfully started cms scan. ✕

- cWatch will begin scanning the domain for CMS vulnerabilities.
- Scan results are shown in the 'Last Scan' box on the right
  - Click the 'Refresh' icon at top-right to reload the results of the scan
- Alerts will be generated if any vulnerabilities are found.
- Click 'View Full Report' for a comprehensive overview of discovered vulnerabilities.
- See **View detailed results of the last scan** for more details.

### Schedule a scan

You can enable an automatic, weekly CMS scan on any of your websites


- Click on registered website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Enable the weekly scan as shown in the screenshot below:


**Daily Scan Allowed:10**

Management System Scan is an online security scanner to search for CMS vulnerabilities. We keep your CMS core site, plugins and themes healthy as soon as possible. We provide you information about what is vulnerable in the code of your site. Our solutions aim to protect you against hackers or malware that might want you penetrate your website.

Click on the 'Scan' button to start the CMS Scan. After this first scan, your CMS website can be scanned on a weekly basis so you always know if your site is safe and secure.

**can**


**LAST SCAN** 

  
**WORDPRESS**

Scan Date 28-10-2018 - 01:33 am

Version 4.9.8

Status **Not Vulnerable**

View Full Report 

Enable Weekly Scan

- Weekly scans will start the next day and will run at the same day/time every week after that.
- For example, if you enable the weekly scan at 6:00 PM on Friday, the scans will run every Saturday at 6:00 PM.

#### View detailed results of the last scan

- Click on registered website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Click 'View Full Report' under 'Last Scan':

**Daily Scan Allowed:10**

Content Management System Scan is an online security scanner to search for CMS vulnerabilities. It helps you keep your CMS core site, plugins and themes healthy as soon as they are updated. We provide you information about what is vulnerable in the components of your site. Our solutions aim to protect you against hackers or malware that want you penetrate your website.

Click on the Scan button to start the CMS Scan. After this first scan, your CMS website can be scanned on a weekly basis so you always know if your site is safe and secure.

**LAST SCAN**

**WORDPRESS**

Scan Date 10-01-2019 - 19:54 pm

Version --

Status **Vulnerable**

[View Full Report >](#)

Enable Weekly Scan

**CMS Scan History**

**January 10 2019** **January 09 2019**

**Translations for the vulnerabilities are not available.**

**CORE** PLUGIN THEME

+ **WORDPRESS** WordPress Scan Date: 10-01-2019 19:54 pm | Version: 5.0.2 | Status: **Vulnerable**

Vulnerability information is available for the following CMS components:

- Core
- Plugins
- Theme
- Select a tab to view a list of vulnerabilities in the component.
- Click the '+' icon at the left of an item to view its details:


← CMS Scan History ⓘ Translations for the vulnerabilities are not available.

January  
10  
 2019
 

 January  
09  
 2019

CORE
PLUGIN
THEME

---



WordPress

WordPress


Scan Date: 10-01-2019 19:54 pm

Version: 5.0.2

Status: Vulnerable

---

CORE
PLUGIN
THEME



WordPress

WordPress

Scan Date: 10-01-2019 19:54 pm

Version: 5.0.2

Status: Vulnerable

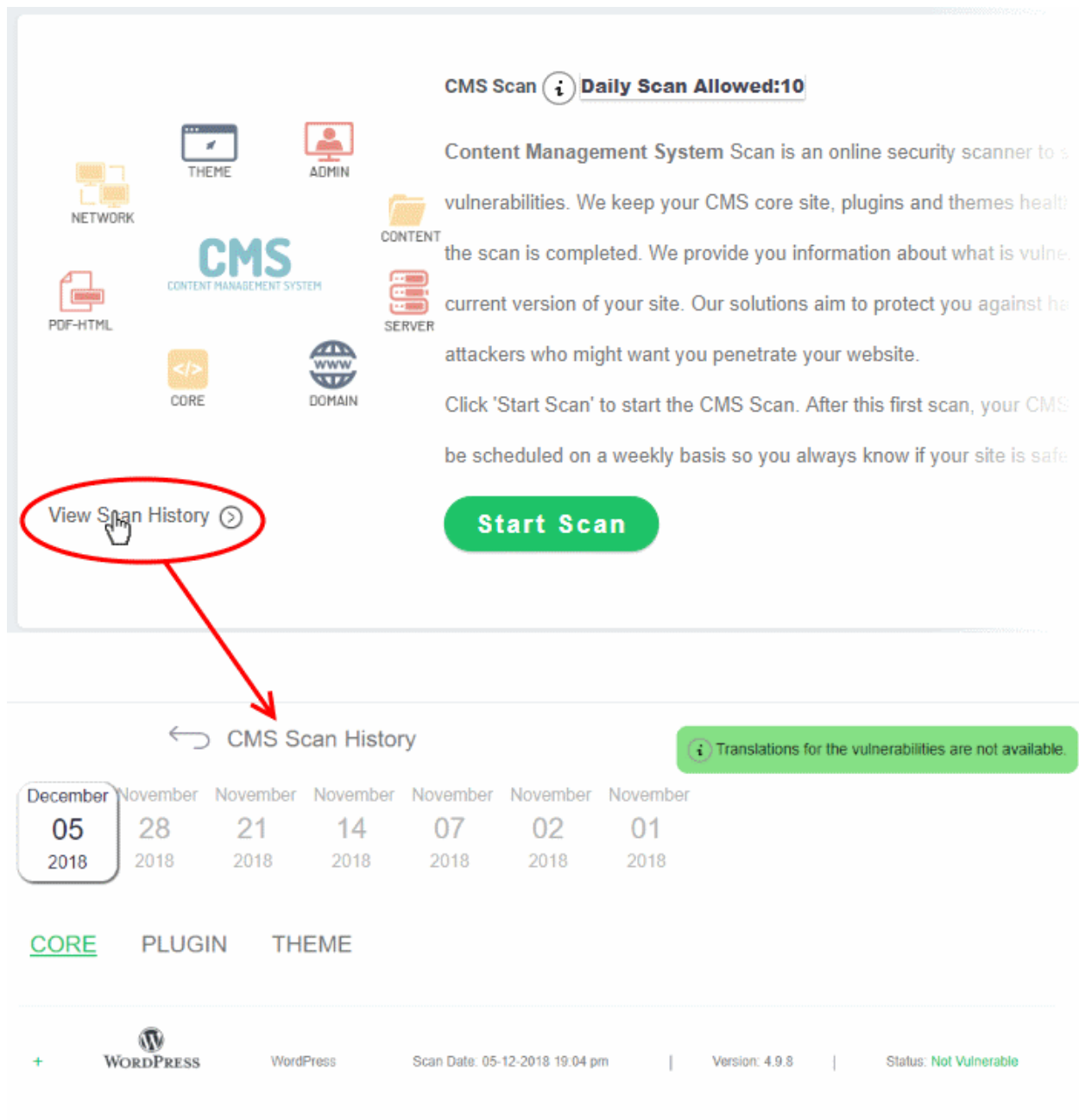
	PATCH		FOUND IN	LATEST VERSION
VULNERABILITY	FIX ↕	REFERENCE ↕	↕	↕
XSS vulnerability in WordPress before 5.0.1	--	<a href="https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/">https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/</a>	5.0 <a href="#">See More</a>	--
XSS vulnerability in WordPress before 5.0.1	--	<a href="https://github.com/WordPress/WordPress/commit/246a70bdfac3bd45ff71c7941deef1bb206b19a">https://github.com/WordPress/WordPress/commit/246a70bdfac3bd45ff71c7941deef1bb206b19a</a> <a href="#">See More</a>	5.0 <a href="#">See More</a>	--
UNSPECIFIED vulnerability in	--	<a href="https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/">https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/</a>	5.0 <a href="#">See More</a>	--

CMS Vulnerabilities - Column Descriptions	
Column Header	Description
Vulnerability	A short description of the weakness
Patch Fix	The version of the CMS in which the vulnerability was fixed. Update your CMS to this version to remove the vulnerability from your site.
Reference	Links to detailed information about the vulnerability and guidance to fix the issue. <ul style="list-style-type: none"> <li>Click 'See More' to view a list of reference pages</li> </ul>
Found in	The version of the CMS in which the vulnerability was discovered. <ul style="list-style-type: none"> <li>Click 'See More' to view a list of versions in which the vulnerability is found</li> </ul>
Latest Version	The most recent version of the CMS available. We advise customers to upgrade to the latest version if possible.

### View results of previous scans

You can view the results of the 10 most recent CMS scans on your site.

- Click on registered website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Click 'View Scan History' in the 'CMS Scan' pane



The dates of the previous scans are shown at the top of the history window.

- Select a date to view detailed results from the scan run on that day
- See **View detailed results of the last scan** if you need more help with this.

## 4.2.2 OWASP Top 10 Vulnerability Scans

- Click on a website in the left-hand menu and select 'Vulnerabilities'
- cWatch scans your sites for the top-ten vulnerabilities published by the Open Web Application Security Project (OWASP).

- The results identify any weaknesses found on your site along with guidance to fix them.
- You can run OWASP scans on-demand and/or schedule weekly scans. You can also view the results of the last ten scans.

### Run OWASP top 10 vulnerability scans and view results

- Click on a registered domain on the left
- Choose 'Vulnerabilities' from the sub-menu:

The 'OWASP Top 10' pane contains the results of the last scan and lets you run or schedule a new scan.:

The screenshot displays the 'VULNERABILITIES - CWATCHDEMO.COM' page. On the left, the navigation menu shows 'cwatchdemo.com' and 'Vulnerabilities' highlighted. The main content area features a 'Start Scan' button and a 'View Scan History' link. The 'Last Scan' summary box on the right provides the following details:

Last Scan	
Scan Date	02-05-2018 - 14:24 pm
Information	0
Score	8 out of 10
High	0
Med	8
Low	1
View Full Report	<a href="#">View Full Report</a>
Enable Weekly Scan	<input type="checkbox"/>

The 'Last Scan' area on the right shows the results of the most recent scan.

- Scan Date - Date and time at which the last scan was run.
- Score - The number of OWASP top-10 categories passed by your site.
- High, Medium, Low and Information - Number of vulnerabilities found at each risk level.
- Click the 'Refresh' icon at top-right to re-load results if you have just completed a more-recent scan.

The pane lets you:

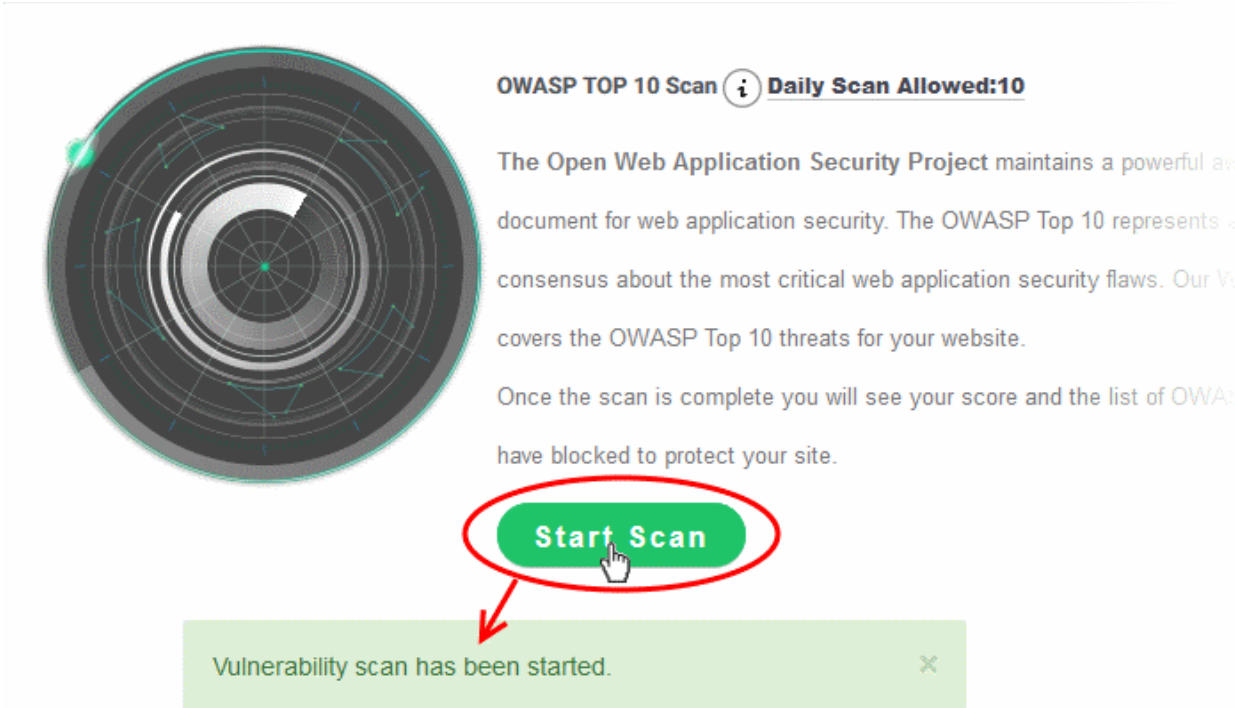
- **Run an on-demand scan**
- **Configure Scheduled Scans**
- **View detailed results of the last scan**
- **View the results of previous scans**

### Start an on-demand OWASP top 10 vulnerability scan

You can manually start a CMS scan at anytime:

- Click on website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Click 'Start Scan' in the 'OWASP Top 10 Scan' pane:





**OWASP TOP 10 Scan ⓘ Daily Scan Allowed:10**

The Open Web Application Security Project maintains a powerful advisory document for web application security. The OWASP Top 10 represents a consensus about the most critical web application security flaws. Our Vulnerability Scan covers the OWASP Top 10 threats for your website.

Once the scan is complete you will see your score and the list of OWASP vulnerabilities that have been blocked to protect your site.

**Start Scan**

Vulnerability scan has been started. ×

- cWatch will begin scanning the domain for OWASP top 10 vulnerabilities.
- Scan results are shown in the 'Last Scan' box on the right
- Click the 'Refresh' icon at top-right to reload the results of the scan
- Alerts will be generated if any vulnerabilities are found.
- Click 'View Full Report' for a comprehensive overview of discovered vulnerabilities.
- See **View detailed results of the last scan** for more details.

### Schedule a scan

You can enable an automatic, weekly CMS scan on any of your websites

- Click on registered website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Use the switch in the OWASP pane to enable the scan, as shown in the screenshot below:

10 Scan ⓘ **Daily Scan Allowed:10**

Web Application Security Project maintains a powerful awareness of web application security. The OWASP Top 10 represents a broad list of the most critical web application security flaws. Our Web Security scans for OWASP Top 10 threats for your website.

When the scan is complete you will see your score and the list of OWASP threats we found to protect your site.

**Scan**

**Last Scan** ↻

**OWASP**  
Open Web Application Security Project

Scan Date 23-03-2018 - 21:43 pm

Information 0

Score 9 out of 10

High 0 | Med 16 | Low 1

View Full Report ⌵

Enable Weekly Scan

- Weekly scans will start the next day and will run at the same day/time every week after that.
- For example, if you enable the weekly scan at 6:00 PM on Friday, the scans will run every Saturday at 6:00 PM.

**View detailed results of the last scan**

- Click on registered website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Click 'View Full Report' under 'Last Scan' in the 'OWASP Top 10' Scan pane

10 Scan ⓘ **Daily Scan Allowed:10**

Web Application Security Project maintains a powerful awareness of web application security. The OWASP Top 10 represents a broad list of the most critical web application security flaws. Our Web Security scans for OWASP Top 10 threats for your website.

When the scan is complete you will see your score and the list of OWASP threats we found to protect your site.

**Scan**

**Last Scan** ↻

**OWASP**  
Open Web Application Security Project

Scan Date 10-01-2019 - 19:55 pm

Information 0

Score 9 out of 10

High 0 | Med 2 | Low 1

View Full Report ⌵

Enable Weekly Scan

The results page shows the number of threats in each OWASP attack category.



**SAFE**

Scan Date: 10-01-2019 - 19:55 pm

High 0 | Med 2 | Low 1

Score: 9 out of 10

RANK	VULNERABILITES	DESCRIPTION
A1	0	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2	0	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3	0	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4	0	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5	0	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6	3	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7	0	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8	0	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9	0	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10	0	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

OWASP Top 10 Vulnerabilities - Column Descriptions	
Column Header	Description
Rank	Order of the attack category as per OWASP top ten vulnerabilities list.
Vulnerabilities	Number of threats identified in that attack category. <ul style="list-style-type: none"> <li>Click the number to view the complete details of the threat, list of files affected and guidance to fix the issue</li> <li>See View Details of Identified Vulnerabilities information for more details</li> </ul>
Description	A short description of the vulnerability.

## View Details of Identified Vulnerabilities

The OWASP Scan Results page contains detailed information about each vulnerability, and has guidance to help

you fix them.

**Tip:** You can also submit a request for Comodo specialists to manually remove the threats. Manual removal is only available for domains with a premium license.

### View detailed vulnerability information

- Click on registered website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Click 'View Full Report' under 'Last Scan' in the 'OWASP Top 10' Scan pane

The numbers of vulnerabilities identified in each of the top ten OWASP vulnerability categories is shown as a list.

- Click the number in a category in which vulnerabilities were found

The screenshot shows a list of vulnerabilities. The first entry is A6, with a red circle around the number '3' and a red arrow pointing down to a detailed dialog box. The dialog box is titled 'A6 VULNERABILITY DETAIL' and contains two entries: 'Unhandled error in web application' with a count of 2, and 'Code disclosure vulnerability' with a count of 1. A red 'Close' button is visible in the bottom right corner of the dialog.

Vulnerability Category	Description	Count
A6	Many web applications do not properly protect sensitive data, such as credit cards, tax authentication credentials. Attackers may steal or modify such weakly protected data to credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection: encryption at rest or in transit, as well as special precautions when exchanged with the	3
A7	Most web applications verify function level access rights before making that functional	1

A6 VULNERABILITY DETAIL	
Unhandled error in web application	2
Code disclosure vulnerability	1

The detail dialog lists which specific threat types were found within that category.

- Click a threat type to view affected files. The results also show guidance to remediate the threat:

**A6 VULNERABILITY DETAIL** ×

**Unhandled error in web application** 2

**Vulnerabilities:** ↓

- Medium** http://www.cwatchdemo.com/cw-login.php
- Medium** http://www.cwatchdemo.com/cw-admin/js/cw-fullscreen.js

**Fix Guidance:**

- \* Ensure that the application source handles exceptions and errors in a such a way that no sensitive information is disclosed to the users
- \* Configure the application server to handle and log any exceptions that the application might yield

**Long Description:**

Information Leakage is an application weakness where an application reveals sensitive data, such as technical details of the web application, environment, or user-specific data. Sensitive data may be used by an attacker to exploit the target web application, its hosting network, or its users.

In its most common form, information leakage is the result of one or more of the following conditions:

- \* A failure to scrub out HTML/Script comments containing sensitive information
- \* Improper application or server configurations
- \* Improper application error handling

**Code disclosure vulnerability** 1

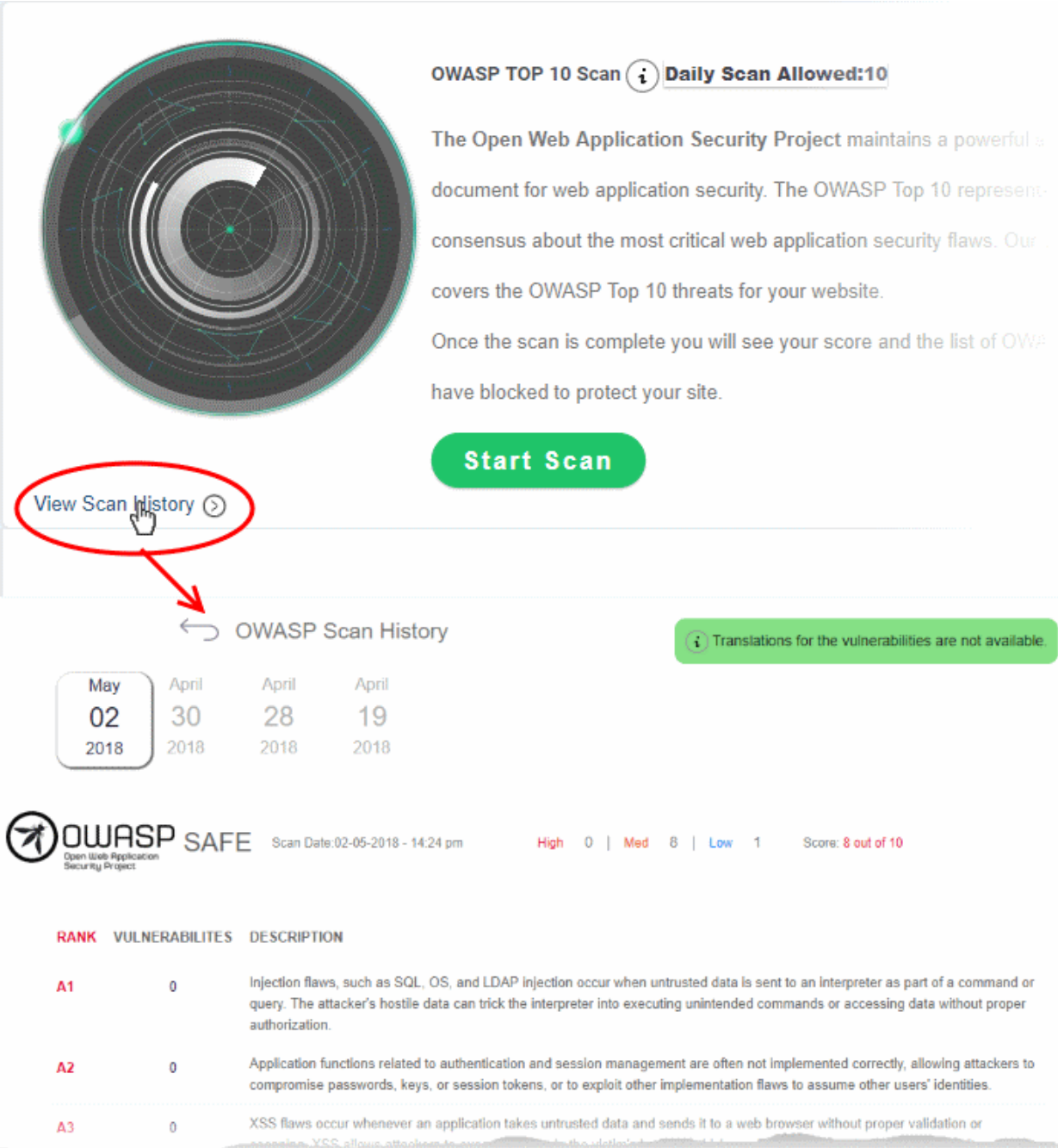
× Close

- The 'Vulnerabilities' pane shows a list of affected files
- The 'Fix Guidance' pane summarizes the fix recommendations.
- The 'Long Description' pane contains detailed background information on the threat

### View the results of previous scans

You can view the results of the 10 most recent OWASP top 10 vulnerability scans on your site.

- Click on registered website on the left
- Choose 'Vulnerabilities' from the sub-menu
- Click 'View Scan History' in the 'OWASP Top Scan' pane



**OWASP TOP 10 Scan** ⓘ **Daily Scan Allowed:10**

The Open Web Application Security Project maintains a powerful document for web application security. The OWASP Top 10 represents a consensus about the most critical web application security flaws. Our scan covers the OWASP Top 10 threats for your website.

Once the scan is complete you will see your score and the list of OWASP vulnerabilities that have blocked to protect your site.

**Start Scan**

**View Scan History** ⓘ

← OWASP Scan History ⓘ Translations for the vulnerabilities are not available.

Month	Day	Year
May	02	2018
April	30	2018
April	28	2018
April	19	2018

**OWASP SAFE** Scan Date: 02-05-2018 - 14:24 pm High 0 | Med 8 | Low 1 Score: 8 out of 10

RANK	VULNERABILITES	DESCRIPTION
A1	0	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2	0	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3	0	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute arbitrary code within the victims' browser.

The dates of the previous scans are shown at the top of the history window.

- Select a date to view detailed results from the scan run on that day
- See **View detailed results of the last scan** if you need more help with this.

## 4.3 Malware Scans

- Click on a website in the left-hand menu and select 'Malware'

You need to upload the scanner agent to your site to enable malware scans.

There are two ways to do this:

1. **Automatically** - Use the cWatch interface to upload the file to your site.
  - Click 'website name' > 'Malware' > 'Enable Scanner' to get started. You need to provide your web-server details.

- See **Upload the agent automatically** for more details.
2. **Manually** - Download the agent and copy it to your site. The agent is a .php file.
    - Click the website name on the left and choose 'Settings'
    - Open the 'Malware Scan' tab
    - Click the 'Activate Manually' link.
    - See **Manual Configuration** if you need more help with this.

One done, cWatch will run scheduled scans on all files hosted on the website. You can also start manual scans from the 'Malware' page.

- cWatch uses a range of malware detection mechanisms to identify threats on your site:
  - Comodo Cloud - Identifies malware using our cloud based file lookup system (FLS)
  - CWW - Uses heuristic technologies to identify malware
  - Dynamic - Uses signature based malware detection
- Automatic malware removal is enabled by default for 'Pro' and 'Premium' licenses. The scan and cleanup will automatically take place according to your schedule. You can manage automatic malware removal in **'Settings' > 'Malware Scan'** page.
- Automatic malware removal is not covered by Basic and Starter license types. If you enable automatic malware removal in **'Settings' > 'Malware Scan'** page, you will be prompted to upgrade your license for the website
- The frequency of the scheduled scans depends on your license type:
  - Basic - Once per day
  - Pro - Twice per day
  - Premium - Four times per day
- The number of scans per day includes both scheduled and manual scans. For example, if you have a premium license and perform two manual scans, then only two scheduled scans will run that day.

### The 'Malware Scans' interface

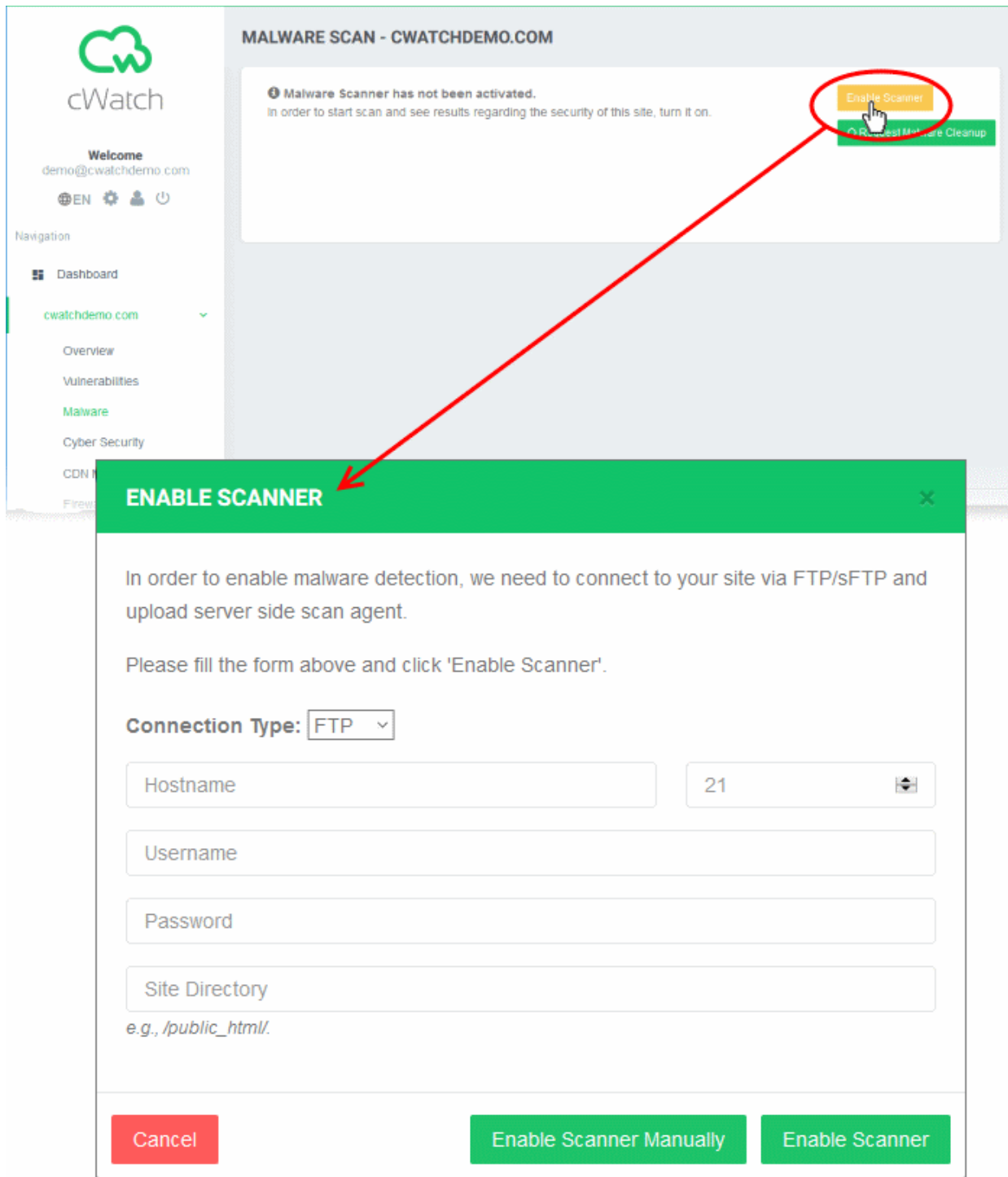
- The 'Malware Scan' page shows the last ten scheduled and manual scans on the site.
- Each row shows the number of malicious files found, and the time of the scan. See **'View malware scan results'** for more details.
- You will receive a notification email if malware is found by a scan.
- You can request Comodo technicians manually remove all threats from your site.

From this interface you can:

- **Upload the scanner agent to your site**
- **Start a manual scan**
- **Submit a malware cleanup request**
- **Start a scan and request a cleanup in a single step**
- **View malware scan results**

### Upload the scanner agent to your site

- Click the name of the target website in the left-menu
- Click the 'Malware' menu-item
- Click 'Enable Scanner':



- Configure the way you want cWatch to access your site to upload the file:

s/FTP Settings - Table of Parameters	
Parameter	Description
Connection Type	Choose whether cWatch should use FTP or sFTP protocol to connect to your server.
Hostname	The hostname or IP address of your FTP or sFTP server
Port	The port through which the website can be securely accessed by cWatch.
Username/Password	The login credentials for the FTP or sFTP server



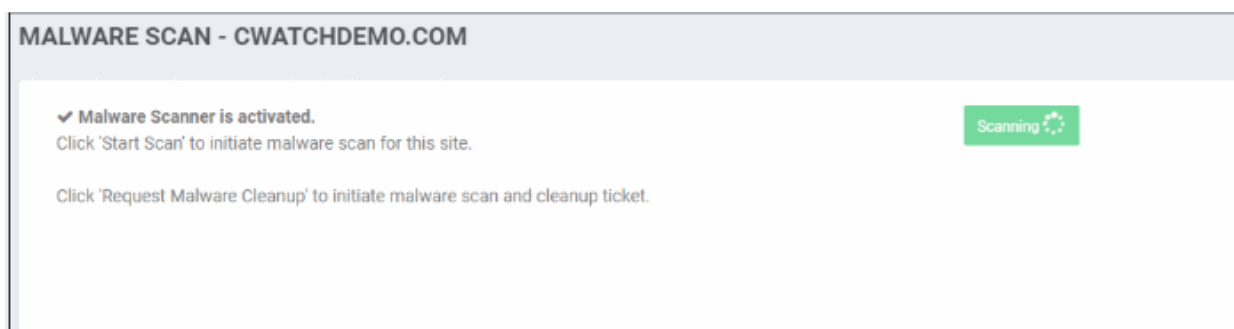
Site Directory	The path to the location of the website in the FTP/sFTP server
----------------	--

- Complete all details and click 'Enable Scanner'. cWatch will upload the file to your website and enable the malware scanner.
- Alternatively, click 'Enable Scanner Manually' to download the file so you can manually upload it to your site. You will be taken to the 'Manual Scan' settings interface for the website. See **Manual Configuration** for more details.

### Start a manual scan

- Click on a website and choose 'Malware'
- Click the 'Start Scan' button

The scanning process starts:



The results are shown at the end of the scan:

+	Scan Start Time: 15.11.2018 - 17:53	Malware Found: 45	<a href="#">Request Malware Cleanup</a>	
+	Scan Start Time: 15.11.2018 - 17:07	Malware Found: 1 ✔ Cleanup Completed	Malware Cleanup Request Progress 100% Completed	Request ID: 1185195 ⬇ Cleanup Report
+	Scan Start Time: 15.11.2018 - 17:00	Malware Found: 0		
+	Scan Start Time: 15.11.2018 - 16:53	Malware Found: 0 ❗ Scan Failed.	❗ Scan Failed.	
+	Scan Start Time: 15.11.2018 - 16:43	Malware Found: 0 ❗ Scan Failed.	❗ Scan Failed.	

- Click the '+' symbol to view malware details and file location.

#	FILE VERDICT	FILE PATH	SHA1	STATUS
1	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.014	b2e3c69c68ad60215164c11fa4d0aefa93fd585b	Safe
2	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.011	97911046502913843b7690f3d4c9ed8b0edba5d7	Safe
3	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.012	7b2b18821ece72cc512e7df3148109c7fa896518	Safe
4	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.013	bccf8fea02332a17ef0dab189761f6717adff703	Safe
5	TrojWare.5153	//CHECK_ME_QUICKLY	ar9d135564406510ee4d05a040fa0488b2280b0d	Safe

- Click 'Request Malware Cleanup' to instruct Comodo technicians to remove the malware. See the following section **Submit a malware cleanup request** for more details.

### Submit a malware cleanup request

You can send a request to Comodo to remove malware, found by any scheduled or manual scan. You can also specify any problems that you encounter with your website when submitting your malware removal request so our technicians can remediate them.

- Click on a website and choose 'Malware'
- Click the 'Request Malware Cleanup' button in the row of a scan where malware was found:

#	FILE VERDICT	FILE PATH	SHA1	STATUS
1	TrojWare.5153	./CHECK_ME_QUICKLY /usr/sample_014	b2e3c69c68ad60215164c11fa4d0aefa93fd585b	Safe
2				Safe

**MALWARE CLEANUP REQUEST**
✕

Submitting this will create a malware removal (cleanup) request on your infected site 'cwatchdemo.com'. Depending on the complexity of the case removal can take couple of hours. You can follow the progress under 'Malware Removal' column.

I'm having trouble with:

- My website is blacklisted (has bad reputation)
- Google shows warning for my site
- Sitecheckers say issue found with my site
- My website is sending emails out of my control
- My shared hosting provider says they will shut my site due to malware
- I see unknown strange files
- My website redirects strangely
- My website does not load
- I want to know if everything is fine with my site
- After your cleanup my website stopped working

Details:

During malware removal process you may realize that some files modified, removed, added on your site. When needed we will access your database, admin panels and necessary locations. Although we will try to keep everything running with no downtime on your site, there can still be minimal downtimes. By filling this form and submitting malware removal request you authorize us to do all above mentioned operations.

Cancel
Submit Request

- Select all issues affecting your site (optional)
- Enter your message to the technician in the 'Details' text box (mandatory)
- Read the information and click 'Submit Request'.
- A request ID is created.
- Our technicians will access your site to remove the malware and remediate the issues you reported.
- The progress of the cleaning operation is shown on-screen.
  - Click 'Request ID' if you want to message the technician while the clean is in progress:

The screenshot shows a dashboard with a 'Malware Cleanup Request Progress' section at 0% and a 'Request ID: 1343750' circled in red. Below this is a modal window titled 'MALWARE REMOVAL REQUEST'. The modal contains the following information:

- Request ID:** 1343750
- Scan Date and Time:** 26.11.2018 - 16:33
- Status:** SCANNING
- Malware Found:** 0
- User:** You
- Date:** 26.11.2018 - 16:33
- Comment:** The site is slow
- Post Comment:** A green button to submit the request.
- Clear:** A grey button to clear the comment.

You will see the following when the cleanup is complete:

The screenshot shows the 'Malware Cleanup Request Progress' section updated to 100% Completed. The status is 'Cleanup Completed' with a green checkmark. A 'Cleanup Report' link is visible next to the Request ID: 1343750.

- Click 'Cleanup Report' to download a summary of the operation. The report itemizes each piece of malware removed.

**Start a manual scan and request a cleanup in a single step**

- The 'Malware' page lets you start a scan and request a cleanup operation in one step.
- You need to upload the malware scanner agent to your site to enable scans.

**To start a scan and submit malware cleanup request**

- Click on a website and choose 'Malware'
- Click the 'Request Malware Cleanup' button on the top right

**MALWARE SCAN - TESTMYPC.COM**

**Malware Scanner has not been activated.**  
In order to start scan and see results regarding the security of this site, turn it on.

Enable Scanner

Request Malware Cleanup

---

**MALWARE CLEANUP REQUEST** [X]

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'.

I'm having trouble with:

- My website is blacklisted (has bad reputation)
- Google shows warning for my site
- Sitecheckers say issue found with my site
- My website is sending emails out of my control
- My shared hosting provider says they will shut my site due to malware
- I see unknown strange files
- My website redirects strangely
- My website does not load
- I want to know if everything is fine with my site
- After your cleanup my website stopped working

Details:

[Text Input Box]

Connection Type:

Hostname:  Port:

Username:

Password:

Site Directory:   
*e.g., /public\_html/*

Cancel [Submit Request]

- Select all issues affecting your site
- Enter your message to the technician in the 'Details' text box

- If the website has not been already enabled for malware scanning, enter the FTP/sFTP access details for the website for cWatch to upload the scanner agent to the website. Note - These options appear only for websites not pre-configured for malware scans.

s/FTP/FTP Settings - Table of Parameters	
Parameter	Description
Connection Type	Choose whether cWatch should use FTP or sFTP to connect to your server.
Hostname	The hostname or IP address of your server
Port	The port through cWatch can should access your site
Username/Password	The login credentials for your server
Site Directory	The location of the website on your server. Enter the full path.

- Complete all details and click 'Submit Request'.

cWatch will upload the agent to your site and commence scanning.

- A cleanup request is created if the scan finds malware.
- Our technicians will access your site to remove malware and remediate any other issues you reported.
- Click 'Request ID' if you want to send a message to the technician while the cleaning is in progress.

**MALWARE REMOVAL REQUEST** ✕

**Request ID:** 1343750      **Scan Date and Time:** 26.11.2018 - 16:33

**Status:** SCANNING      0%

**Malware Found:** 0

**You**      26.11.2018 - 16:33

The site is slow

Please perform a deep clean

Post Comment
Clear

- Enter you message in the text box and click 'Post Comment'. The message will be sent to the technician attending to your malware removal request ticket.

You will see the following screen when the cleanup is complete:

+	Scan Start Time: 15.11.2018 - 17:53	Malware Found: 45 ✔ Cleanup Completed	Malware Cleanup Request Progress 100% Completed	Request ID: 1343750 ⬇ Cleanup Report
---	-------------------------------------	--	--	--

- Click 'Cleanup Report' to download the report in .pdf format. The report contains the numbers of malware of cleaned in different categories.

## View malware scan results

- The 'Malware Scan' page shows the results of all scheduled and manual scans.
- You can view the list of malware identified in any scan with their details
- You can also create a malware cleanup request to our technicians. The technicians access your website and remove the malware identified.
- You can also download a report of the malware cleanup operation.

### To view the malware scan results

- Click on a website and choose 'Malware'

#### MALWARE SCAN - CWATCHDEMO.COM

✔ **Malware Scanner is activated.**  
Click 'Start Scan' to initiate malware scan for this site.

Click 'Request Malware Cleanup' to initiate malware scan and cleanup ticket.

Start Scan

  
 Daily Scan Limit left : 10

+	Scan Start Time: 15.11.2018 - 17:53	Malware Found: 45	<div style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">Request Malware Cleanup</div>	
+	Scan Start Time: 15.11.2018 - 17:07	Malware Found: 1 ✔ Cleanup Completed	Malware Cleanup Request Progress 100% Completed	Request ID: 1185195 ⬇ Cleanup Report
+	Scan Start Time: 15.11.2018 - 17:00	Malware Found: 0		
+	Scan Start Time: 15.11.2018 - 16:53	Malware Found: 0 ❗ Scan Failed.	❗ Scan Failed.	
+	Scan Start Time: 15.11.2018 - 16:43	Malware Found: 0 ❗ Scan Failed.	❗ Scan Failed.	

- Scan Date and Time - Start time of the scan
- Malware Found - Number of threats found by the scan
- Status - Indicates the scan progress and malware cleanup progress (only for scans for which 'Malware Cleanup Request' was raised).
- Request ID - The support ticket number generated malware removal request (MRR).
  - Click the ID to send a message to the technician during the progress of the cleanup process or to view the result of the cleanup process after cleaning is completed.

- Click 'Cleanup Report' to download a .pdf file of the cleanup report

### To view the list of malware identified by a scan

- Click the '+' symbol beside a scan row

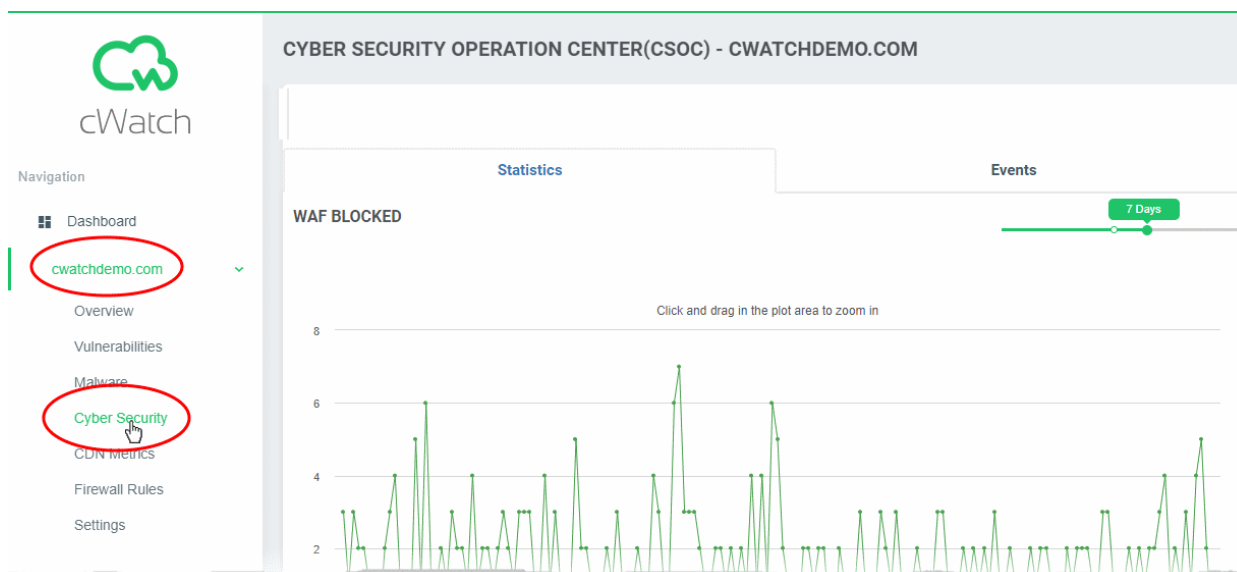
#	FILE VERDICT	FILE PATH	SHA1	STATUS
1	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.014	b2e3c69c68ad60215164c11fa4d0aefa93fd585b	Safe
2	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.011	97911046502913843b7690f3d4c9ed8b0edba5d7	Safe
3	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.012	7b2b18821ece72cc512e7df3148109c7fa896518	Safe
4	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.013	bccf8fea02332a17ef0dab189761f6717adff703	Safe
5	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.004	ac9d135564406510ee4d05a940fa9488b2280b9d	Safe
6	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.003	49f9f6b30ef37967d363e3c207dec4a63e43e1c3	Safe
7	TrojWare.5153	//CHECK_ME_QUICKLY /cure/sample.007	2148b5eaf44a7393cfcfd1452e86b94b4a253b4ce	Safe

Malware Scans - Column Descriptions	
Column Header	Description
File Verdict	The name of the malware
File Path	The location where the malware was detected
SHA1	The Secure Hash Algorithm 1 (SHA1) hash value of the malware file
Status	The action taken on the malware file

## 4.4 Cyber Security Operation Center Results

- Click on a website in the left-hand menu and select 'Cyber Security'
- The Cyber Security Operation Center (CSOC) is a team of dedicated analysts at Comodo who investigate and remove threats discovered by Comodo's enterprise security solutions.
- The CSOC team monitors the event logs of registered websites and constantly updates security rules to deliver unrivaled protection to our users.
- The CSOC interface shows detailed stats about attacks that were blocked on your site. It also lets you choose an action that cWatch should take if similar attacks take place.
- Click the name of a website on the left then choose 'Cyber Security' to open the results interface.





The 'Cyber Security Operation Center (CSOC)' interface has two tabs:

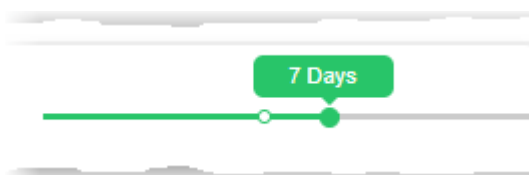
- **Statistics** - Summary of attacks blocked by the Web Application Firewall (WAF). You can specify the action taken on future access attempts from the same origin. See [WAF Statistics](#) for more.
- **Events** - Lists all incidents recorded by the Web Application Firewall (WAF), and the actions taken upon them. You can change the future action from here if required. See [WAF Events](#) for more details.

#### 4.4.1 WAF Statistics

- Click on a website in the left-hand menu and select 'CSOC' > 'Statistics' tab
- The statistics page shows attacks identified and blocked by the web application firewall. This includes the top 5 attack types and top 5 attack sources.
- You can also choose the action taken on future threats from the same sources. cWatch updates your WAF rules accordingly.

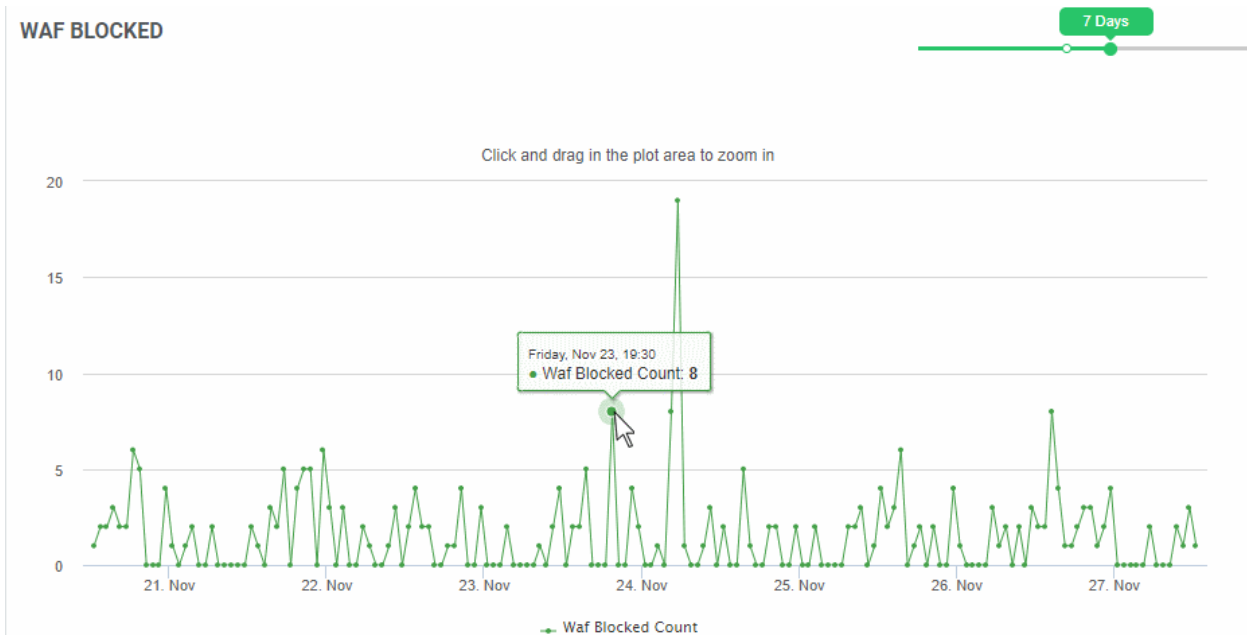
##### View WAF statistics

- Click on a registered domain on the left then choose 'CSOC'
- Open the 'Statistics' tab if not already open



##### WAF Blocked

Timeline of attacks blocked by the web application firewall (WAF). The WAF is constantly updated with new rules to combat the very latest threats.



- Place your mouse anywhere on the chart to see the number of attacks blocked at that point in time.
- Click and drag the line to zoom in on a time range. Click 'Reset Zoom' to return to the original view.

## Threat Summary

The number of attacks identified and blocked, and the number of custom WAF rules active on the website.

827 Threats Stopped

99 Active Custom Firewall Rules

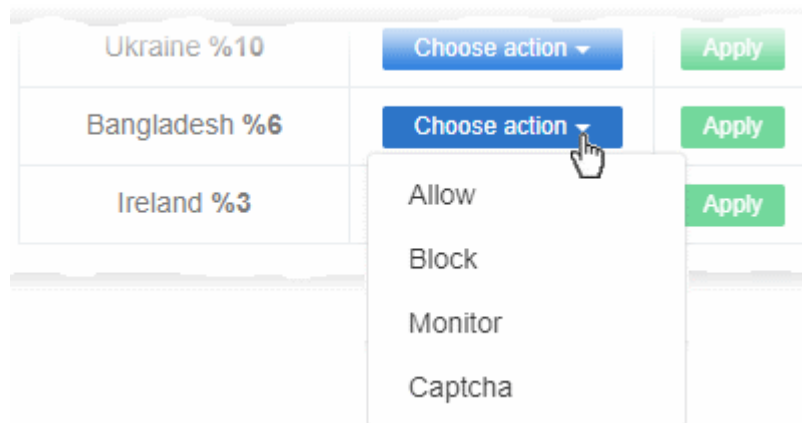
- **<NN> Threats Stopped** - Click to view a list of the threats blocked. See **WAF Events** for more details.
- **<NN> Active Custom Firewall Rules** - Click to view and manage the WAF rules active on the site. See **Configure Firewall Rules** for more details.

## Top Countries

The top 5 countries from which attacks originated. You can also see the percentage of all attacks that came from the country.

Top Threat Countries		
United States %50	Choose action ▾	Apply
United Kingdom %11	Choose action ▾	Apply
Ukraine %10	Choose action ▾	Apply
Bangladesh %6	Choose action ▾	Apply
Ireland %3	Choose action ▾	Apply

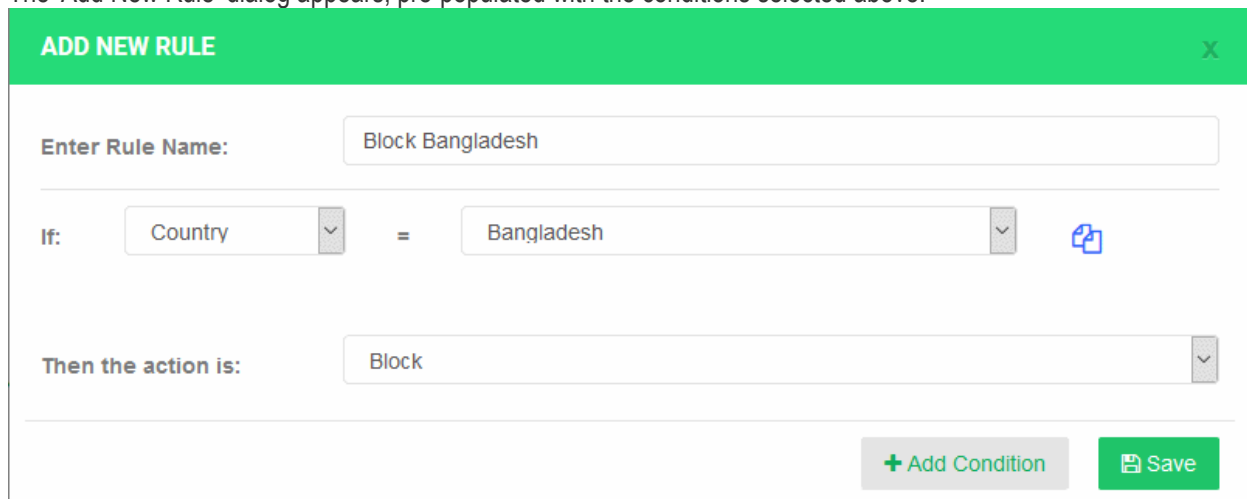
**Choose action** - Specify the action that should be taken on future attacks from the country:



- **Allow** - All traffic from the country is permitted. This includes legitimate traffic, bots etc.
- **Block** - No traffic is allowed from the country. An error message is shown to users.
- **Monitor** - Traffic from the country is recorded. This action is particularly useful for testing out potential 'Captcha' and 'Block' rules. You can check what specific traffic will be affected before setting up a rule that might negatively impact customers.
- **Captcha** - Shows an interactive test that allows visitors to prove they are human. Users need to pass the test to access the website. Captcha images are generated randomly.

Click 'Apply' to save your choice.

The 'Add New Rule' dialog appears, pre-populated with the conditions selected above.



- Edit the rule name and conditions if required
- Click 'Save' to add the rule.

You can view the rule from the 'Firewall Rules' interface. An example is shown below:

**Custom WAF Rules** Total 100 rules + Add New Rule

RULE ID	RULE NAME	TYPE	DETAILS	ACTION	
1202936	Block Bangladesh	Country	BD	Block	<span style="color: green; font-size: 1.2em;">✎</span> <span style="color: red; font-size: 1.2em;">✖</span> <span style="margin-left: 10px;"> <input checked="" type="checkbox"/> On                 </span>

- See [Configure Firewall Rules](#) for more details on managing custom firewall rules.

### Top Organizations

Shows the top 5 entities from which attacks originated:

Top Threat Organizations		
Amazon Technologies Inc. %22	<a href="#" style="background-color: #007bff; color: white; padding: 2px 10px; border-radius: 3px;">Choose action ▼</a>	<a href="#" style="background-color: #28a745; color: white; padding: 2px 10px; border-radius: 3px;">Apply</a>
Microsoft Corporation %9	<a href="#" style="background-color: #007bff; color: white; padding: 2px 10px; border-radius: 3px;">Choose action ▼</a>	<a href="#" style="background-color: #28a745; color: white; padding: 2px 10px; border-radius: 3px;">Apply</a>
Proxad LTD %7	<a href="#" style="background-color: #007bff; color: white; padding: 2px 10px; border-radius: 3px;">Choose action ▼</a>	<a href="#" style="background-color: #28a745; color: white; padding: 2px 10px; border-radius: 3px;">Apply</a>
Webhost, Inc. %5	<a href="#" style="background-color: #007bff; color: white; padding: 2px 10px; border-radius: 3px;">Choose action ▼</a>	<a href="#" style="background-color: #28a745; color: white; padding: 2px 10px; border-radius: 3px;">Apply</a>
GENIUS IT %5	<a href="#" style="background-color: #007bff; color: white; padding: 2px 10px; border-radius: 3px;">Choose action ▼</a>	<a href="#" style="background-color: #28a745; color: white; padding: 2px 10px; border-radius: 3px;">Apply</a>

**Choose action** - Specify the action that should be taken on future attacks from the organization.

The rest of the process is similar to creating a rule for a country. See the [explanation above](#).

- See [Configure Firewall Rules](#) for help with custom firewall rules.

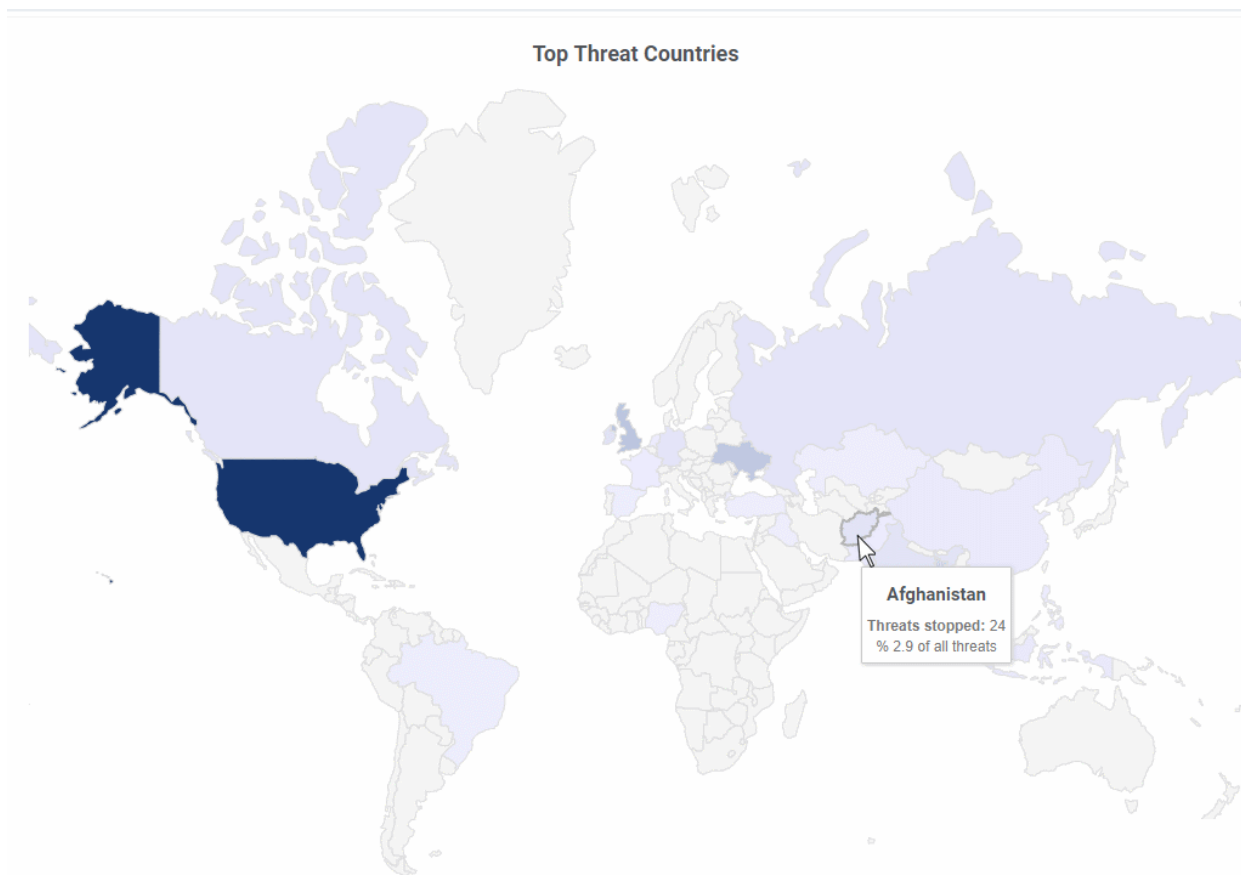
### Top Threats

Shows the top 5 attack types blocked by WAF:

Top Threats Stopped
Traffic From Hosting Services %39
Unknown User Agent Prevention %15
Traffic Via Proxy Networks %13
Traffic Via a VPN %7
CSRF %6

### Top Threat Countries

A map showing the countries from which most attacks came:



- Mouse-over a country to view the number of attacks and percentage of total attacks from that country.

#### 4.4.2 WAF Events

- Click on a website in the left-hand menu and select 'CSOC' > 'Events' tab
- The 'Events' page lists all access attempts intercepted by Web Application Firewall (WAF) rules.
- Details include the source IP of the attempt, the rule that caught the attempt, and the action taken on the traffic. Actions include allow, block, monitor, or allow with captcha verification.
- 'Choose Action' - Specify the action to be taken on future incidents of the same type from the same source. cWatch updates your WAF rules automatically.

WAF Events - Column Descriptions	
Column Header	Description
Rule Name	The label of the firewall rule that intercepted the access request
Action	The activity of the access request on the website
Result	Whether the traffic was blocked, allowed, monitored or allowed with a captcha verification
IP	The IP address of the source from which the access request originated
Country	The country from which the access request originated
Date	The date and time of the access request

### Sorting and Filtering options:

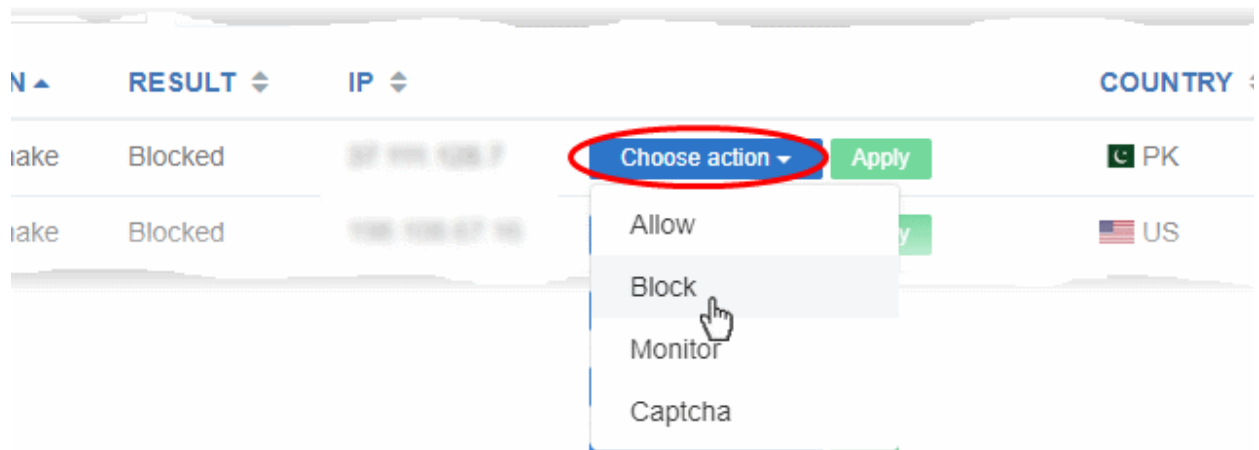
- Use the buttons along the top to filter events by action taken on the traffic

- Use the time buttons to select the interval over which you want to view events

- Search box - Enter an IP to find access requests from a specific address

Create a custom rule to filter traffic from a specific address

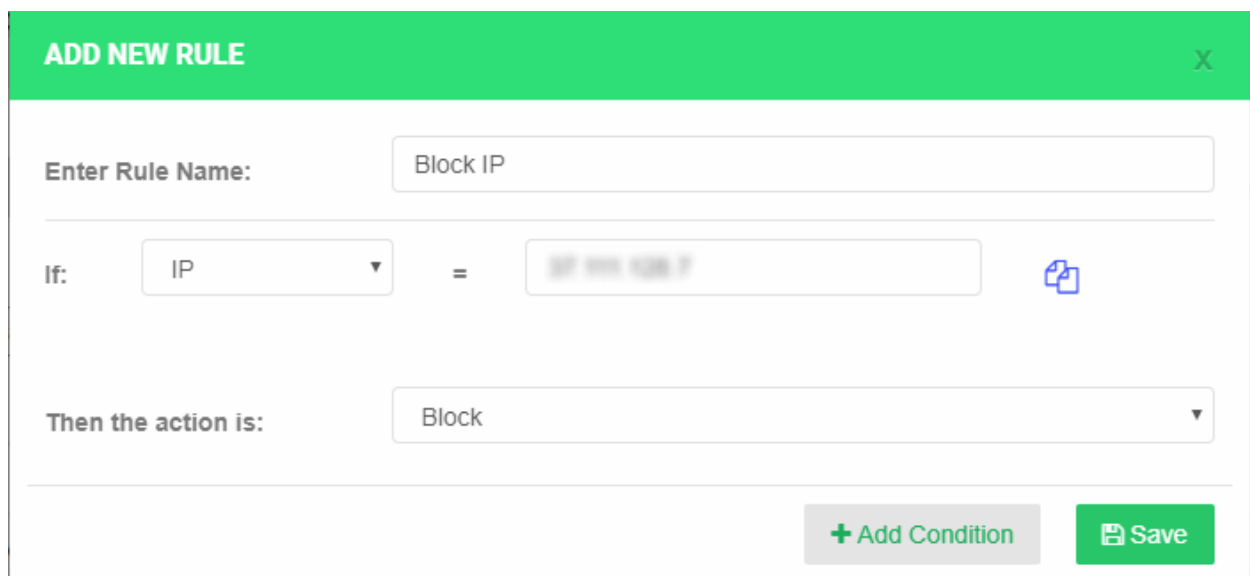
- Click the 'Choose an action' button beside an IP address and select an action:



- **Allow** - All traffic from the IP is permitted. This includes legitimate traffic, bots etc.
- **Block** - No traffic from the IP is allowed.
- **Monitor** - Traffic from the IP is recorded. This action is particularly useful for testing out potential 'Captcha' and 'Block' rules. You can check what specific traffic will be affected before setting up a rule that might negatively impact customers.
- **Captcha** - Shows an interactive test that allows visitors to prove they are human. Users need to pass the test to access the website. Captcha images are generated randomly.

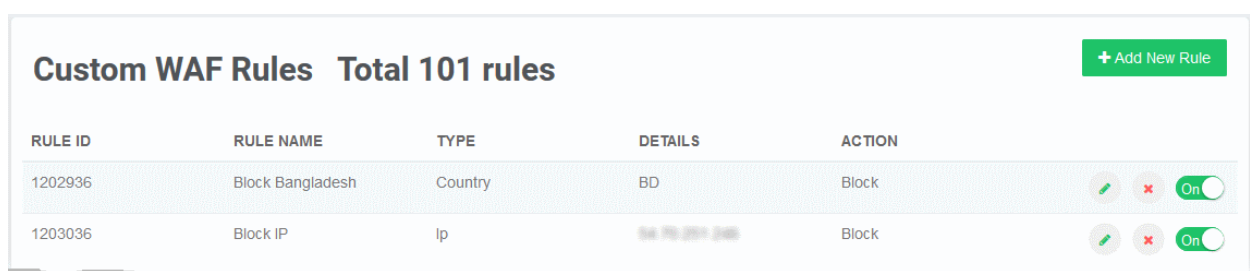
Click 'Apply' to save your choice.

The 'Add New Rule' dialog appears, pre-populated with the conditions as selected above.



- Edit the rule name and conditions if required
- Click 'Save' to add the rule.

You can view the rule in the 'Firewall Rules' interface:



- See [Configure Firewall Rules](#) for more details on managing custom firewall rules.

## 4.5 Content Delivery Network Metrics

- Click on a website in the left-hand menu and select 'CDN Metrics'
- Your cWatch license includes a content delivery network (CDN) service for your websites. The service will improve page load-times for your customers and improve the reliability/uptime of your site.
- You can configure your sites to use the service by changing your domain's authoritative DNS to Comodo, or by adding a CNAME entry to your DNS records.
- Comodo Authoritative DNS name server (NS) details are provided in 'Settings' > 'Domain'. The CNAME entry is generated by cWatch. See [Add Websites](#) and [Website Configuration](#) for more details.

Once configured, the CDN service will:

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

The Content Delivery Network (CDN) Metrics page for a website displays statistics on your CDN usage and traffic throughput.

- Click a website name on the left then choose 'CDN Metrics' .
- The slider at the top right allows you to choose the time period for which you want to view the statistics.



The page contains the following charts:

### CDN Usage

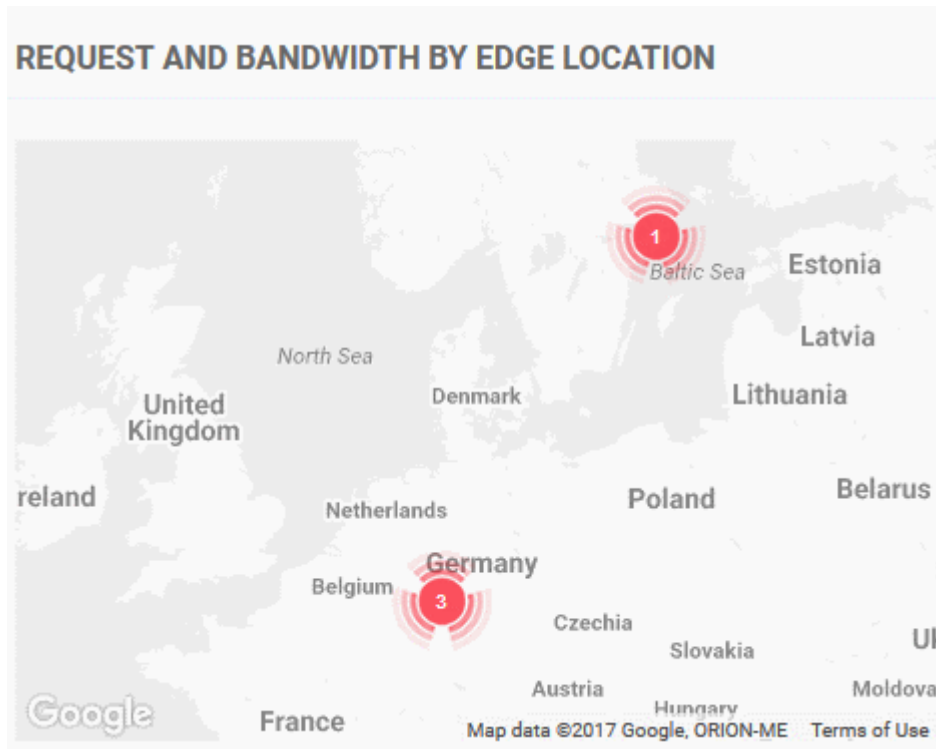


The 'CDN Usage' field shows how much CDN data your website has used.

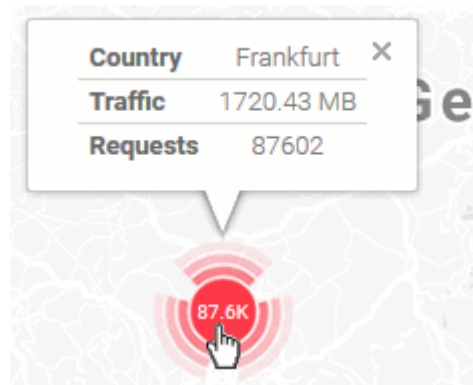


## Request and Bandwidth by Edge Location

The 'Request and Bandwidth by Edge Location' map shows the regions from which your traffic originated. You can also view the number of access requests from each region.



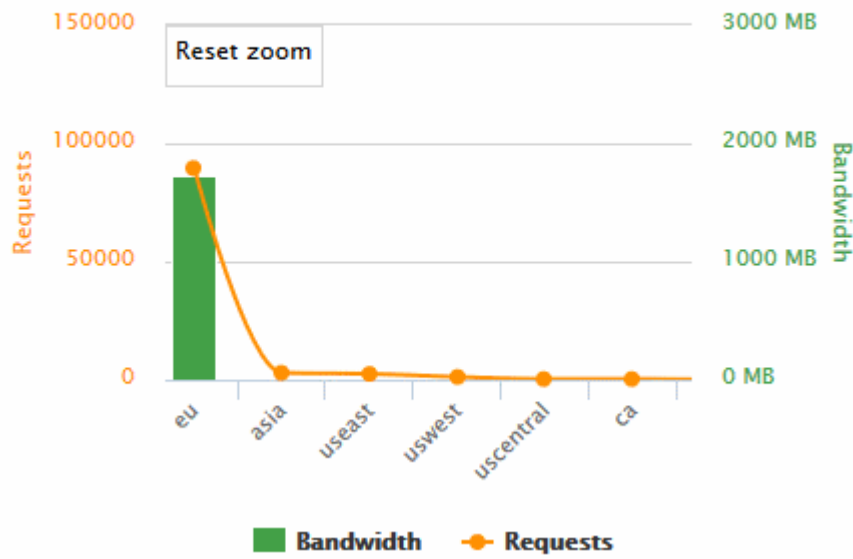
- Click on an regional hot-spot to view the traffic and number of access requests from that region.



## Request and Bandwidth by Region

This graph shows the number of website requests and the amount of data used by each continent.

### REQUEST AND BANDWIDTH BY REGION

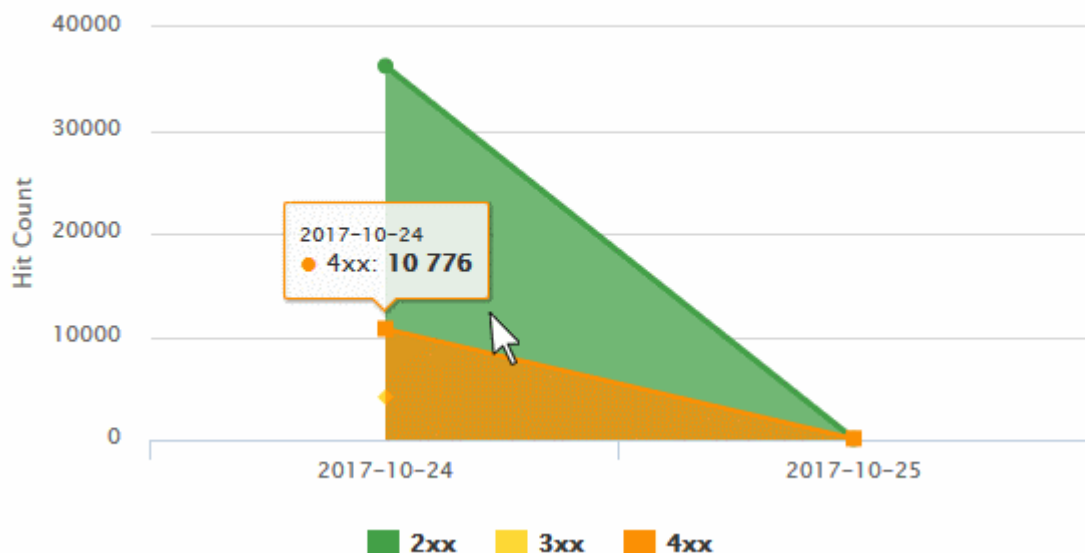


- You can choose the time period using the slider at top-right.
- Select a portion of the graph to zoom-in
- The yellow line graph shows the number of requests from different continents
  - Place your mouse on the line to view the number of requests from the respective continent
- The green bar graph shows the bandwidth usage from different continents
  - Place your mouse on a bar to view the precise traffic bandwidth from the respective continent

### Status Codes by Types

- Shows the different HTTP status codes sent to your visitors in response to their page requests.

### STATUS CODES BY TYPES



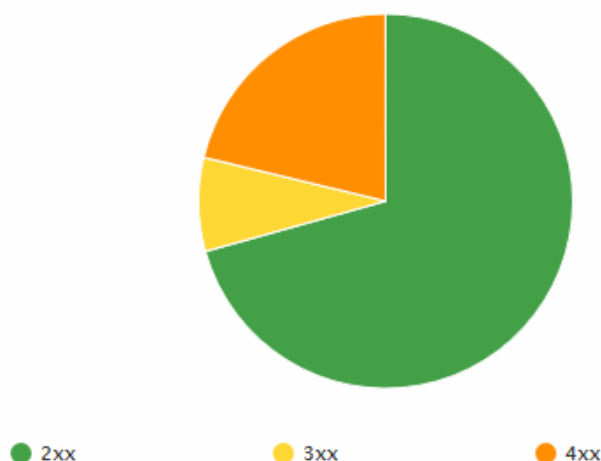
- 2xx = Success
- 3xx = Redirection
- 4xx = Client errors
- 5xx = Server errors
- You can choose the time period using the slider at top-right.
- Select a portion of the graph to zoom-in
- Place your mouse on the graph to view the number of responses of that type returned at that time point

### Status Code Distribution by Percentage

Shows the percentage of HTTP response status codes generated by your site within the set time period. HTTP status codes are as follows:

- 1xx Informational responses.
- 2xx Success.
- 3xx Redirection.
- 4xx Client errors.
- 5xx Server errors.

#### STATUS CODE DISTRIBUTION BY PERCENTAGE



- You can choose the time period using the slider at top-right.
- Place your mouse on a sector to view the number of responses of that type

### Status Code Details

The 'Status Code Details' pane displays the precise HTTP response status codes returned within the selected time period.

A detailed explanation of each code is available at [https://en.wikipedia.org/wiki/List\\_of\\_HTTP\\_status\\_codes](https://en.wikipedia.org/wiki/List_of_HTTP_status_codes).

**STATUS CODE DETAILS**

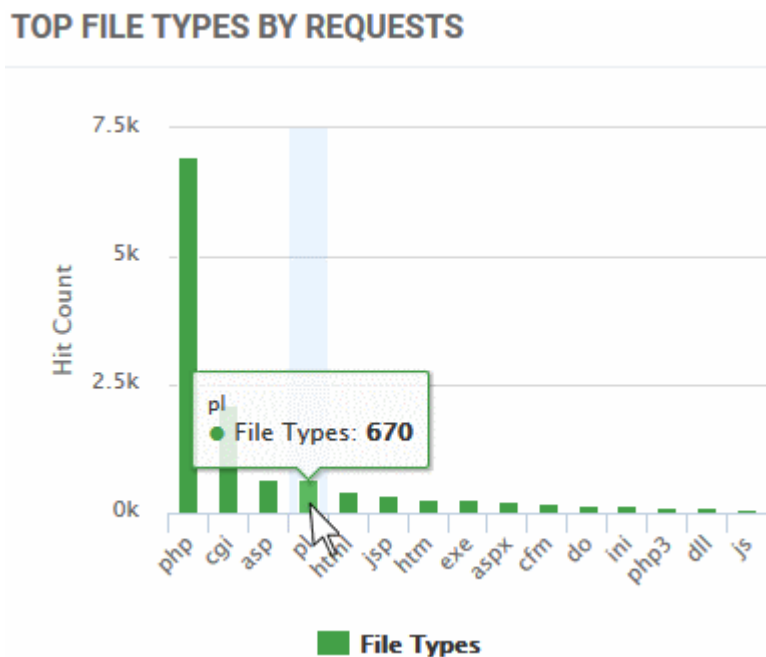
STATUS CODE ↕	HITS ↕
200	36346
301	4155
400	65
403	10821
404	30
<b>Total</b>	<b>51421</b>

Showing 5 out of 7 < 1 of 2 >

- You can choose the time period using the slider at top-right.
- Use the search box at the right to search for a particular status code
- Click any column header to sort the items in alphabetical ascending/descending order of entries in that column.

**Top File Types by Requests**

The 'Top File Types by Requests' graph shows the numbers of different file types requested by your website visitors over the set time period.

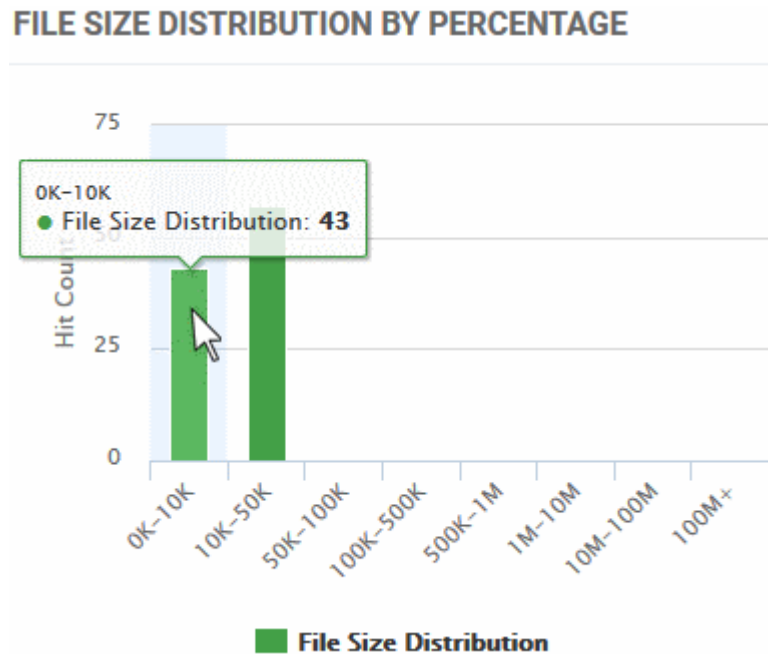


- You can choose the time period using the slider at top-right.

- Place your mouse on a bar to view the exact number of files of that type served to your visitors.
- Select a portion of the graph to zoom-in

## File Size Distribution by Percentage

The 'File Size Distribution by Percentage' graph shows the numbers of files of different file sizes requested by and served to your visitors from your website.



- You can choose the time period using the slider at top-right.
- Place your mouse on a bar to view the exact number of files of that size range delivered to your visitors.
- Select a portion of the graph to zoom-in

## All File Types

The 'All File Types' pane displays the exact numbers of different types of files delivered to your visitors from your website within the selected time period.

### ALL FILE TYPES

FILE TYPE	HITS
php	6959
cgi	2115
asp	678
pl	670
html	415
<b>Total</b>	<b>14843</b>

Showing 5 out of 50 < 1 of 10 >

- You can choose the time period using the slider at top-right.
- Use the search box at the right to search for a particular file type.
- Click any column header to sort the items in alphabetical ascending/descending order of entries in that column.

## 4.6 Configure Firewall Rules

- Click on a website in the left-hand menu and select 'Firewall Rules'

You can define custom rules to block, allow, monitor or challenge specific types of traffic. These are in addition to the firewall rules built-in to cWatch. You need to enable the firewall for custom rules to work (click 'Settings' > 'WAF').

- You can create custom rules for specific IPs, IP ranges, countries, organizations and more.
- You can add multiple conditions to a rule. For example you can configure a rule to block traffic from a specific IP in a certain country.
- Messages are shown to site visitors for actions such as block and captcha.

**Important** - The firewall prioritizes rules by action type. It does not use a 'ladder' system whereby rules are prioritized by their position in the interface. Action priority is as follows:

1. Monitor
2. Allow
3. Block
4. Captcha

... so in the event of a conflict, 'Monitor' rules overrule 'Allow' rules, which in turn overrule 'Block' rules and so on.

For example, suppose a piece of traffic is covered by three separate rules:

- Rule A - 'Block' the traffic based on country
- Rule B - 'Allow' the traffic based on URL
- Rule C - Show 'Captcha' based on content type




The traffic is allowed as allow rules supersede block and captcha rules.

### Open the Firewall Rules interface

- Click a website name on the left and select 'Firewall Rules' .

The screenshot displays the 'FIREWALL RULES - CWATCHDEMO.COM' interface. On the left, the navigation menu includes 'Firewall Rules' which is circled in red. The main content area shows 'Custom WAF Rules' with a total of 7 rules. A table lists the rules with their IDs, names, types, and actions. Each rule has edit, delete, and toggle icons.

RULE ID	RULE NAME	TYPE	DETAILS	ACTION
1162940	InMotions IP	Ip	192.168.1.1-10	Allow
1162984	Joe Home IP	Ip	192.168.1.10	Allow
1162985	Thomas Home IP	Ip	192.168.1.10-15	Allow
1162986	Office IP	Ip	192.168.1.10-20	Allow
1162987	Wilson Home IP	Ip	192.168.1.10	Allow
1163117	Whitelisting cron jobs from InMotion Hosting	Complex	Complex	Allow
1208557	Block Namibia	Country	NA	Block

Custom WAF Rules - Column Descriptions	
Column Header	Description
Rule ID	An auto-generated identity number for each rule
Rule Name	The label of the rule.
Type	The category targeted by the rule. For example IP, country, content type, organization.
Details	Specific items within the chosen category. For example, if 'Country' is the 'Type', this column shows the two letter country code of the country.
Action	The process the firewall will execute on the target if rule conditions are met
Buttons	 - Edit the firewall rule   - Remove the rule   - Enable / disable the rule

### Add a new WAF rule

- Click 'Add New Rule' at the top right

MO.COM

Rules Total 99 rules

+ Add New Rule

NAME	TYPE	DETAILS	ACTION
hist IP	Ip	192.168.2.1, 192.168.2.2	Allow
	Ip	192.168.2.1-192.168.2.2	Allow

**ADD NEW RULE**

Enter Rule Name:

If:  =


Then the action is:

+ Add Condition Save

- Rule Name - Type a label which describes the rule.
- Condition 'If' - Choose the source of the traffic:
  - **IP** - Enter a specific IP
  - **IP Range** - Enter an IP range. For example, 192.168.2.1,192.168.255
  - **URL** - Enter a domain you want to block.
  - **User Agent** - Client software. For example, a browser, mail client or crawler which makes a request to the website. You need to enter the string to identify the client.
    - You can view a list of user agent strings at <http://www.useragentstring.com/pages/useragentstring.php>
    - For example, The string for Firefox 64.0 is 'Mozilla/5.0 (X11; Linux i686; rv:64.0) Gecko/20100101 Firefox/64.0'
    - Select 'Exact Match' if you have entered the string in full. The rule will only apply to requests from the specific version of the user-agent.
  - **Header** - The HTTP header field.
  - **HTTP Method** - Options are: Post, Get, Head, Put, Delete, Patch and Options.
  - **File Type / Extension** - Enter the file type / extension parameter. For example - pdf. exe
  - **Content Type** - Enter the content type. For example: application/json
  - **Country** - Select a country from the drop-down
  - **Organization** - Name of the organization with whom the IP is registered. For example, Google,



Amazon, Facebook and so on. So, if you enter Amazon, all IPs registered by Amazon will apply for the condition.

-  - Duplicate the condition. The duplicate condition is shown underneath the original, ready for you to modify as required.
- **Add Condition** - Create another criteria for the action. Conditions are always 'And', so all conditions must be satisfied before the selected action is implemented.
- **Action** - The action you want taken on the traffic. Choose from the following:
  - **Allow** - All traffic from the country is permitted. This includes legitimate traffic, bots etc.
  - **Block** - No traffic is allowed from the country. An error message is shown to users.
  - **Monitor** - Traffic from the country is logged. This action is particularly useful for testing out potential 'Captcha' and 'Block' rules. You can discover what traffic is affected before setting up a rule that might negatively impact customers.
  - **Captcha** - Shows an interactive test that allows visitors to prove they are human. Users need to pass the test to access the website. Captcha images are generated randomly.
- Click 'Save' to add the new rule

## 4.7 Website Configuration

- Click a website name on the left
- Click 'Settings'

The 'Settings' interface lets you:

- Configure vulnerability and malware scanning on a website
- Configure FTP access so cWatch technicians can resolve issues on your site
- Register your website with the content delivery network (CDN)
- Upload the SSL certificate used to secure the site if you are using HTTPS
- Configure CDN cache management settings for your website
- Configure custom Web Application Firewall (WAF) rules
- Endorse your website with a 'Trust Seal' from Comodo.

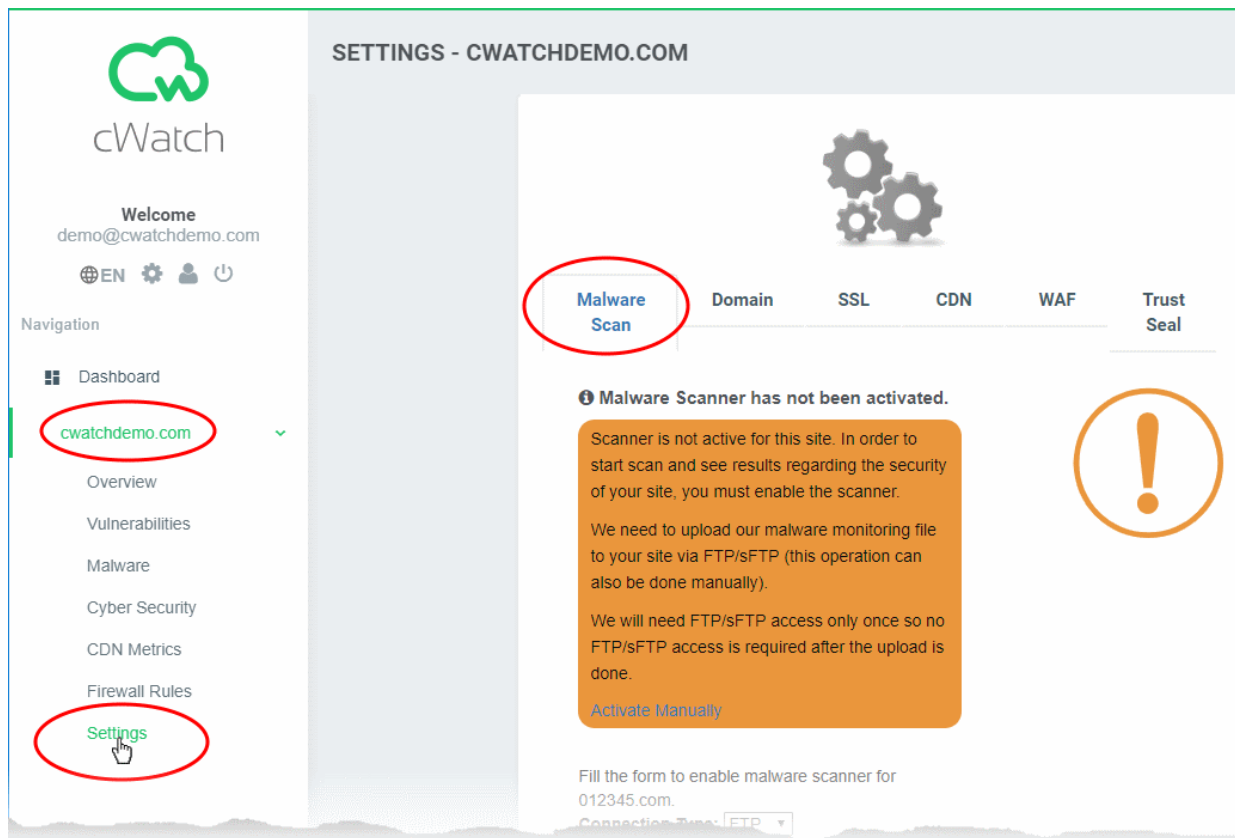
The screenshot shows the 'SETTINGS - CWATCHDEMO.COM' interface. On the left, the navigation menu includes 'Dashboard', 'cwatchdemo.com', 'Overview', 'Vulnerabilities', 'Malware', 'Cyber Security', 'CDN Metrics', 'Firewall Rules', and 'Settings' (highlighted with a red circle). The main content area has six tabs: 'Malware Scan', 'Domain', 'SSL', 'CDN', 'WAF', and 'Trust Seal'. The 'Malware Scan' tab is active, showing a warning: 'Malware Scanner has not been activated.' Below this is an orange box with instructions: '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'. Below the warning is a form to enable the scanner for 012345.com, with fields for 'Connection Type' (set to FTP), 'Hostname', 'Username', 'Password', and 'Site Directory' (with an example: /public\_html/). An 'Enable Scanner' button is at the bottom right.

The interface contains six tabs:

- **Malware Scan Settings** - Configure settings for manual or automatic scans on your site. See **Configure Malware Scan Settings** for more details.
- **Domain** - Configure DNS and nameservers in order to enable cWatch protection. See **Domain Configuration Instructions** for more information.
- **SSL Configuration** - Specify whether your site uses HTTP or HTTPS. You can get a complimentary SSL certificate from Comodo if you choose HTTPS. Alternatively, you can upload an existing certificate. See **SSL Configuration** for more details.
- **CDN Settings** - Configure CDN cache and CDN edge settings. See **CDN Settings** for more details.
- **WAF Settings** - Configure Web Application Firewall policies. See **WAF Settings** for more information.
- **Trust Seal** - Configure your website's site seal. There are two types of seals: 'Malware Free' and 'Protected' trust seals. See **Trust Seal** for more details.

## 4.7.1 Configure Malware Scan Settings

- Click the website name > 'Settings' > 'Malware Scan'
- You need to upload a file to your site to activate malware scans.
- You can have cWatch upload the file for you, or you can manually upload the file.



See following sections for detailed guidance on:

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

### 4.7.1.1 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/

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.

### 4.7.1.2 Manual Configuration

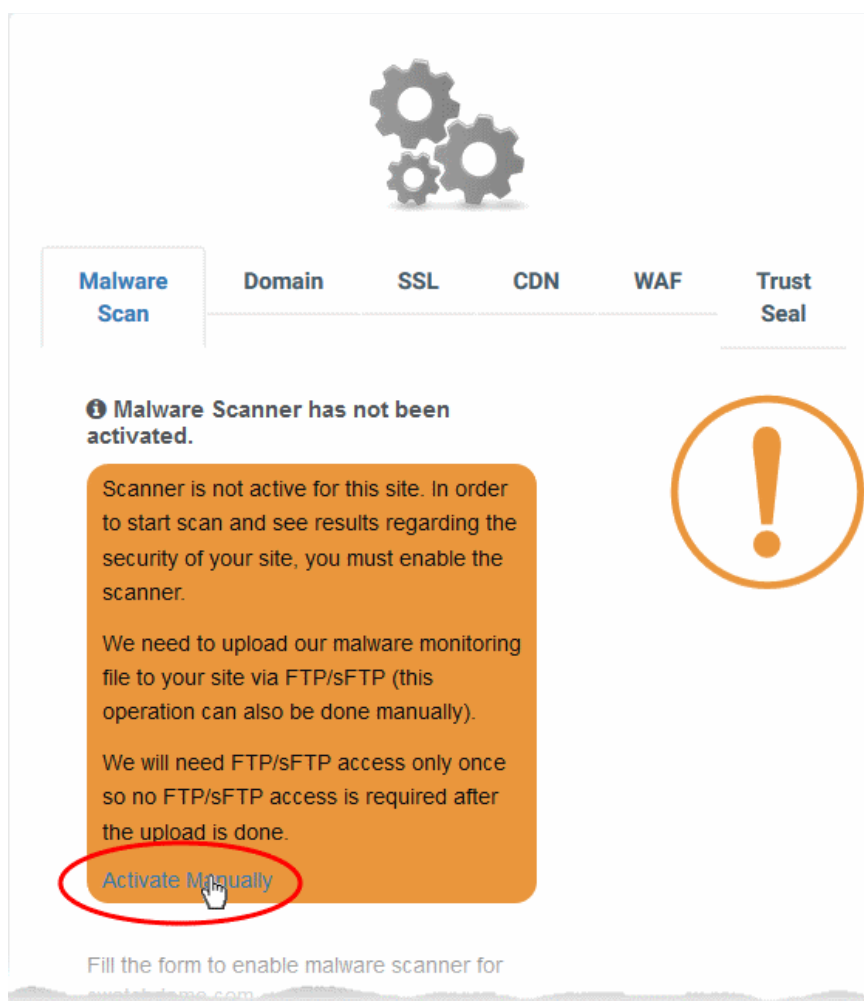
- You need to upload a .php file to your website to enable automatic malware scans.
- cWatch will verify the file at the location you specify and commence scanning.
- You have the option to automatically remove the malware at the end of every scan.

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

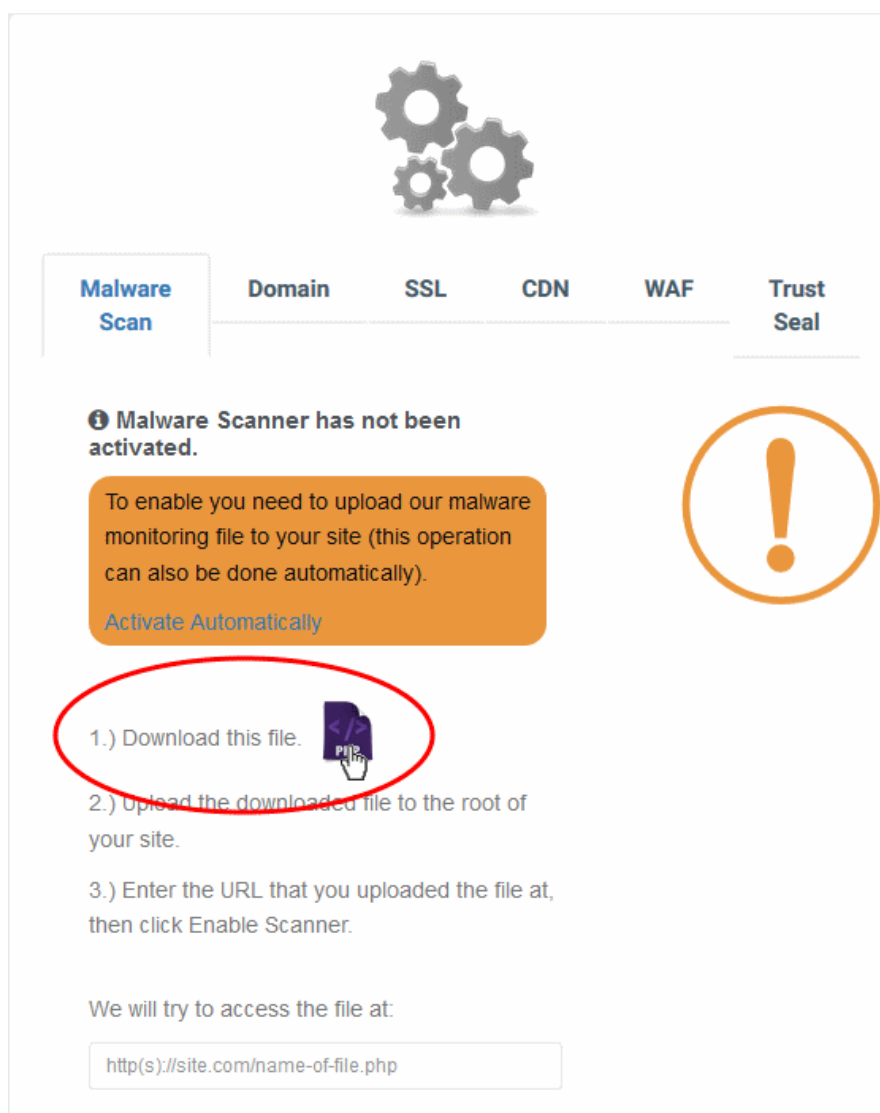
1. **Automatic** - Provide website access details and let cWatch automatically upload the file via FTP.
  - Click the website name on the left and choose 'Malware'
  - Click 'Enable Scanner' and provide website details.
  - See '**Malware Scans**' if you need more help with this.
2. **Manual** - Download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

#### Manual Download

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



- This opens the file download page:




**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.

## 4.7.2 Domain Configuration Instructions

**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.

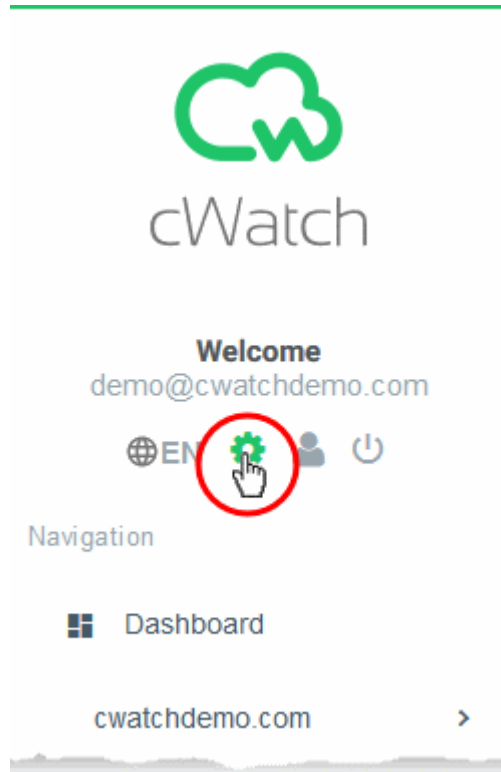
After **adding a website** to cWatch, you next have to configure DNS settings. You need to do this in order to enable cWatch protection, the content delivery network, and the Web Application Firewall (WAF). There are two ways this can be done:

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

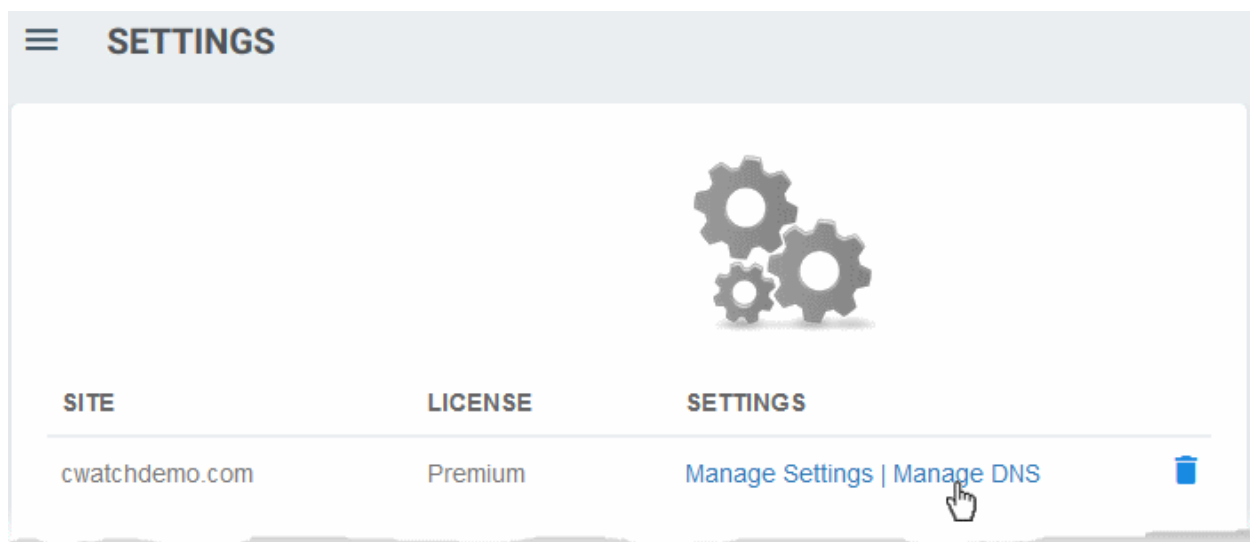
### **Option A - Change your domain's authoritative DNS servers to Comodo**

**Important Note** - After changing your domain's DNS servers 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. See '**Manage DNS Records**' in '**The Settings Interface**' for more information.

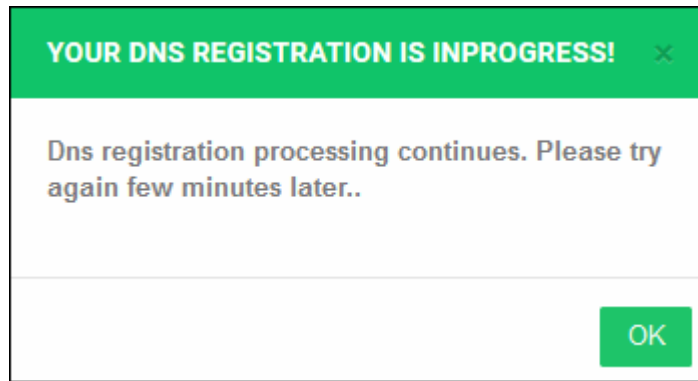
- Click the settings icon above the navigation menu:



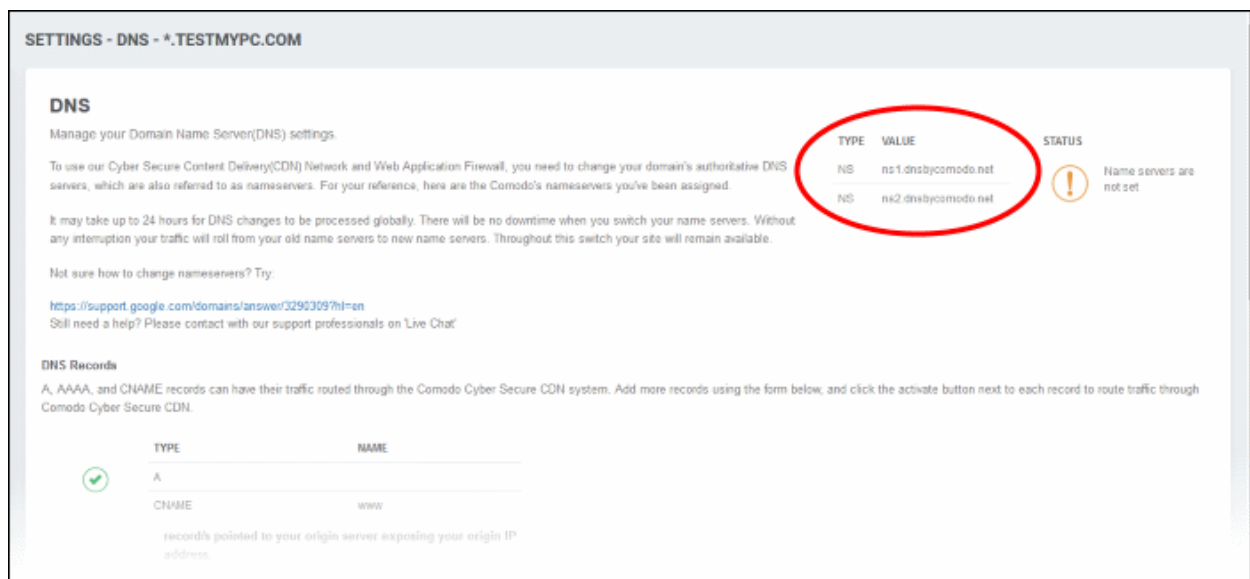
The main settings page opens:



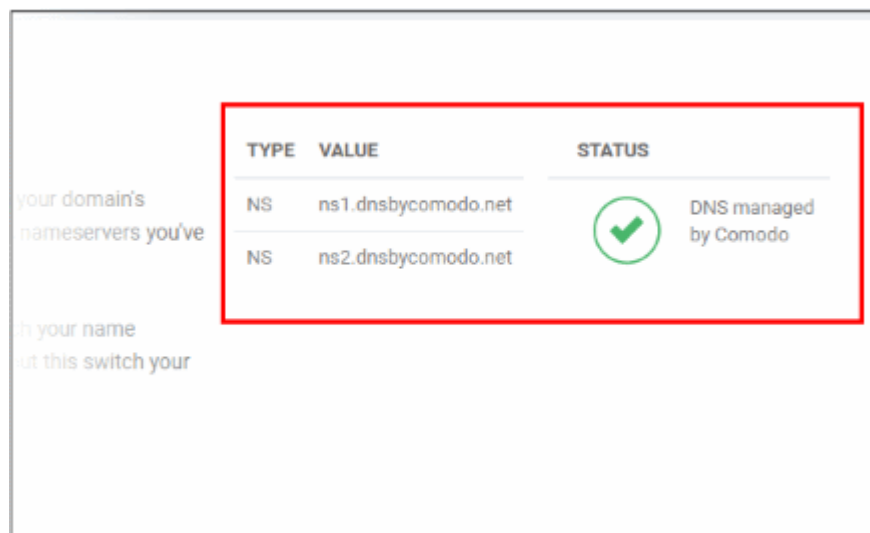
- Click 'Manage DNS' under 'Settings' in the row of the added website
- You will see the following message while registration is in progress:



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



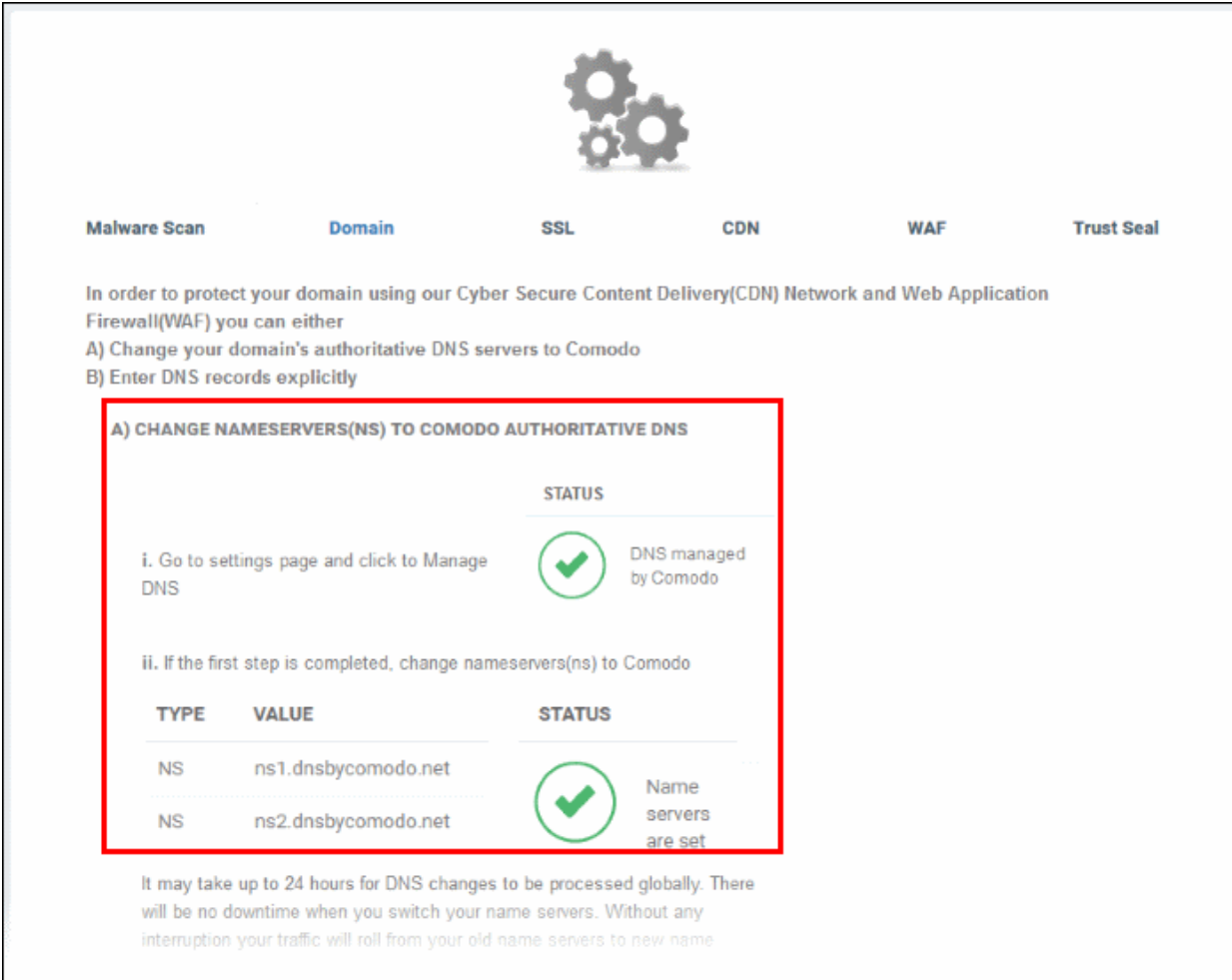
- Go to your website's DNS management page and enter the new nameservers
- See <https://support.google.com/domains/answer/3290309?hl=en> if you need more help regarding changing nameservers
- Open the settings page and click 'Manage DNS' to view the nameserver update status:






OR

- Click the website name in the left menu, then 'Settings' > 'Domain' tab






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

In order to protect your domain using our Cyber Secure Content Delivery(CDN) Network and Web Application Firewall(WAF) you can either


A) Change your domain's authoritative DNS servers to Comodo  
B) Enter DNS records explicitly

**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 the DNS changes to be processed globally.
- Please note there will no downtime on your website when you switch your name servers.

**Important Note** - After pointing your name servers to Comodo, you have to use cWatch to manage your DNS records. 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. See '**Manage DNS Records**' in '**The Settings Interface**' for more information.

### 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.

### 4.7.3 SSL Configuration

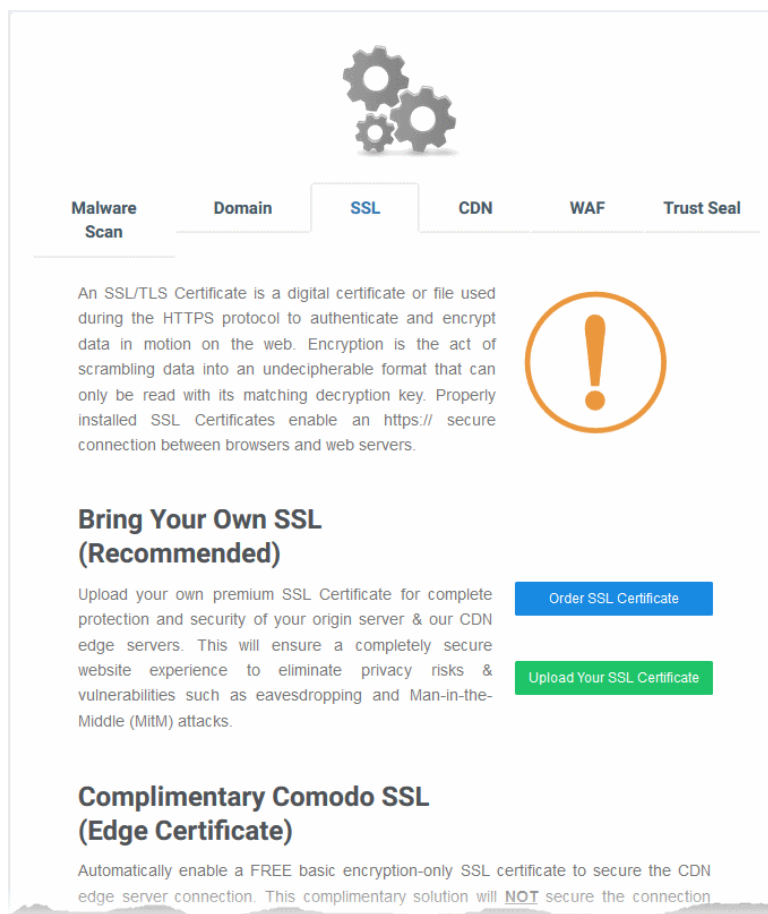
- An SSL/TLS certificate is placed on a website to identify the domain owner and encrypt all data that passes between the site and a visitor's browser.
- Sites that use a SSL/TLS certificate have a URL that begins with HTTPS. For example, <https://www.example.com>
- Comodo strongly recommends you use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



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.

[Order SSL Certificate](#)

[Upload Your SSL 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

- 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

	<p>this:</p> <pre> -----BEGIN CERTIFICATE----- MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGEw JDTjEL MAkGA1UECBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1 UECxMC VU4xFDASBgNVBAMTC0hlcm9uZyZyZW5nMB4XDTA1MDcxNTIxMTk0N1oXDT A1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAGTA1BOMQswCQYDVQ QHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTA1VOMRQwEgYDVQQDEwtIZXJvbm cgWwFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBew KE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbMOoRcKK9vEcgmTcLFuQTWDl3Rag MBAAGj gbEwga4wHQYDVR0OBBYEFFXI70krXeQDxZgbaCQoR4jUDncEMH8GA1UdIw R4MHaA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMQswCQYDVQQGEwJDTjELMA kGA1UE CBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECxMVCVU 4xFDAS BgNVBAMTC0hlcm9uZyZyZW5nggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvc NAQEE BQADQQA/ugzBrjjK9jcWnDVfGHlk3icNRq0oV7Ri32z/ +HQX67aRfgZu7KWdI+Ju Wm7DCfrPNGVvFWUQOmsPue9rZBgO -----END CERTIFICATE----- </pre>
<p>SSL Chain Certificate</p>	<p>If your certificate contains an intermediate certificate then paste it here. If not, leave this field blank.</p>
<p>Certificate Key</p>	<p>Private key of your certificate</p>

- 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



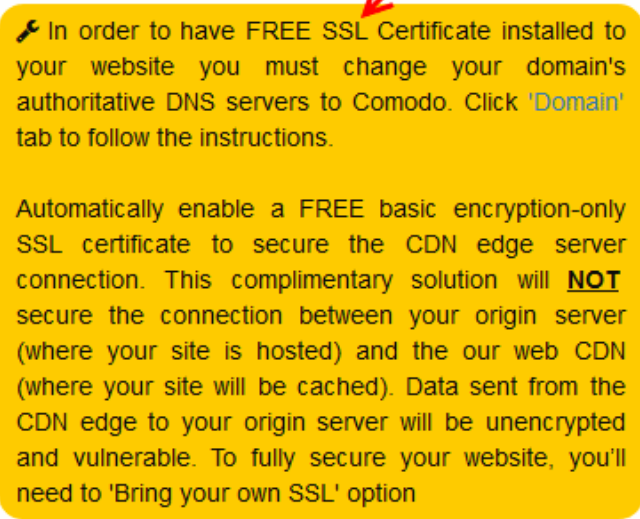
## Option A - Change your domain's authoritative DNS servers to Comodo

- 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.

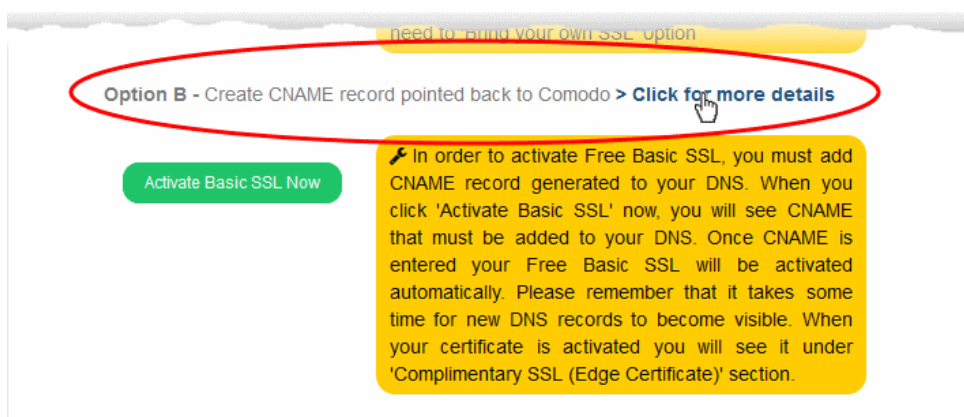
Domain	cwatchdemo.com
Expiration date	Jan 23, 2020 (365 days left)
Wildcard	No

[Uninstall](#)

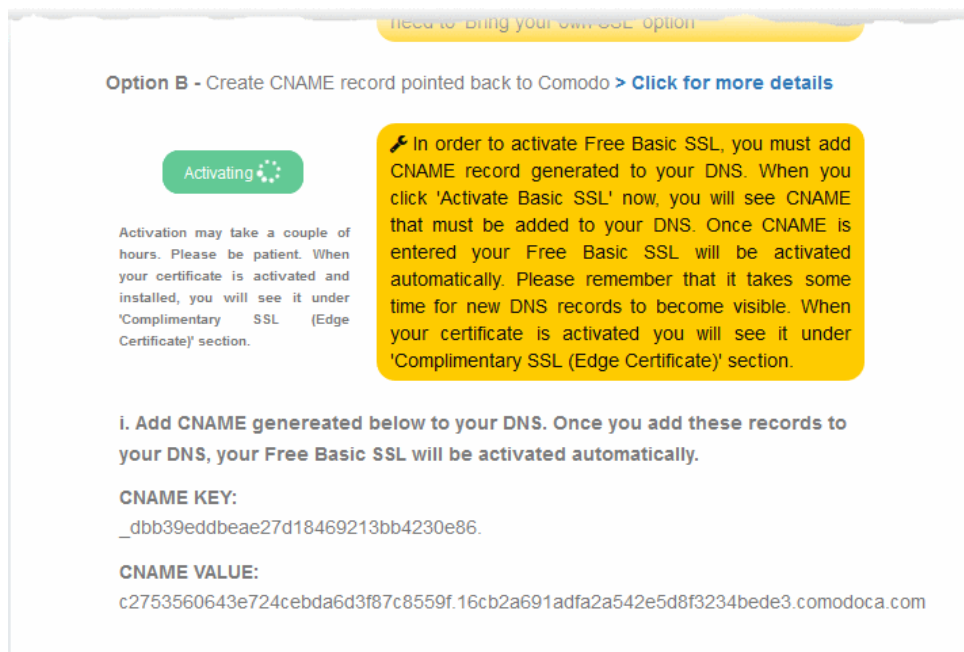
- The certificate is valid for one year and is set for auto-renewal.
- Note - This certificate encrypts the connection between the CDN servers, which host a copy of your site, and your website visitors.
- It does not encrypt the traffic between your web-server and the CDN edge servers.
- You need to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

### 4.7.4 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 (CWF) protection for your domains. The CSOC team constantly improves the Mod Security rules in the firewall to provide cutting edge protection for our customers.

#### To open the CDN Settings page

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

OR

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

- Open the 'CDN' tab

## Cache Settings

Cache Settings - Table of Parameters	
Parameter	Description
Set Default Cache Time	<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><b>Background Note:</b> Cache Control Headers are used to specify how long content fetched from site should remain in the browser's cache. The local cache is used by the browser to render the site when it is re-visited by the user, avoiding the need to fetch the content again from the server.</p>
Cache Control Header	<p>The validity period of the CCH on the end-user's web browser.</p> <p>This defines how long cached content in the web browser can be reused without checking the web server for updates.</p>
Use State	Select 'Serve expired content' if you want the CDN to deliver cached content when:

	<ul style="list-style-type: none"> <li>The CDN is currently checking the website for updated content</li> <li>Your website is down.</li> </ul>
Query String	<p>Treat as separate cachable item! - web-pages with query string parameters (e.g. '?q=something') will be cached as separate files.</p> <p>This will instruct the CDN to update cached files whenever the original pages are updated.</p>
Ignore Cache	<p>'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.</p> <p>Web browsers will use the 'Set default cache time' setting for the cache time.</p>

- 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	<p>Remove specific files from the cache so that the CDN is forced to check your website the next time the files are requested.</p> <ul style="list-style-type: none"> <li>Enter the URI of the file in the text box and click the green '+' button</li> <li>Repeat the process to add more files</li> <li>Click 'Purge'</li> </ul>
Purge All Files	<p>Remove all files from the cache so that the CDN is forced to check your website the next time the files are requested.</p> <ul style="list-style-type: none"> <li>Click 'Purge'</li> </ul>

## 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**

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

[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	Currently being developed by Google, WebP is an image format that provides both lossy

separate caching for WebP files	and lossless compression. If enabled, cWatch will have separate cache for these files.
---------------------------------	--


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

#### 4.7.5 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	<span style="background-color: green; color: white; padding: 2px 5px; font-weight: bold;">Active</span>
• 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 will be applied. Any custom firewall rules will also be disabled. See '[Configure Firewall Rules](#)' for more information.

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

#### WAF POLICIES

---

NAME	STATUS
Application DDoS Protection	<span style="background-color: green; color: white; padding: 2px 5px;">Active</span>
+ 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.

### 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.

#### 4.7.6 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:

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


## 5 The Settings Interface















- The 'Settings' interface lets you configure and manage website settings and DNS records.

### To open the 'Settings' interface

- Click the 'Settings' cog icon underneath your username

**SETTINGS**



SITE	LICENSE	SETTINGS	
cwwtest.pp.ua	Premium	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
one.bh1-cwatch.online	Basic	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
nurd.gq	Premium Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
wp.fowlercwatch.com	Pro Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
cwatchweb.ml	Pro Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
cwatch.pp.ua	Premium Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
removetest.qacww.cf	Pro Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
testmypc.com	Pro Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
whatismyipaddress.com	Basic	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
imap.nurd.gq	Basic	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
nurd.ga	Premium Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
nurd.tk	Basic	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
qacww.cf	Premium Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	
com-services-vip.testmypc.com	Basic	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>	

Settings Interface - Column Interface	
Column Header	Description
Site	Website URL.
License	Type of license associated with the website. Protection features vary according to license type. See <b>License Types</b> for a license comparison.
Settings	<ul style="list-style-type: none"> <li><b>Manage Settings</b> - Configure FTP, Malware Scan, Domain, SSL, CDN and WAF for your website(s). See <b>Website Configuration</b> more details.</li> <li><b>Manage DNS</b> - Add and manage your DNS records. See <b>Manage DNS Records</b> for more information.</li> </ul>

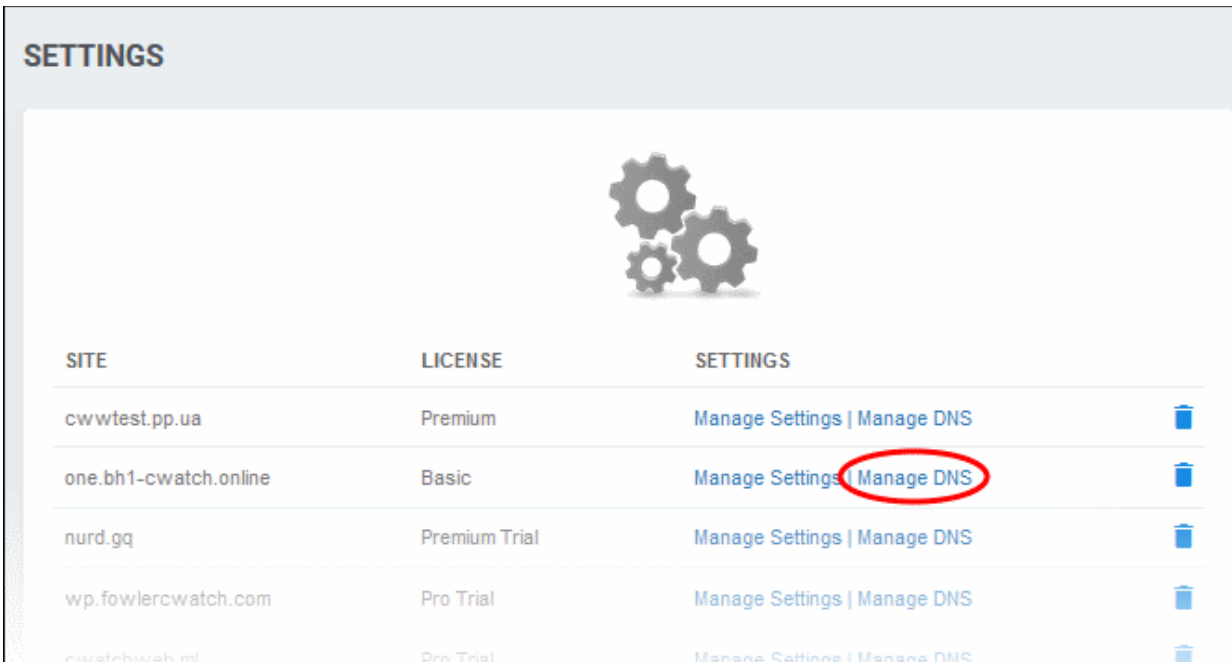
**Manage DNS Records**

You can add multiple DNS records to route traffic through the CDN service. Adding and managing DNS records is similar to what you do in your webhost's DNS management page.

- You can only manage DNS records in cWatch if your nameservers are pointed to Comodo. See '**Option A - Change your domain's authoritative DNS servers to Comodo**' for more information. Please note - this option means you will only be able to manage DNS settings in cWatch. You will not be able to manage them from your host's DNS manager.
- If you selected '**Option B - Enter DNS records explicitly**', then you must use your webhost's tools to manage your DNS records. Any updates to DNS records that you make in the cWatch interface will have no effect.

#### To manage your DNS records

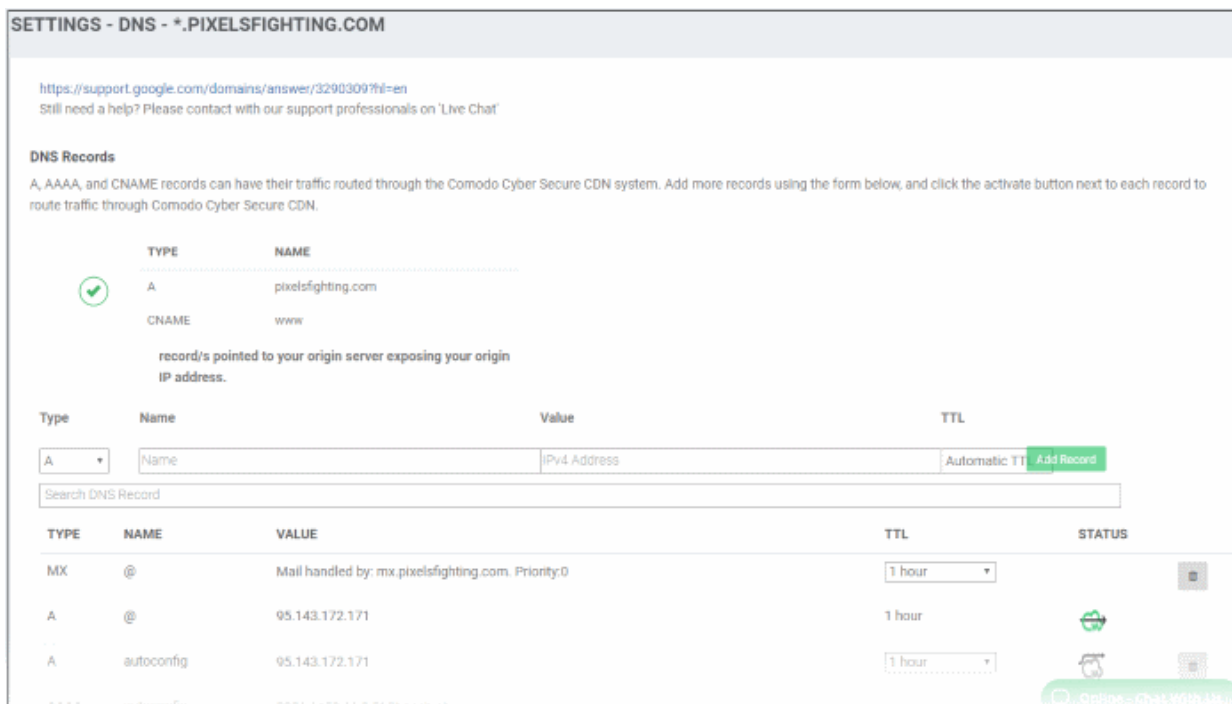
- Click the 'Settings' cog icon underneath your username
- Click 'Manage DNS' in the row of the site you want to configure:



The screenshot shows the 'SETTINGS' page in the cWatch interface. At the top, there is a gear icon representing settings. Below it is a table with three columns: 'SITE', 'LICENSE', and 'SETTINGS'. The table lists several sites with their respective licenses and links to manage settings and DNS. The 'Manage DNS' link for the site 'one.bh1-cwatch.online' is circled in red.

SITE	LICENSE	SETTINGS
cwwtest.pp.ua	Premium	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>
one.bh1-cwatch.online	Basic	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>
nurd.gq	Premium Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>
wp.fowlercwatch.com	Pro Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>
cwatchweb.ml	Pro Trial	<a href="#">Manage Settings</a>   <a href="#">Manage DNS</a>

The 'Settings - DNS' page of the selected website will open. Scroll down the page to the 'DNS Records' section:



DNS Records - Table of Parameters	
Column Header	Description
Type	DNS record type
Name	Entered name for the record
Value	Configured value for the record
TTL	Time-To-Live value for the record
Status	Indicates whether the website is protected or not. Status icon in green indicates, the site is added for protection. Please note protection is available for websites (if not enrolled already to cWatch) added for CNAME and A records.
Trash can icon	Allows you to remove a record from the list

### To add a DNS record

The procedure to add a DNS record in cWatch is similar to what you do in your regular DNS management page.

- Type - Select the DNS record type from the drop-down
- Name - Enter an appropriate name for the record
- Value - Enter an appropriate value for the record. For example if CNAME is selected, then enter the alias domain name
- TTL - Time-To-Live value for the record. Select the TTL period from the drop-down.
- Click 'Add Record' after entering the required parameters

The record will be added and displayed:

Type	Name	Value	TTL	
CNAME	Name	Domain Name	Automatic TTL	Add Record
Search DNS Record				
TYPE	NAME	VALUE	TTL	STATUS
A	@	107.180.12.116	1 hour	
CNAME	._32fd365612636e1eb143cf9fea820cdc	dc9028559014ad778876a41a7abdc7b7.2980bf9e4e332d68765	1 hour	
CNAME	._b57d2ac29fc0992f4320e0c8a7a92874	bd5efd28815926a79588846c08ff1e30.f05fa150f95120c17109ft	1 hour	
A	subdomain	107.180.12.116	Automatic TTL	
A	www	107.180.12.116	1 hour	

You can enable protection for a site after adding the DNS record. See below more on this.

- See <https://support.google.com/domains/answer/3290309?hl=en> if you need more help on changing nameservers

### Configure cWatch protection for a site

- Click the icon beside the DNS record
- If the website is licensed then the protection starts after you click the icon.
- If not licensed then the 'Add Website' wizard will start.

The website name pre-populated. The wizard starts at 'Step 2- Select License'.

- The drop-down menu lists any unused licenses you have on your account. You can apply one of these licenses if available.
- Click 'Buy a license' if you don't have any existing licenses. [Click here](#) if you need help with the order form.

**ADD WEBSITES**
✕

1  
**Add Website**

2  
**Select License**

3  
**Site Provisioning In Progress**

**Step 2 - Select License**

Site will be added with selected license type

Pro (1 Site / 31 days left)
▾

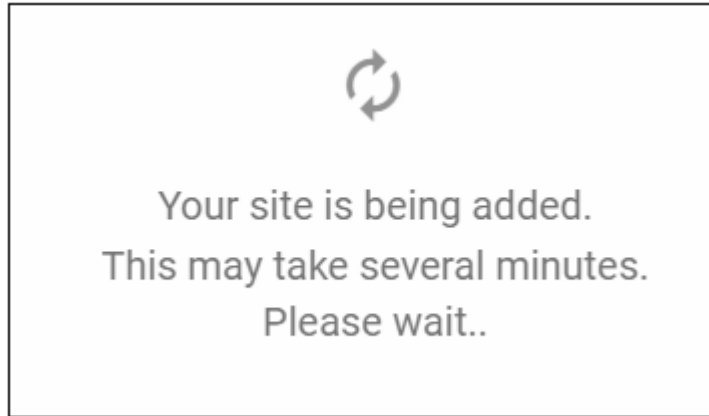
[Learn more](#)

← Back

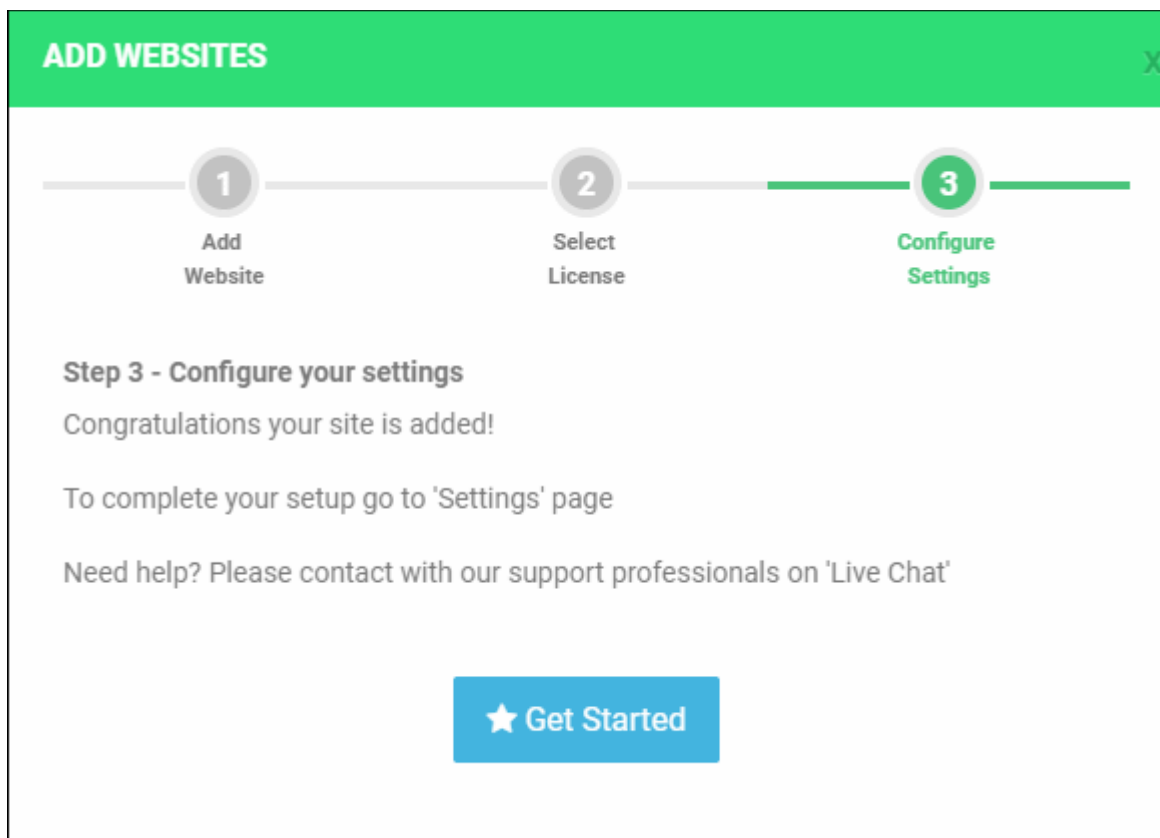
→ Finish

- Click 'Finish' to apply the license

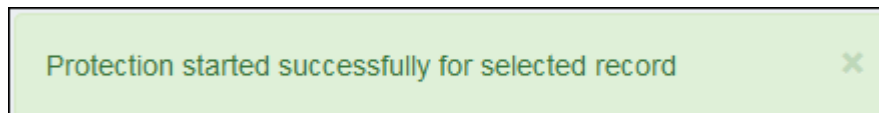





- cWatch will validate your request then show the following confirmation message:



- Click 'Get Started' to activate cWatch protection on your site:



- A green cWatch icon is shown next to protected sites - 
- If you do not have any licenses available then you will be asked to purchase a license:

## ADD WEBSITES X

1 Add Website

2 Select License

3 Site Provisioning In Progress

You don't have license to register new domains. Click to buy a license.

[Buy a License](#)

[← Back](#) [→ Finish](#)

- Click 'Buy a License'.
- You will be taken to the license order form:

COMODO | Creating Trust Online™
 Need Assistance?  
888-351-7956
CHAT NOW!

### cWatch Web Security - Pro PAID (1 Domain)

Please select license period :

cWatch Web Security - Pro PAID (1 Domain) ▾

Monthly  
  1 year  
  2 years  
  3 years

Domains :  \$ 9.90

TOTAL : \$ 9.90

### ENTER CUSTOMER DETAILS

Existing Comodo User

New Comodo User

[Register a new Comodo account with your e-mail address.](#)

E-mail address \* :

### PAYMENT DETAILS

Cardholder Name \* :

Credit Card No. \* :

CVV \* :

Expiration Date \* :  /

Satisfaction Guaranteed,  
No Questions Asked \*

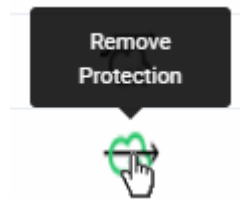
I have read and agree to the [End User license/Service Agreement](#)

Continue »

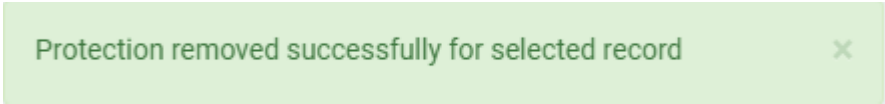
- Select the license you want from the drop-down. See **License Types** for more details about the features of each license.
- Choose the license period.
- Select 'Existing Comodo User' and enter your username and password.
- Complete the payment details section.
- Read the 'End User License/Subscriber Agreement' and tick the checkbox to agree.
- Click 'Continue'. After your order has been successfully processed, you will see the order confirmation screen.
- The new license is added to your account and can be applied to the site in cWatch.

### To remove protection from a site

- Click the icon in the status column beside the record

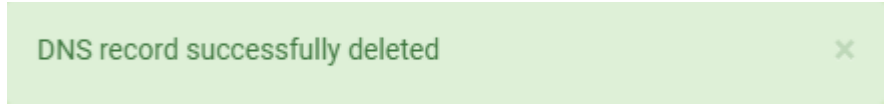


A success message will be displayed:



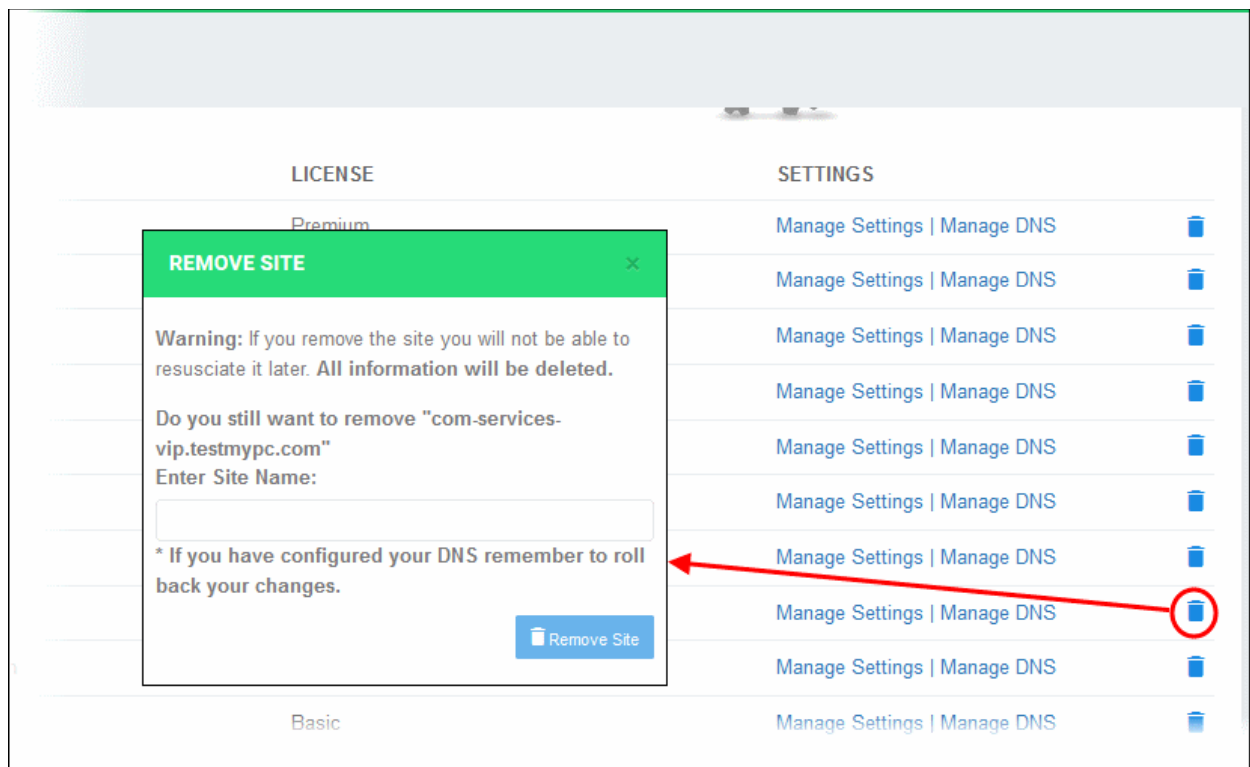
### To remove a DNS record

- Please note you can remove a record that is not cWatch protected
- Click the trash can icon beside a record
- A success message will be displayed:



### To remove a website from cWatch protection

- Click the gear icon on the left to open the 'Settings' interface
- Click the trash can icon in the row of the website you want to delete:



- Enter the website name in the field for confirmation and click 'Remove Site'

**Note:**

- Removing a website will remove its data from cWatch and revert the DNS settings. Its traffic will no longer be routed through the CDN.
- The license used for the website will become available for adding a new website.

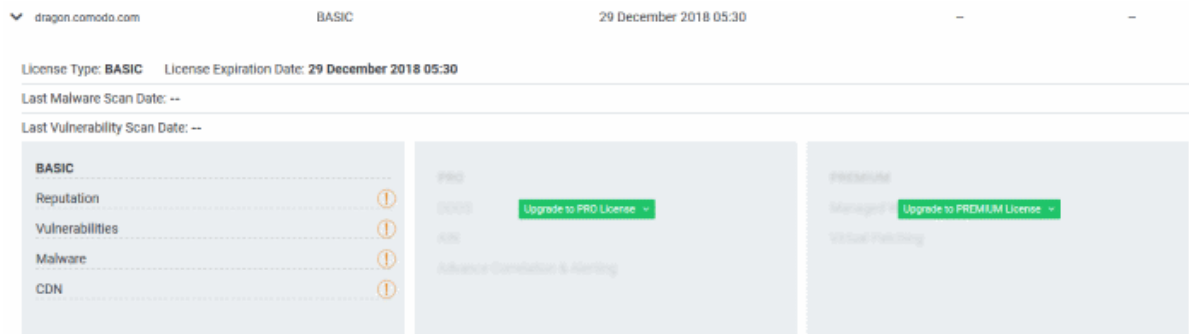
## 6 Upgrade Licenses for Domains

You may want to upgrade your cWatch license if:

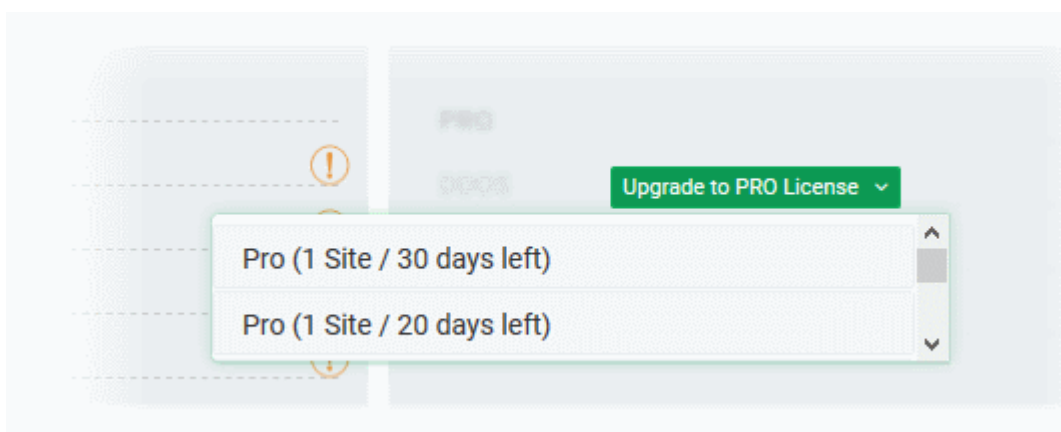
- You wish to enable the superior protection features afforded by a Pro or Premium license
- You want to add sub-domains for a website

**To upgrade your license**

- Click 'Dashboard' then click the name of the site you want to upgrade
- Click the 'Upgrade to Pro License' or 'Upgrade to Premium License':



- Choose the license specs you want from the drop-down:



- Click 'Yes' to apply the upgrade:

**DO YOU CONFIRM?** X

License of dragon.comodo.com will be upgraded

NO

YES


If you do not have any licenses available then you will be taken to the license purchase page:

1  
Select a plan

2  
Process Payment

3  
Finish

X



Premium

Pro

1  
Month

12  
Months

24  
Months

36  
Months

**\$24.90**  
-month-

**\$9.90**  
-month-

### Enable your protection plan.

Malware detection and removal	✓	✓
Security information and event management	✓	✓
24 / 7 / 365 Cybersecurity Ops Analysts	✓	✗
Managed web application firewall	✓	✗
Content delivery network	✓	✓
Technical support	✓	✓
30 days money back guarantee	✓	✓

Continue

- Select the license period and type. See [License Types](#) for more details on the features of each license.
- Click 'Continue'

X


1  
Select a plan

2  
Process Payment

3  
Finish

### Payment Profile ^

Card Number

# 

MM v

YYYY v

CVC

Cardholder Name Total License Period

Name displayed on card

USD\$24.90

Monthly


Please read and accept [End User License/Service Agreement](#)

### Order Summary

<b>\$24.90 / Monthly / PREMIUM plan / dragon.comodo.com</b>	Subtotal
	\$24.90
	Savings
	\$0.00
	Total
	\$24.90

### Billing Address ^

<u>Company Name</u>	<u>Phone Number</u>
<u>Address</u>	<u>Address 2</u>
<u>City</u>	<u>State</u>
<u>Country</u>	<u>Postal Code</u>

I'm not a robot   
reCAPTCHA  
Privacy - Terms

Process Payment


- Complete the payment details section
- Read the 'End User License/Subscriber Agreement' and tick the checkbox to agree
- Enter your billing address
- Complete the captcha verification and click 'Process Payment'

1  
Select a plan

2  
Process Payment


3  
Finish

X


Need help? [Contact Support](#)

**You paid \$24.90 USD** to license your account.

<b>1 x PREMIUM Licenses</b>	<b>\$24.90 USD</b>
<b>Discount</b>	<b>\$0.00 USD</b>
<b>Domain:</b> dragon.comodo.com	
<b>Subscription:</b> Monthly	
<hr/>	
<b>Total</b>	<b>\$24.90 USD</b>
<hr/>	


 You'll receive an order checkout confirmation by email to [cwdemo@cwdemo.com](mailto:cwdemo@cwdemo.com).

---

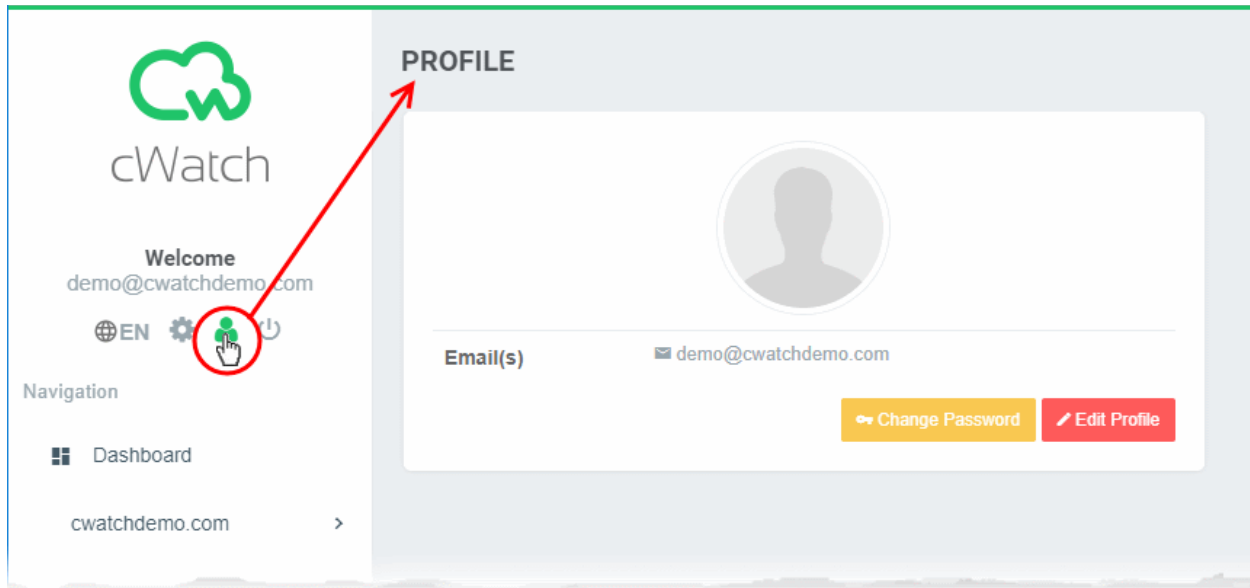
This transaction will appear on your statement as Comodo Security Solutions, Inc.

- The license for the domain will be upgraded to the selected license type
- You will also receive a order confirmation email.

## 7 Manage Your Profile

- The 'Profile' interface lets you view and edit personal information and notification preferences.
- You can also change your password for cWatch and Comodo Account Manager (<https://accounts.comodo.com>).
- Click the  icon to open the profile screen:



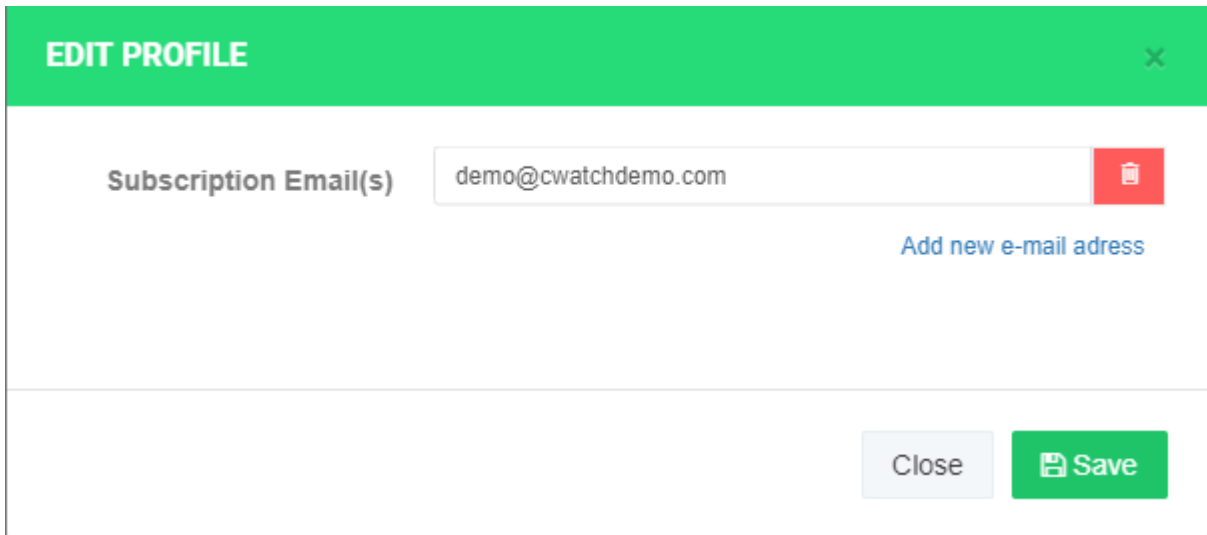


The "Profile interface lets you:

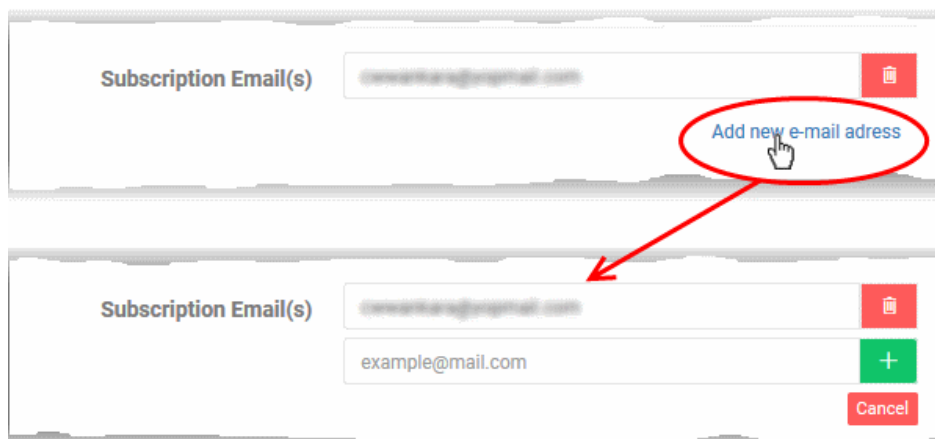
- **Edit your profile**
- **Change your password**


**Edit your profile**

- Click  in the left-hand navigation
- Click 'Edit Profile'





- **Subscription Email(s)** - The email address you entered during sign-up.
  - All alerts, account and license emails are sent to this address.
  - You edit this address, and/or add more addresses to receive these mails.
    - Click 'Add new e-mail address' to add an alternative address:



Subscription Email(s)  

[Add new e-mail address](#)


Subscription Email(s)  



You will get system emails for the following:

- Account Creation
  - Purchase cWatch Web
  - Malware Found
  - When license is expired
  - When a license is distributed for the first time
  - When a license is distributed by partner
  - When license is expired
  - When a license is distributed by partner
  - When a license is purchased or distributed to customer by partner
- Click 'Save' for your changes to take effect.

#### To change your password

- Click  in the left-hand navigation
- Click the 'Change Password' button

### CHANGE PASSWORD

Please keep in mind that after changing your password here, you will be using your new password to access Comodo Account Management (CAM) system as well.

**Current Password**

**New Password**

**Confirm New Password**

- Enter your old password, new password and re-enter your new password in the respective fields
- Click 'Change Password'

You can use the new password to login to both cWatch and Comodo Accounts Manager.

## 8 Get Support

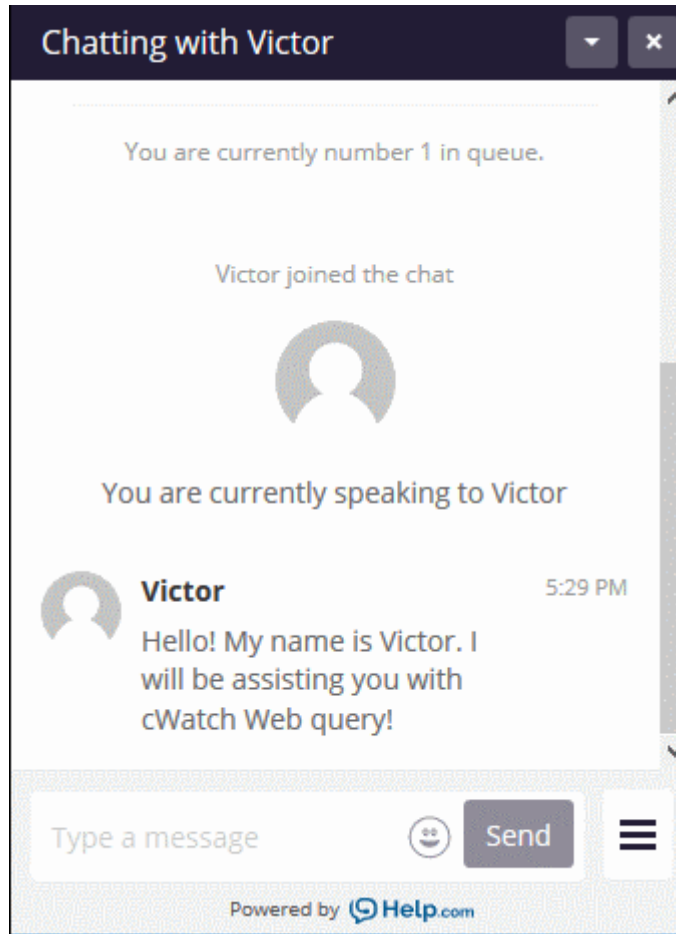
- cWatch live chat support is the fastest way to get help to configure your domains.
- Support chat is included with all cWatch license types, including the free 'Basic' license.
- Click 'Online - Chat with us' at the bottom-right of the interface to chat with a Comodo support technician.

### Launch a chat session

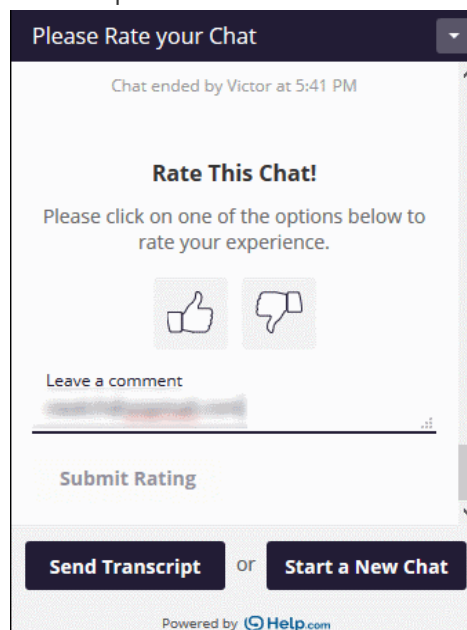
- Click the 'Chat with us button' at the bottom right of the cWatch interface.
- Enter your name and email address in the respective fields
- Type your message
- Click 'Start chat':

The image shows a screenshot of the 'Online - Chat With Us' form. The form has a dark header with the title 'Online - Chat With Us' and a dropdown arrow. Below the header, there is a welcome message: 'Welcome to Live Chat. Please enter the information below to chat with a representative.' The form contains three input fields: 'Your Name', 'Your Email', and 'Your Message'. Below the 'Your Message' field is a dark blue button labeled 'Start chat'. At the bottom of the form, it says 'Powered by Help.com'. Below the form, there is a partial view of the cWatch interface showing a chat button labeled 'Online - Chat With Us' which is circled in red. A red arrow points from this button up to the 'Start chat' button in the form above.

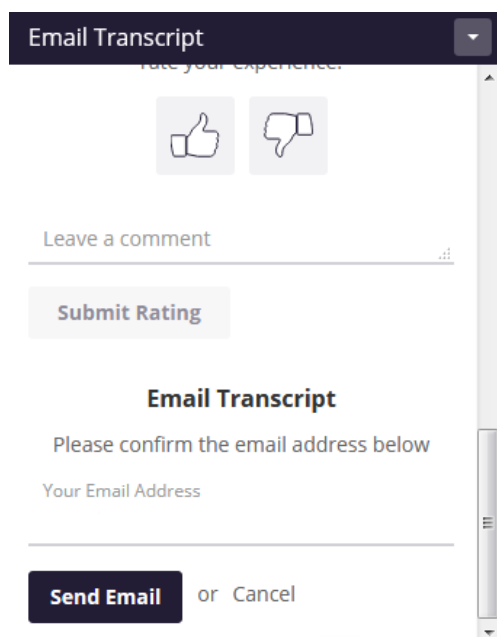
Within seconds, a Comodo Support Technician will respond in a chat window and ask you to describe the problem.



- Start chatting! Use the chat window to explain any problems you are having. The technician will offer advice accordingly.
- End the chat - click the hamburger icon at bottom-right and choose 'End Chat'
- You are given the option to save the chat for future reference.
  - Click 'Send Transcript':



- Confirm the email address where you want to receive the script.



Email Transcript

Like your experience.

Leave a comment

Submit Rating

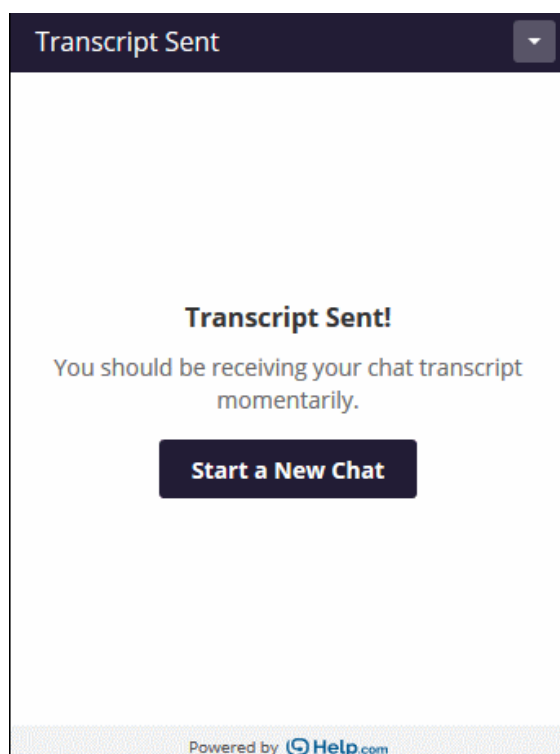
**Email Transcript**

Please confirm the email address below

Your Email Address

Send Email or Cancel

- Click 'Send Email'



Transcript Sent

**Transcript Sent!**

You should be receiving your chat transcript momentarily.

Start a New Chat

Powered by Help.com

You will receive the chat history at the specified email address.

# 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 : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)