

**COMODO**  
CYBERSECURITY



**Comodo**  
**cWatch Web Security**  
Software Version 5.4

**Website Administrator Guide**

Guide Version 5.4.082019

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

## Table of Contents

1 Introduction to Comodo cWatch Web Security.....	4
1.1 Purchase a License.....	6
1.2 License Types.....	20
1.3 Login to the Admin Console.....	20
1.4 Add Websites.....	24
2 The Main Interface.....	29
3 The Dashboard.....	32
4 Website Data and Settings.....	33
4.1 Website Overview.....	35
4.2 Security Scans.....	38
4.2.1 Remote Scans.....	39
4.2.1.1 Run Remote Scans and View Results.....	41
4.2.2 Malware Scans.....	45
4.2.2.1 Configure Malware Scan Settings.....	46
4.2.2.1.1 Automatic Configuration.....	47
4.2.2.1.2 Manual Configuration.....	49
4.2.2.2 Run Malware Scans and View Results.....	50
4.2.2.3 Configure Notifications and Automatic Malware Removal.....	61
4.2.3 Vulnerability Scans .....	63
4.2.3.1 CMS Vulnerability Scans.....	64
4.2.3.2 OWASP Top 10 Vulnerability Scans.....	70
4.3 Cyber Security Operation Center Results.....	77
4.3.1 WAF Statistics.....	78
4.3.2 WAF Events.....	82
4.4 Content Delivery Network.....	85
4.4.1 Activate CDN for a Website.....	86
4.4.2 Configure CDN Settings.....	91
4.4.3 View CDN Metrics.....	96
4.5 Firewall Rules.....	102
4.5.1 Configure WAF Policies.....	103
4.5.2 Manage Custom Firewall Rules.....	106
4.6 SSL Configuration.....	112
4.7 DNS Configuration.....	122
4.8 Add Trust Seal to your Websites.....	133
4.9 Back up your Website.....	135
4.9.1 Purchase a Backup License.....	137
4.9.2 Configure Backup Settings.....	139
4.9.3 On-Demand Backup.....	145
4.9.4 View Backup Records and File Statistics.....	146
4.9.5 Restore and Download Website Files .....	149
5 View and Upgrade Licenses for Domains.....	154

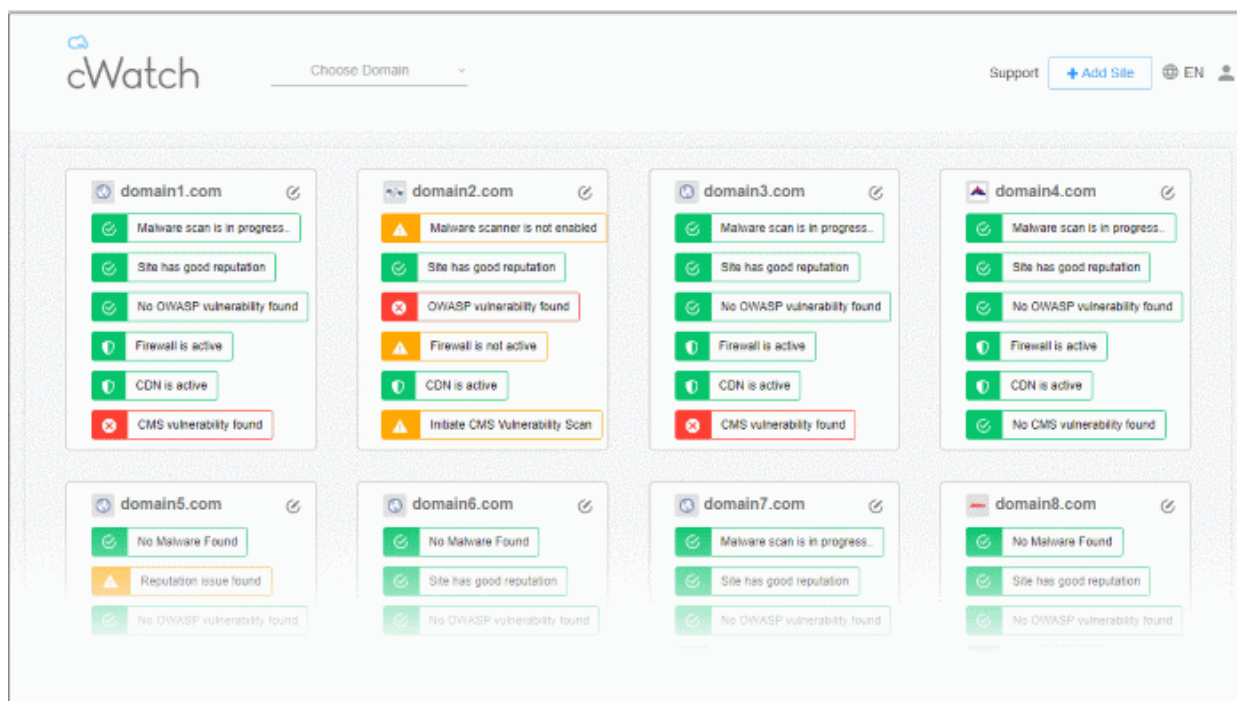
<b>6 Manage Your Profile.....</b>	<b>160</b>
<b>7 Get Support.....</b>	<b>164</b>
<b>About Comodo Security Solutions.....</b>	<b>169</b>

# 1 Introduction to Comodo cWatch Web Security

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

- cWatch runs regular malware scans on your domains and automatically removes any malware. The content delivery network (CDN) accelerates site performance by delivering your web content from data centers near your visitors.
- The service constantly logs events on your domains to identify new attack vectors. These logs allow the Comodo cyber-security team (CSOC) to create new 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 scans for the top 10 OWASP threats and known CMS vulnerabilities. The 'Remote Scan' gives you an immediate heads-up on errors on your front-end pages.
- The backup service lets you copy your entire website and databases to our highly secure servers. An essential disaster-recovery service, cWatch Backup lets you restore your site in a single click.

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



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**
  - **Security Scans**
    - **Remote Scans**
      - **Run Remote Scans and View Results**
    - **Malware Scans**
      - **Configure Malware Scan Settings**
      - **Run Malware Scans and View Results**
    - **Vulnerability Scans**
      - **CMS Vulnerability Scans**
      - **OWASP Top 10 Vulnerability Scans**
  - **Cyber Security Operation Center Results**
    - **WAF Statistics**
    - **WAF Events**
  - **Content Delivery Network**
    - **Activate CDN for a Website**
    - **Configure CDN Settings**
    - **View CDN Metrics**
  - **Firewall Rules**
    - **Configure WAF Policies**
    - **Manage Custom Firewall Rules**
  - **SSL Configuration**
  - **DNS Configuration**
  - **Add Trust Seal to your Websites**
  - **Back up your Website**
    - **Subscribe for a Backup License**
    - **Configure Backup Settings**
    - **On-Demand Backup**
    - **View Backup Records and File Statistics**
    - **Restore and Download Website Files**
- **View and Upgrade Licenses for Domains**
- **Manage Your Profile**
- **Get Support**

## 1.1 Purchase a License

Three types of cWatch license are available:

- Basic
- Pro
- Premium

See **License Types** for details on the differences between licenses.

### General notes

- You can purchase licenses from the cWatch website <https://cwatch.comodo.com/plans.php>. You can also purchase them from within the cWatch console after creating an account.
- Licenses are charged per-website. Sub-domains are not covered if you buy a license for a primary domain, like example.com. You must purchase separate licenses for each sub-domain.
- You can add multiple license types to your account if you want to implement different protection levels on different sites.
- You can associate websites with licenses in the cWatch interface. See **Add Websites** for more details.
- You can only purchase backup licenses after you have purchased a cWatch license. See **'Purchase a Backup License'** if you need help with this.
- cWatch licenses are also distributed by Comodo partners. Contact your Comodo account manager for 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><b>Most Popular</b></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

Own Multiple Domains?

- Choose whether you want single domain license or multi-domain license.
  - **Purchase single domain license** - Enter your domain name (without www.) and click 'Continue' to buy a license for one website. See **Purchase single domain license** if you need further help.
  - **Purchase multi-domain licenses** - Purchase licenses for more than one website. See **Purchase multi-domain licenses** for more details.

### Purchase single domain license

#### Step 1 - Enter your domain name

### ADD SECURITY TO YOUR WEBSITE

Website

- 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'



## EXISTING USER

Email

Password [Forgot your password](#)

**SIGN IN**

————— New to cWatch? —————

**CREATE YOUR ACCOUNT**

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

### Step 3 - Select License Type

1 — 2 — 3 — 4

Add Site    Account Info    Checkout    Activate

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

### 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

DISPLAYED ON CARD

Card Number

0000-0000-0000-0000

Expiration

MM/YYYY

Security Code

000

Currency

▼

**BILLING INFO**

Address

0000 PARK STREET

Country

▼

State

City

CLIFTON

Postal Code

0000-0000

**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

1

Add Site

2

Account Info

3

Checkout

4

Activate



## 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 you invoice »](#)



- Click 'Activate cWatch' to start protecting your website
  - You need to upload the cWatch scanner agent to your site to enable malware scans.
  - There are two ways to do this:
    - **Automatic** - Provide FTP details for your site and cWatch will automatically upload the file.
    - **Manual** - Download the agent and copy it to your site. See **Malware Scans** for help with this.



+1(844) 260-2204

### SHARE FTP SETTINGS

Host

Type  Port

Username

Password

Directory

## Activate cWatch Website Security

Your cWatch Website Security account and license is read This gives us the ability to use cWatch Web comprehensive scanners within your website root directory for a complete scan.

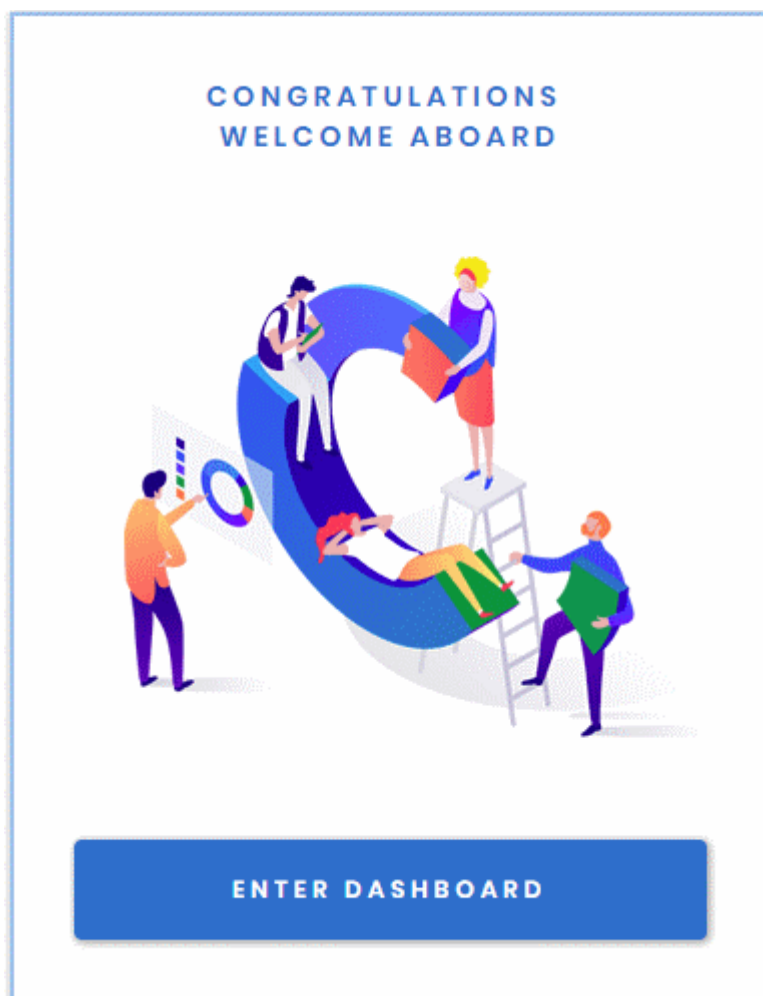
TEST CONNECTION

If you don't remember your FTP settings, don't worry!  
Skip this step and you can always share FTP settings later  
in dashboard

SKIP



- Enter the hostname, login details and upload directory. The location must be publicly accessible.
- Click 'Test Connection' for cWatch to check whether it can reach the location.
  - Note. Our technicians will also use these settings to access your site IF you request them to remove malware.
- Click 'Skip' If you want to configure your malware scan settings at a later time.



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 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:

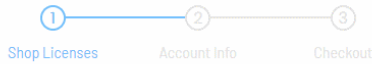
Comodo Security Solutions, Inc., with its principal place of business at 1255 Broad Street, Suite 100, Clifton, New Jersey 07013, United States, or

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 the 'Pro' and/or 'Premium' boxes.
- Each license covers one domain or 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

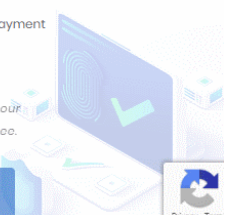
**Subtotal**  
**\$348.90** per year

**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



## 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

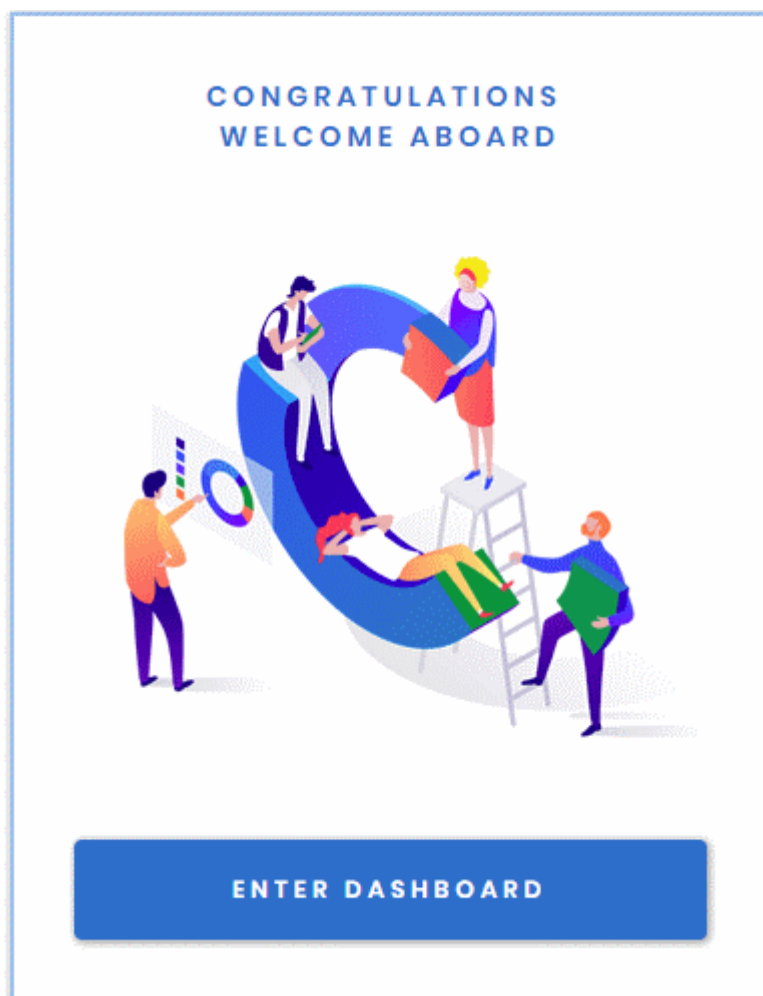
#### Total

**\$348.90** year recurring payment

[Download your invoice »](#)



- Click 'Activate cWatch' to start protecting your website



Your license is now active.

- Click 'Enter Dashboard' to login to cWatch

A screenshot of the cWatch website's login page. The top of the page features the cWatch logo in a light gray header. Below the logo, the text "SIGN IN" is centered in a bold, black, sans-serif font. Underneath, there are two white input fields with gray borders: the first is labeled "Username" and the second is labeled "Password". Below these fields is a prominent blue button with the white text "Log In". At the bottom of the login section, there is a small lock icon followed by the text "Forgot your password?". At the very bottom of the page, in a light gray footer, it says "Don't have an account? Sign Up" where "Sign Up" is a blue link.

- Use your Comodo 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

Each cWatch license offers different levels of monitoring, protection and content-delivery service (CDN).

The three license types are:

- Basic
- Pro
- Premium

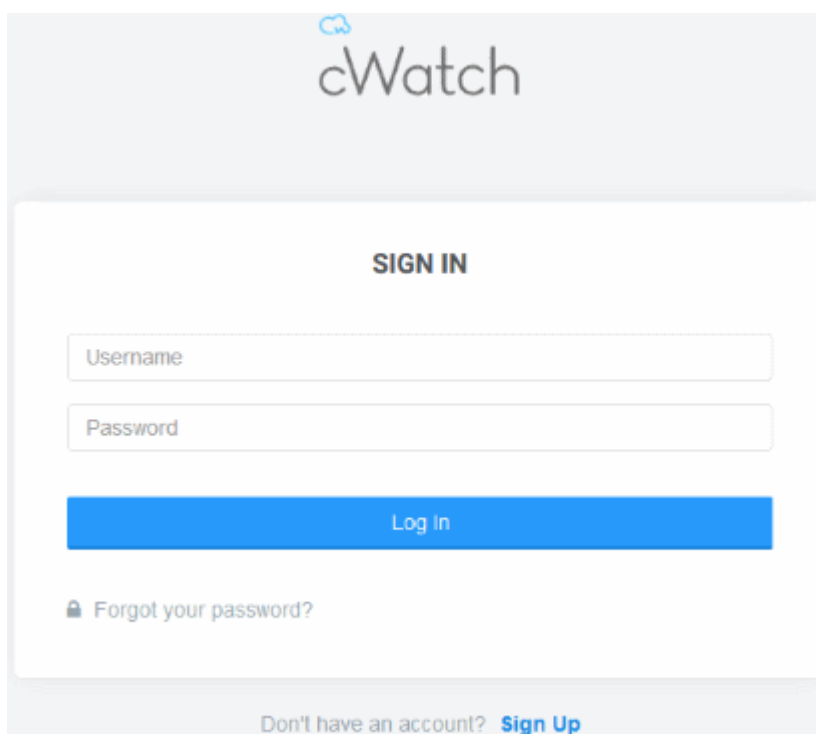
The following table shows the features available with each license type:

Feature/Service	Premium	Pro	Basic
Malware removal by experts Hack repair and restore Vulnerability repair and restore Traffic hijack recovery SEO/Search poisoning recovery	Unlimited	Unlimited	One time
Automatic Malware Removal	✓	✓	✗
Spam & Website Filtering	✓	✓	✗
Malware Scan	Every 6 hours	Every 12 hours	Every 24 hours
Vulnerability (OWASP) Detection	Every 6 hours	Every 12 hours	Every 24 hours
Security Information and Event Management (SIEM)	✓	✓	✗
<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	✓	✓	✓

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

## 1.3 Login to the Admin Console

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



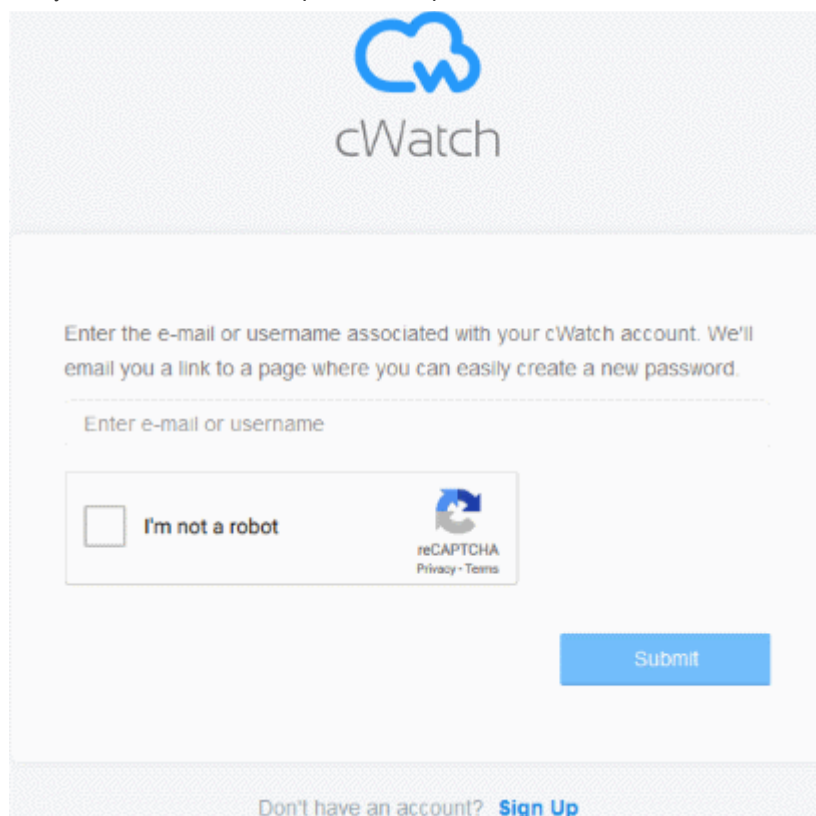
The image shows the cWatch Sign In page. At the top is the cWatch logo. Below it is a white box with a blue border containing the text "SIGN IN". There are two input fields: "Username" and "Password". Below these is a blue "Log In" button. At the bottom of the white box is a link "Forgot your password?". Below the white box is a grey footer with the text "Don't have an account? Sign Up".

#### First time login

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




#### Forgotten password?

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



The image shows the cWatch Password Reset page. At the top is the cWatch logo. Below it is a white box with a blue border containing the text "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." Below this is an input field labeled "Enter e-mail or username". Below the input field is a reCAPTCHA widget with the text "I'm not a robot" and a "Submit" button. At the bottom of the white box is a grey footer with the text "Don't have an account? Sign Up".

- You will receive a password reset mail:

 • **do-not-reply@comodo.com** <do-not-reply@comodo.com>  20 Mar at 2:27 pm   
To: admin@company.com

## Password Reset Request

Dear Customer:

We have received a Password Reset request for the account with the login specified below. To confirm that you made this request and to complete the reset process, please click the login link below:

Login	Click Option Below
admin@company.com	<a href="#">Reset Password</a>

If you did not make this request and/or do not wish to change your password at this time then please ignore this email. If you have any further questions, please forward this email to [subscriptions@comodo.com](mailto:subscriptions@comodo.com)

Thank you for allowing us to serve you.

Sincerely,


Comodo Security Solutions  
[www.comodo.com](http://www.comodo.com)

1255 Broad Street STE 100  
Clifton, NJ 07013  
United States

---

We suggest that you review our [Privacy Policy](#) and keep a copy of this e-mail for your records.

- Click 'Reset Password' to open the password creation page.
- Enter a password and confirm it:



cWatch


Please enter a new password in the fields below.

**New Password**

**Confirm New Password**

[Create Password](#) [Cancel](#)

- Click 'Create Password'



cWatch

Your password has been changed successfully!

[Go to Login](#)

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

## 1.4 Add Websites

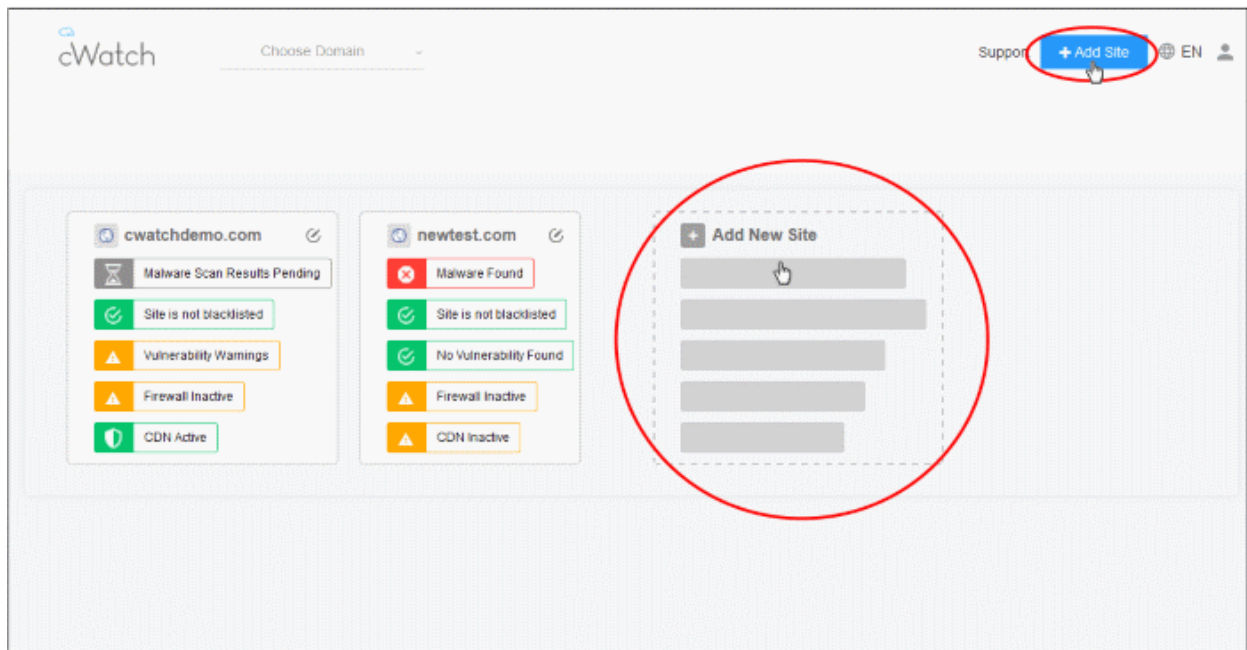
- You need to add websites to cWatch to enable protection and to use the content delivery network (CDN).
- The number of sites you can add depends on your license. See **License Types** more info.
- Once added, you can configure threat monitoring and CDN settings for each site.

### Add a new domain

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

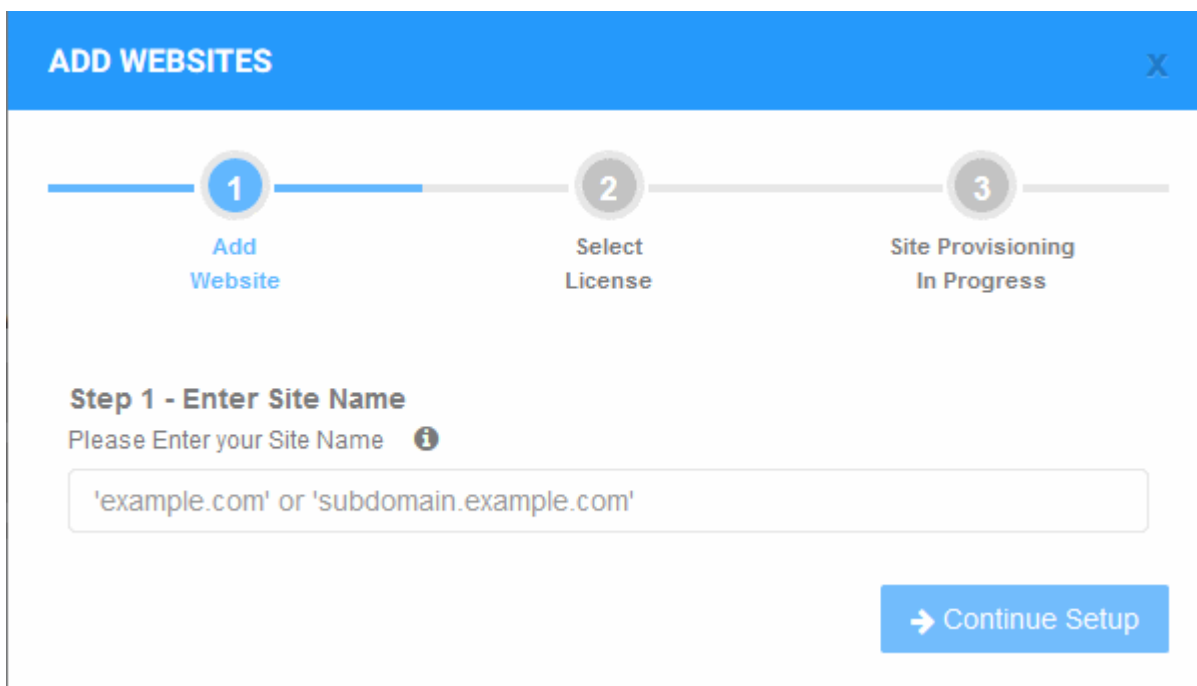
The dashboard shows all protected websites as a tile. Each tile provides an at-a-glance summary of any problems on the site.

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



The 'Add Websites' wizard starts:





**ADD WEBSITES** X

1 Add Website | 2 Select License | 3 Site Provisioning In Progress

**Step 1 - Enter Site Name**  
Please Enter your Site Name ⓘ

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

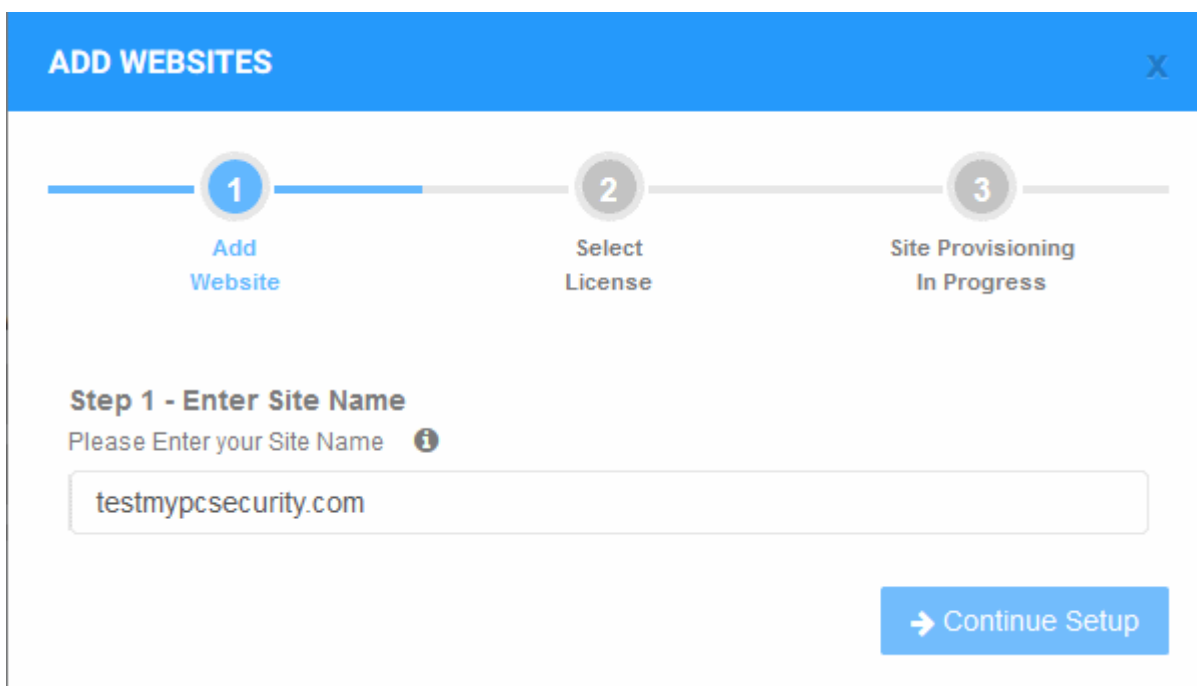
→ Continue Setup

The wizard has three steps:

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

### Step 1 - Register your website

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



**ADD WEBSITES** X

1 Add Website | 2 Select License | 3 Site Provisioning In Progress

**Step 1 - Enter Site Name**  
Please Enter your Site Name ⓘ

testmypcsecurity.com

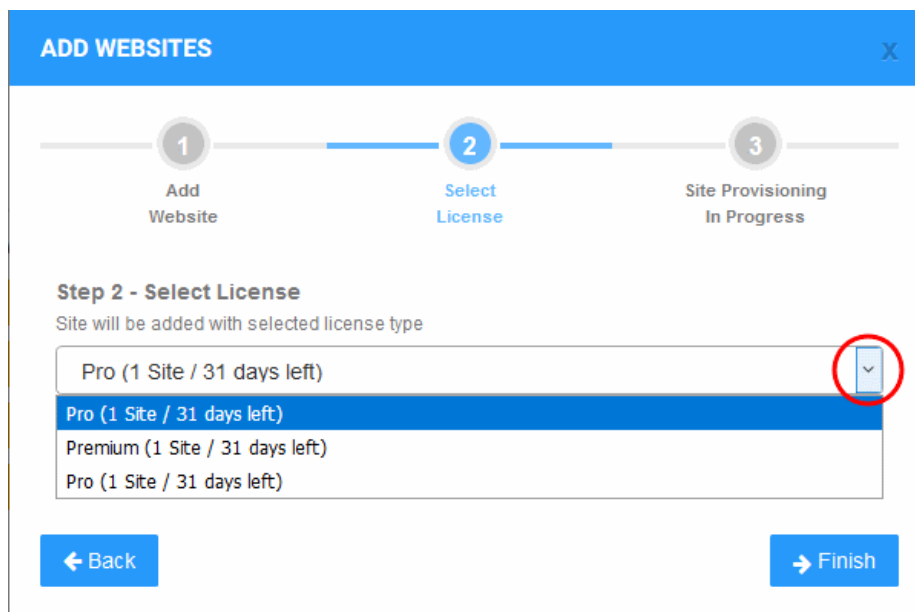
→ Continue Setup

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

### Step 2 - Select License

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

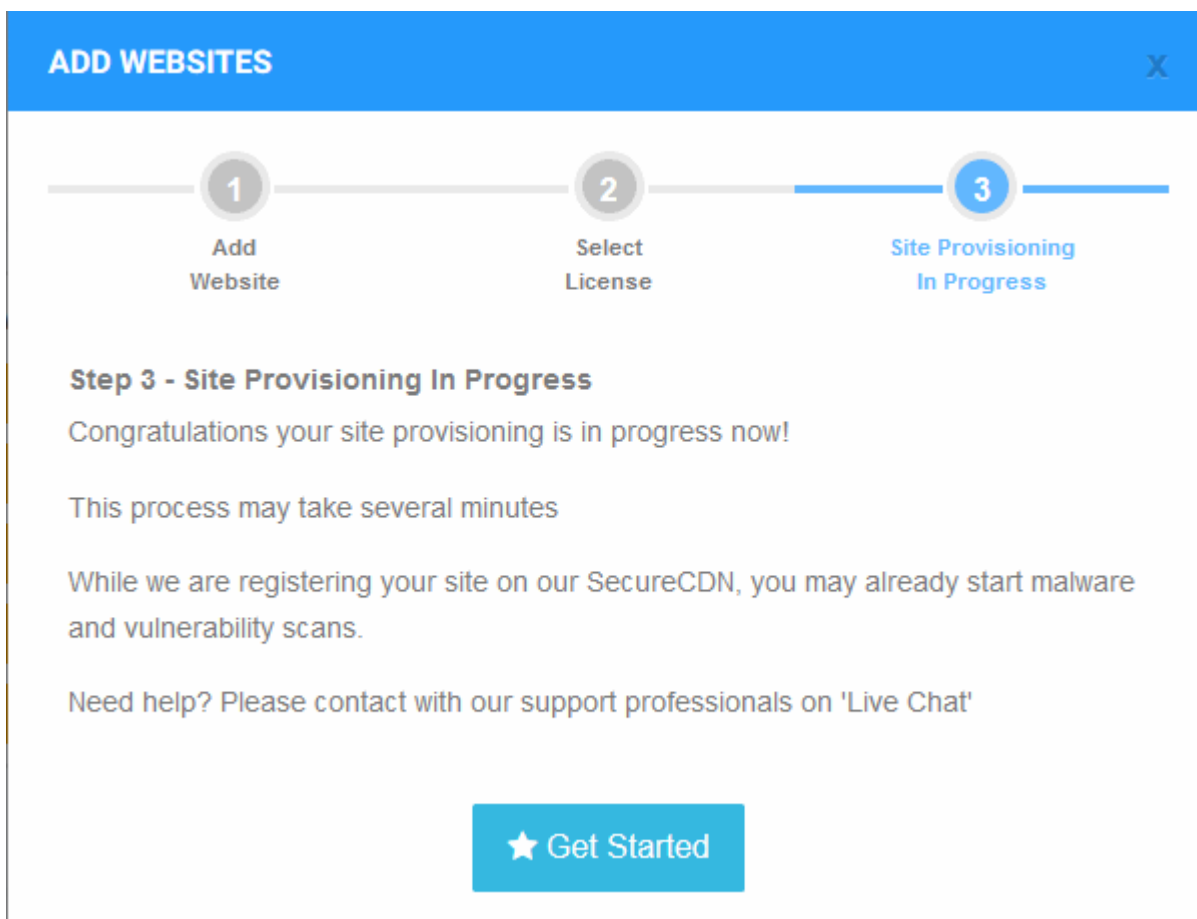
- cWatch features vary according to license type. See **License Types** for more details.
- The drop-down menu lets you select from all licenses you have purchased.
- Choose the type of license you wish to associate with the domain:



- Click 'Finish' to proceed
- See **Purchase a License** if you need help to buy more licenses

### Step 3 - Finalization

The final stage is for cWatch to provision your site:



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

A light green rectangular box with a thin black border. Inside, the text "Your site is registered successfully" is written in a dark green font. A small green 'x' icon is located in the top right corner of the box, indicating it is a notification or alert.

Your site is registered successfully

- Next up is to enable cWatch protection on the site.
- Click 'Get Started' to open the 'Overview' page for the website
- The overview page lets you configure malware and vulnerability scans, firewall rules, CDN settings, and more.
- This is covered in more detail in the **Website Overview** section.

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

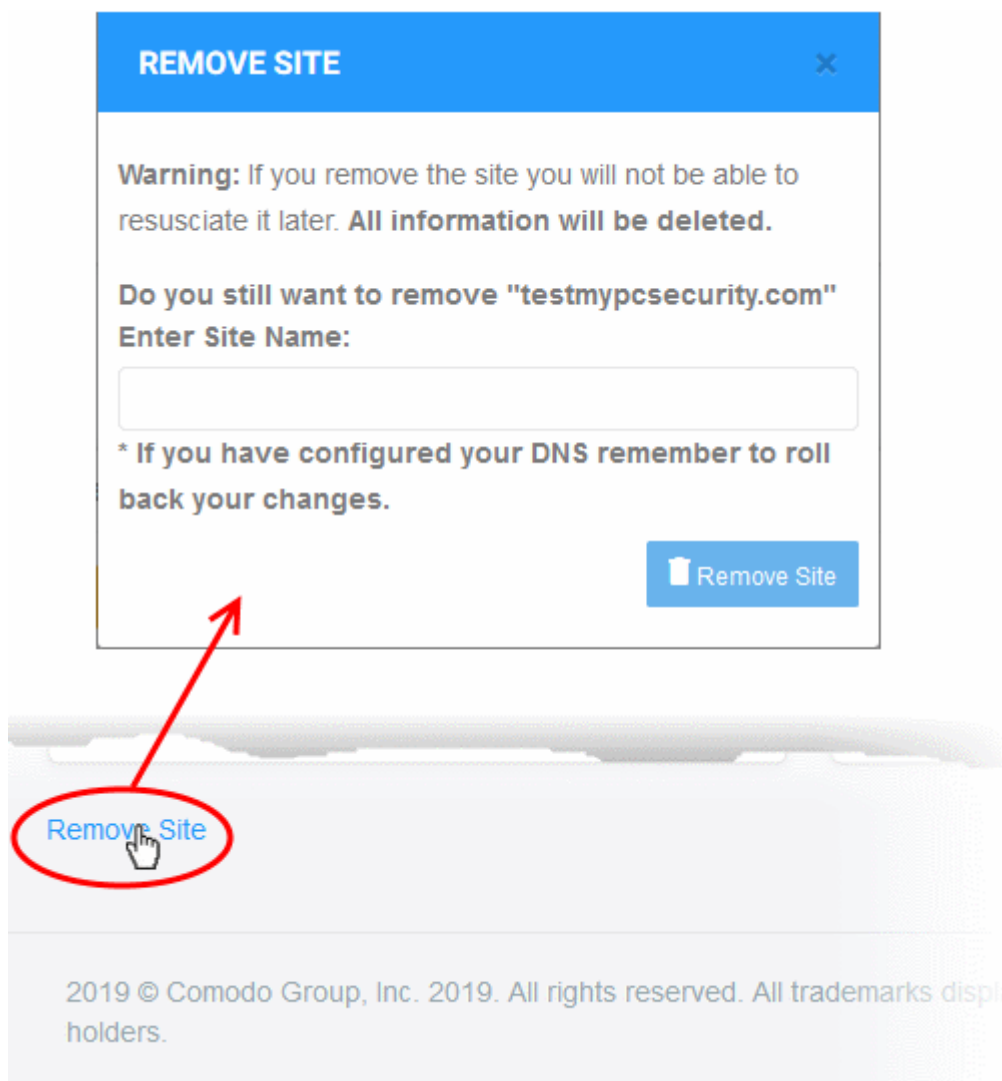
**Tip:** You can skip this step for now and add the CNAME to DNS later. See **DNS Configuration** for help with this.

- Repeat the process to add more websites.

**Remove Websites**

You can remove any site that you no longer want to protect with cWatch.

- Select the website from the drop-down at top-left of the dashboard
- Click the 'Overview' tab (or click the hamburger button and select "Overview")
- Click 'Remove Site' at the bottom-left of the interface:



A warning message is shown.

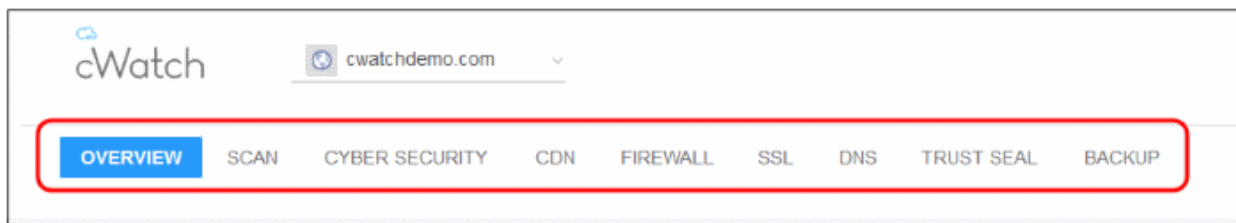
- Enter the URL of the site you want to delete. For example, my-website.com
- Click 'Remove Site'.

**Note:**

- Removing a website will delete all its data from cWatch. The site's traffic will no longer be routed through the CDN.
- You should manually revert the name servers in the site's DNS settings to their default servers.
- The site license will become available for use on a different website.

## 2 The Main Interface

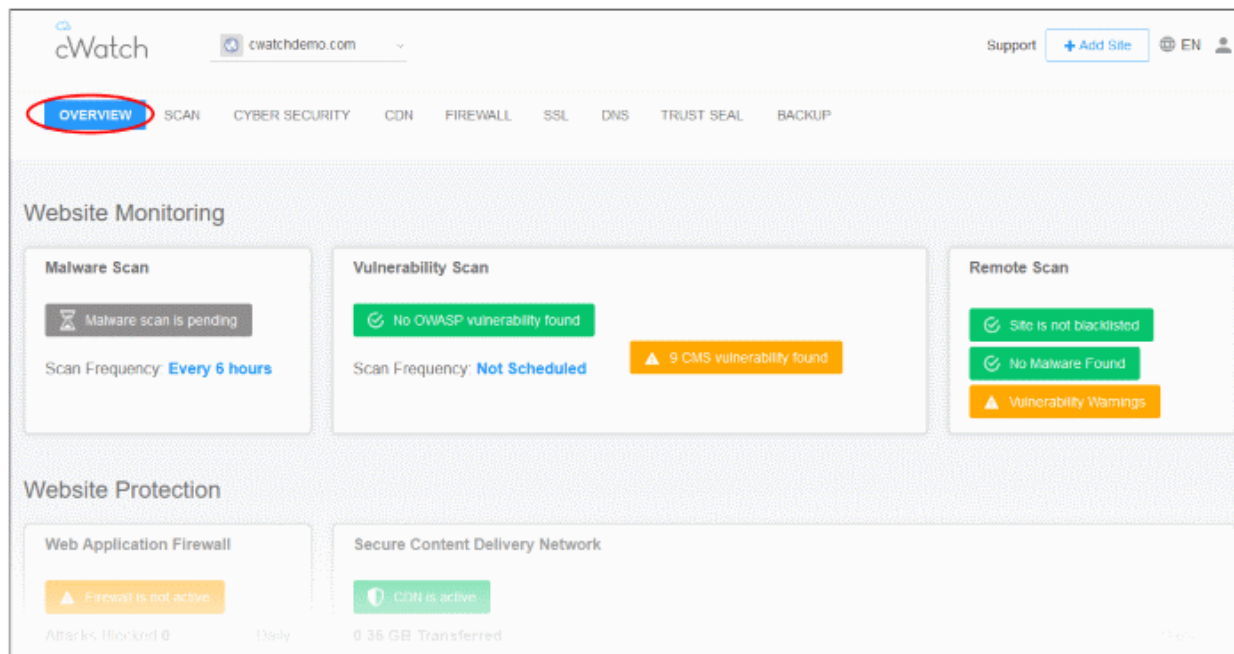
- The cWatch dashboard shows the security status of all protected domains.
- Click the 'cWatch' logo in the top-left corner to open the dashboard at any time
- The drop-down next to the logo lets you change to a different site. Use the links in the top-menu to access each major area of cWatch.



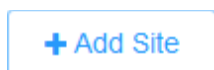
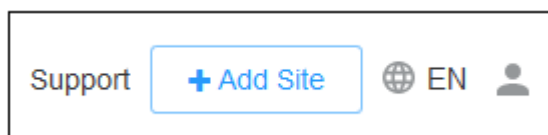
- **Overview** – Shows security and performance data from each cWatch module, for each protected site. Click on a specific site tile to open its statistics and configuration pages. See **Website Overview** for more details.
- **Scan** – cWatch offers three types of security scans:
  - **Remote Scan** - A first-level scan that checks front-end files for threats, blacklist status, missing headers, SSL errors, and more. The remote scan runs automatically straight after you add a site to cWatch. No configuration required. See **'Remote Scan'** for more details.
  - **Malware** – A full, deep-scan of your website's front-end and back-end files for all known threats. You can schedule malware scans to run at a time that suits you, and you can also configure automatic removal of discovered threats. You need to upload our .php file to the server to enable malware scans. See **Malware Scans** for more details.
  - **Vulnerability** – contains two types of scan:
    - **CMS vulnerability scans** - Identify weaknesses in your content management system (CMS). You can enable weekly automatic scans on each protected site, and can also run on-demand scans at any time.  
The scanner supports the following CMS types:
      - WordPress
      - Joomla
      - Drupal
      - ModX
      - Typo3
    - **OWASP top-ten threats** – Scans for the top-10 threats as identified by the Open Web Application Security Project (OWASP). You can enable weekly automatic scans on each protected site, and can also run on-demand scans at any time.  
See **Vulnerability Scans** for more details.
- **Cyber Security** - Real-time analysis of attack patterns on your website from the Comodo Security Operations Center (CSOC). The CSOC team is a group of dedicated Comodo experts who constantly monitor the event logs of protected websites. This allows them to identify potential threats ahead-of-time and deploy updated firewall rules on your behalf. See **Cyber Security Operation Center Results**
- **CDN** - Configure the cWatch content delivery network and view traffic for your site. This includes total data usage, status/error-code distribution, and the geographic locations from which your site was accessed. See **Content Delivery Network Metrics**
- **Firewall** - Configure Web Application Firewall (WAF) policies for the domain and create your own custom firewall rules. See **Firewall Rules** for more information.
- **SSL** - Secure traffic between the CDN edge servers and your website visitors. You can get a complimentary

SSL certificate from Comodo. Alternatively, you can upload an existing certificate. See [SSL Configuration](#) for more details.

- **DNS** - Configure DNS and nameservers in order to enable cWatch protection. See [DNS Configuration](#) for more information.
- **Trust Seal** - Add a cWatch site seal on managed websites. There are two types of seals: 'Malware Free' and 'Protected'. See [Add Trust Seal to your Websites](#) for more details.
- **Backup** – Back up your entire website and databases to our highly secure servers. Restore your site with a single click. See [Back up your Website](#) for more information.
  - The main display shows data for the selected item.



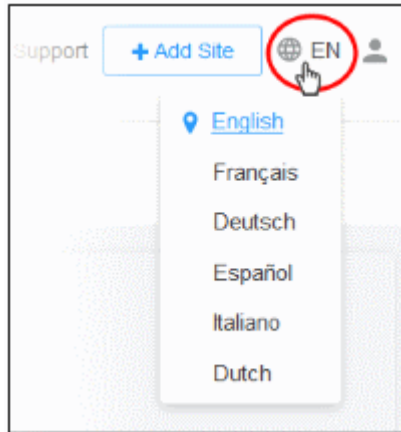
- The options on the top right let you to add a new website, select your language, manage your profile, view your subscriptions, submit a support ticket and logout:



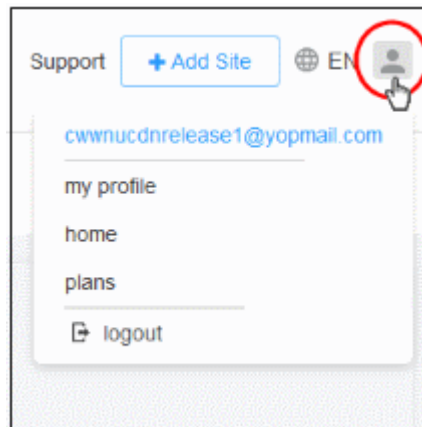
- Starts the site enrollment wizard. See [Add Websites](#) for more details.



- The current interface language.
  - Click the globe icon to view and change interface language (Default = English)



- Click to manage your profile and view your subscriptions.



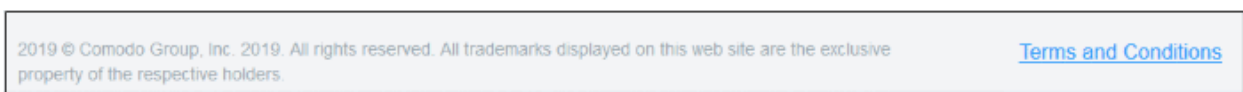
- **My Profile** - Your user information. Change your contact details, alert settings and password. See **Manage Your Profile** for more details.
- **Home** - Takes you to the dashboard. See **The Dashboard** for more details.
- **Plans** - List of licenses added to your account, domains associated with them, their status and more. You can also upgrade and renew licenses. See **View and Upgrade Licenses for Domains** for more details.
- **Logout** - Sign out from cWatch

- Help and support:

**Support**

- Click the 'Support' link to submit tickets. See **'Get Support'**

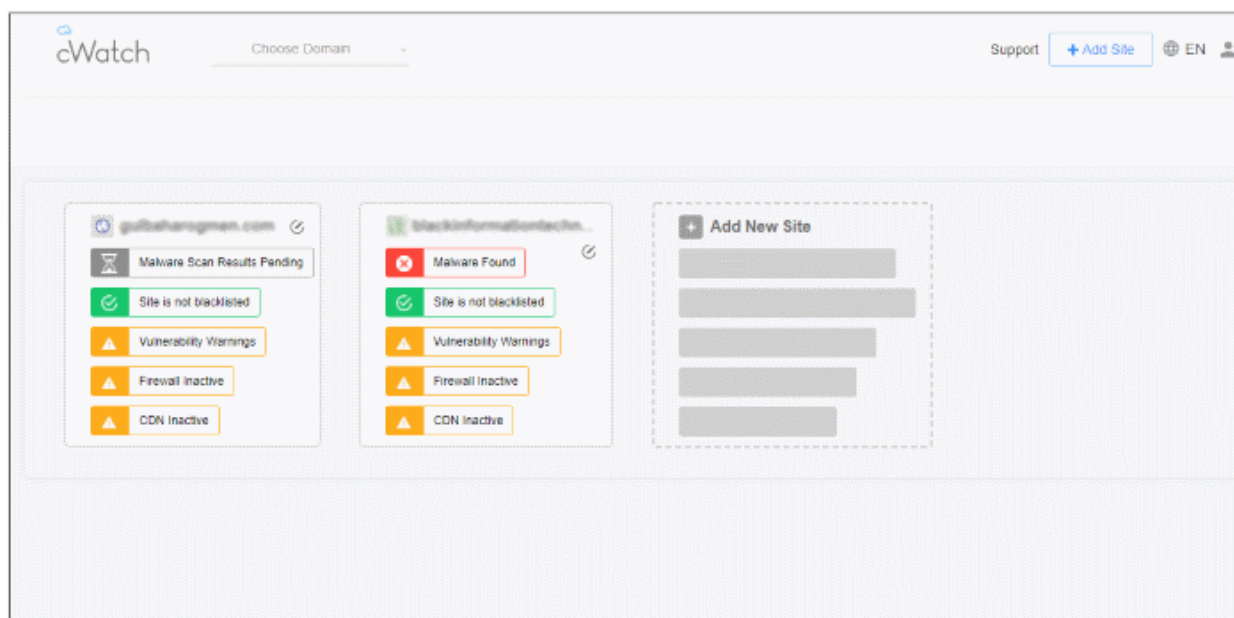
The footer contains copyright information, terms and conditions:



- Click the 'Terms and Conditions' link to view the cWatch EULA.

## 3 The Dashboard

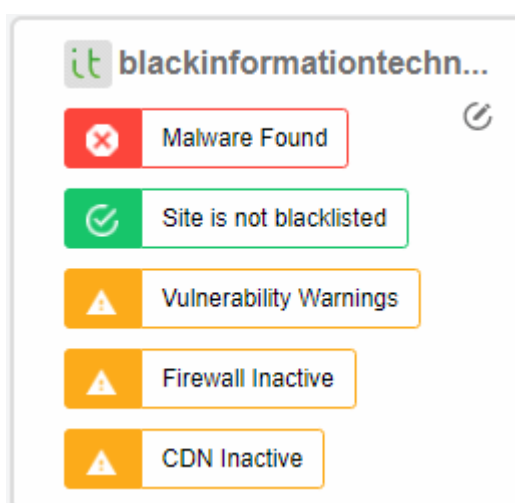
- Click the cWatch logo at top-left to open the dashboard.
- The condensed view shows a security summary for each site on your account:



- Click a site tile to open its dedicated statistics and settings pages. Alternatively, select a site in the drop-down next to the cWatch logo.

### Condensed view

- Each site on your account is shown as a separate tile.
- The rows on each tile tell you the security status of cWatch component:





- Green - No threats found in the category
- Yellow - Requires action. For example, activate the firewall or run a malware scan.
- Red - Threats found in this category
- Click the refresh icon at the top left corner of a tile to go to the domain overview page. See [Website Overview](#) for more details.



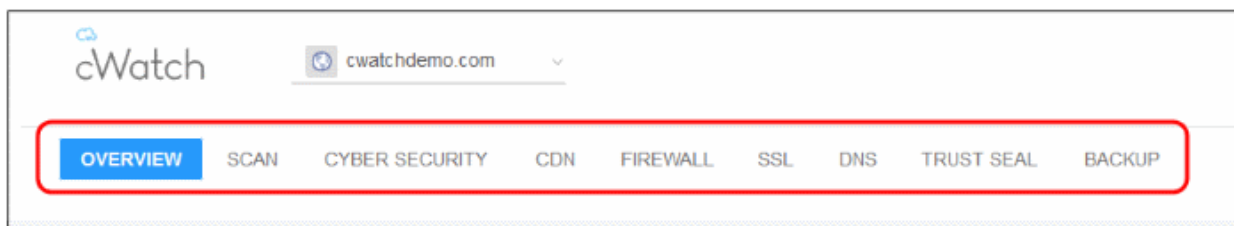
- Click a row to go to the respective configuration or results page

**Examples:**

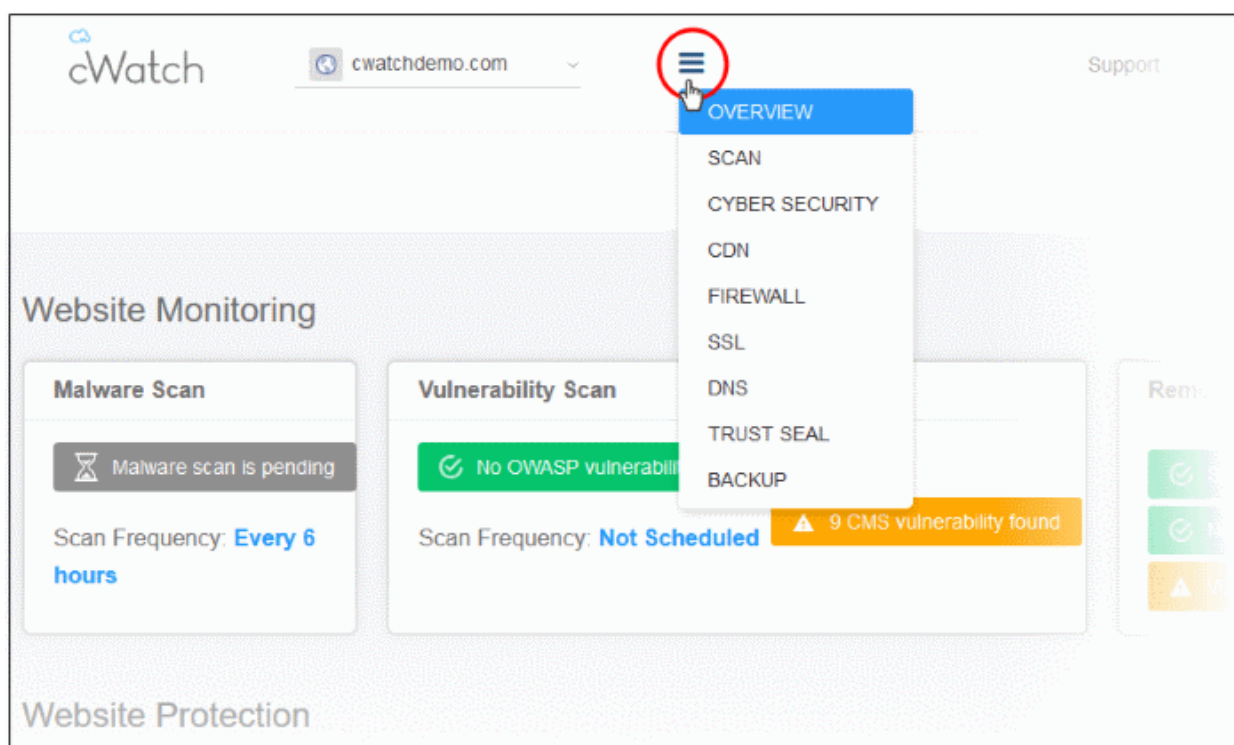
-  **Firewall Inactive** - Opens the web application firewall settings page. See [Configure WAF Policies](#).
-  **CMS vulnerability found** - Opens the vulnerability scan results page. You can review the results and take further actions. See [CMS Vulnerability Scans](#) for more details.

## 4 Website Data and Settings

- cWatch shows panoramic data about all events on your website.
- These include attacks monitored and blocked, the results of malware and vulnerability scans, statistics on your CDN usage, and more.
- Choose a website from the drop-down on the left.
  - Links to all major areas of the interface are in the top menu.



- They may be collapsed into a hamburger menu if your browser window is not wide enough.



- **Overview** - Summary of monitored parameters, security status and CDN performance. See **Website Overview** for more details.
- **Scan** – cWatch offers three types of security scans:
  1. **Remote Scan** - A first-level scan that checks front-end files for threats, blacklist status, missing headers, SSL errors, and more. The remote scan runs automatically straight after you add a site to cWatch. No configuration required. See '**Remote Scan**' for more details.
  2. **Malware** – A full, deep-scan of your website's front-end and back-end files for all known threats. You can schedule malware scans to run at a time that suits you, and you can also configure automatic removal of discovered threats.

You need to upload our .php file to the server to enable malware scans. See **Malware Scans** for more details.
  3. **Vulnerability** – two types:

**CMS scans** - Identify weaknesses in your content management system (CMS). You can enable weekly automatic scans on each protected site, and can also run on-demand scans at any time.

The scanner supports the following CMS types:

    - WordPress
    - Joomla
    - Drupal
    - ModX
    - Typo3


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

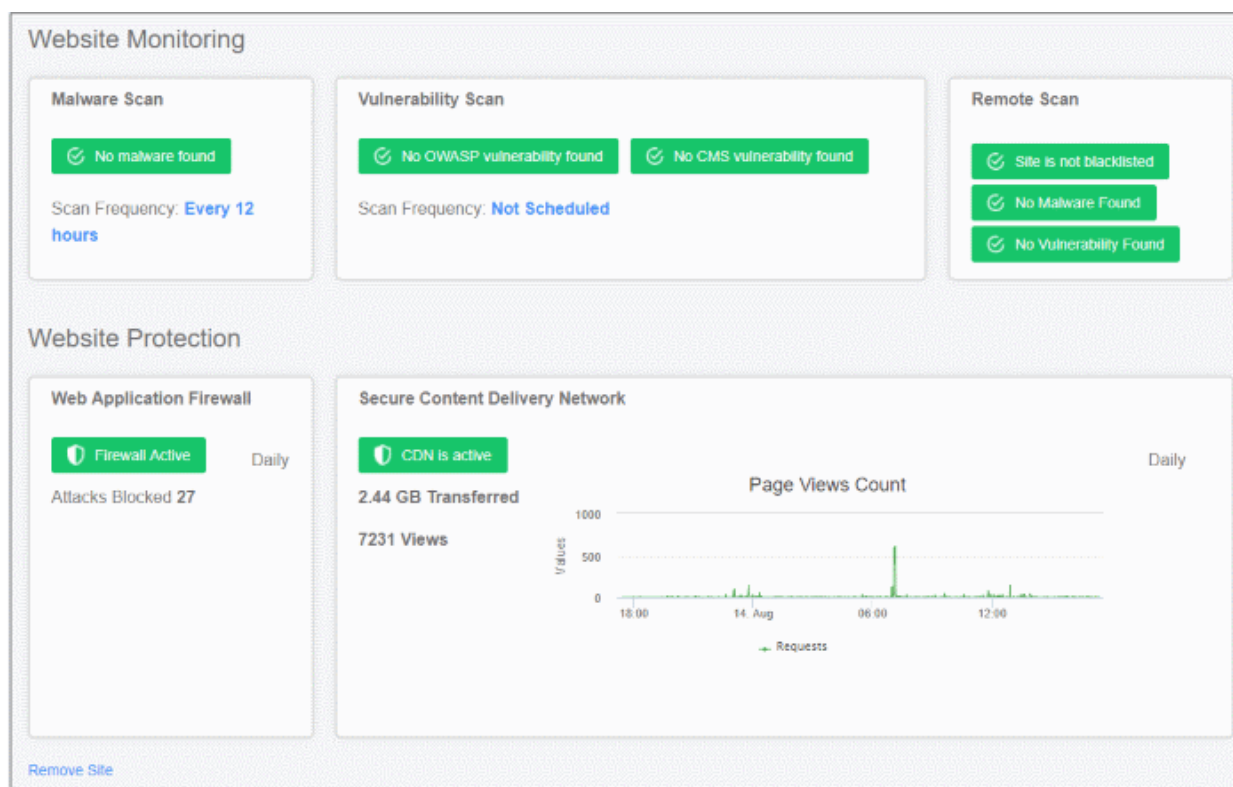
See **Vulnerability Scans** for more details.
- **Cyber Security** - Real-time analysis of attack patterns on your website from the Comodo Security Operations Center (CSOC). The CSOC team is a group of dedicated Comodo experts who constantly monitor the event logs of protected websites. This allows them to identify potential threats ahead-of-time and deploy updated firewall rules on your behalf. See **Cyber Security Operation Center Results**
- **CDN** - Configure the cWatch content delivery network and view traffic for your site. This includes total data usage, status/error-code distribution, and the geographic locations from which your site was accessed. See **Content Delivery Network Metrics**
- **Firewall** - Configure Web Application Firewall (WAF) policies for the domain and create your own custom firewall rules. See **Firewall Rules** for more information.
- **SSL** - Secure traffic between the CDN edge servers and your website visitors. You can get a complimentary SSL certificate from Comodo. Alternatively, you can upload an existing certificate. See **SSL Configuration** for more details.
- **DNS** - Configure DNS and nameservers in order to enable cWatch protection. See **DNS Configuration** for more information.
- **Trust Seal** - Add a cWatch site seal on managed websites. There are two types of seals: 'Malware Free' and 'Protected'. See **Add Trust Seal to your Websites** for more details.
- **Backup** – Backup your entire website and databases to our highly secure cWatch servers. Restore your website with a single click. See '**Back up your Website**' for more information.

## 4.1 Website Overview

- Select a website from the drop-down at top-left and choose 'Overview'
- The overview page shows a summary of blocked threats, the reputation of your sites, and visitor activity on your sites.
- Each tile shows important security information from various cWatch modules.
- The tiles also contain shortcuts to more detailed results and threat remediation advice.

### Open the overview page

- Select the website from the drop-down at top-left of the dashboard
- Click the 'Overview' tab
  - Or click the hamburger button and select "Overview"
- Alternatively, click the  icon at the top-left of a domain tile in the dashboard



- Tiles are broken down into two categories:
  - **Website Monitoring**
  - **Website Protection**
- Each tile shows data from a different cWatch module. Threat information is color-coded as follows:
  - Green - No threats found / The module is running OK
    - Click the stripe to view a history of actions by the module
  - Yellow - Action required. For example, activate the firewall or run a vulnerability scan.
    - Click the stripe to activate the module or initiate a scan.
  - Red - Threats found
    - Click the stripe to open the module's configuration page. For example, you can start a malware scan or submit a request for Comodo to remove the malware. See '**Malware Scans**' for more information

## Website Monitoring

- Shows key information from cWatch scans. This includes malware scan results, vulnerability scan results, and site reputation checks.

### Malware Scan:

The result of the most recent manual or scheduled virus scan.

**Scan Frequency** - Scan timings.

**Note:** You need to upload the cWatch agent to your site to enable malware scans.

✘ 20 malware Found

- Click the 'malware found' stripe to see full malware details and read threat remediation advice.

⚠ Malware scanner is not enabled

- Click the 'not enabled' stripe to enable to scanner.

### Malware Scan

✘ 20 malware Found

Scan Frequency: **Daily**

### Vulnerability Scan

✘ 20 OWASP vulnerability found

✘ 7 CMS vulnerability found

Scan Frequency: **Not Scheduled**

Scan Frequency: **Weekly**

## Vulnerability Scan

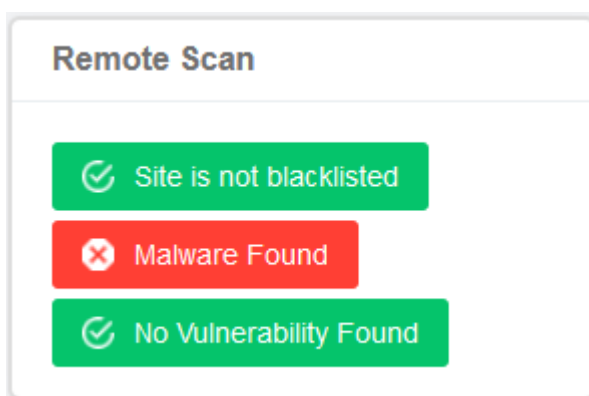
**OWASP Vulnerabilities** - The number of vulnerabilities on your site that are listed in the Open Web Application Security Project (OWASP). Threats listed in OWASP are serious and should be fixed.

- Note - cWatch automatically blocks any OWASP threats it finds.
- Click the stripe to go to the 'Vulnerabilities' page.
  - Click 'View full report' under OWASP
  - 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 **Manage Custom Firewall Rules** for help to create custom WAF rules.
- You can also initiate on-demand OWASP vulnerability scans from the 'Vulnerabilities' page
- Scan Frequency** - Whether automatic OWASP vulnerability scans are scheduled for the domain and the scan periodicity.

**CMS Vulnerabilities** - Number of active risks on your site's content management system (CMS).

- The scanner supports the following types of CMS:
  - WordPress
  - Joomla
  - Drupal
  - ModX
  - Typo3
- Click the stripe to go to the 'Vulnerabilities' page.
- Click 'View full report' under CMS scan
- The risk factors identified in the CMS components are shown as a list under the respective tab
- The details also include the version number of the CMS system in which vulnerability is found and the version to be updated to, to mitigate it.
- See **CMS Vulnerability Scans** for more help with this interface.
- Scan Frequency** - Whether automatic OWASP vulnerability scans are scheduled for the domain and the scan periodicity.

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



**Remote Scan** - The result of the most recent automatic or manual remote scan.

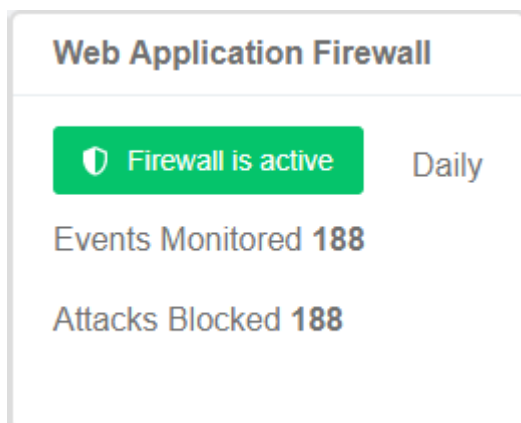
- Site is blacklisted / Site is not blacklisted** – States whether or not your site is listed as harmful on one of the major website blacklists.
- Malware Found / No Malware Found** – States whether or not threats were found by the last remote scan.
- Vulnerabilities Found / No Vulnerability Found** – States whether the last remote scan found any OSWASP or CMS vulnerabilities.

Click any strip to open the remote scan settings pages.

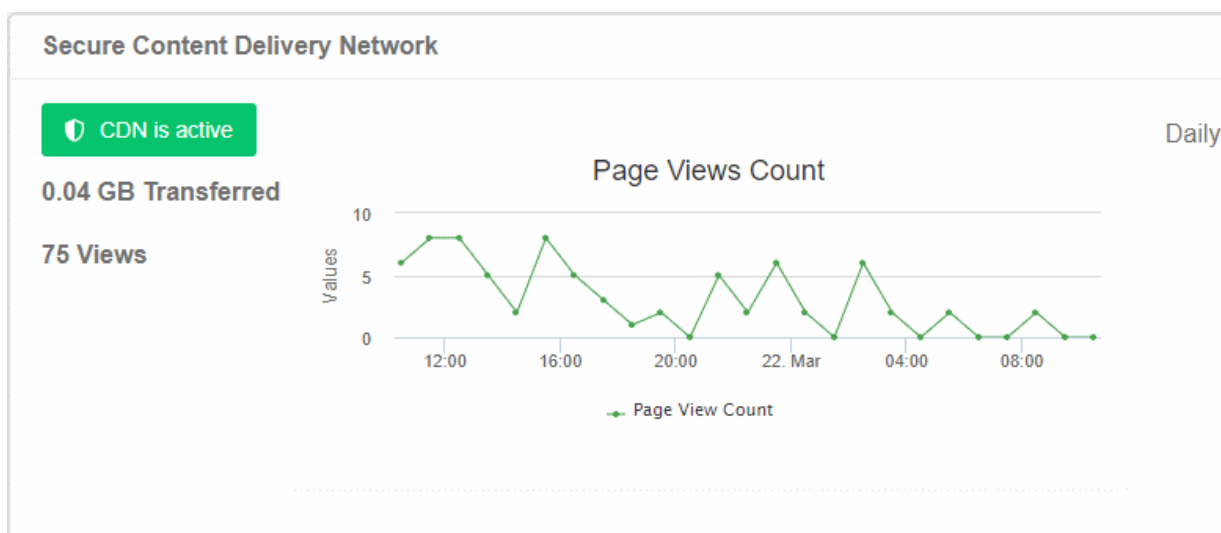
See **'Remote Scans'** for more information.

## Website Protection

- Shows attacks blocked by web application firewall (WAF) and CDN usage statistics.




- 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.
  - Click the stripe to configure the WAF policies and create custom firewall rules for the domain.
  - The period covered by the report is shown at the right of the stripe
- Events Monitored** - Number of incidents that triggered a firewall rule.
- Attacks Blocked** - Number of incidents identified as potential intrusion attempts and blocked



### Secure Content Delivery Network

- The status of your CDN configuration live data about your CDN usage and the number of times your pages were viewed.
  - The period covered by the report is shown at the right of the stripe
  - Click the stripe to go to the CDN page of the domain

**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' > 'Activation' to view the CNAME record for your site.
- If you haven't configured the CNAME then no data is shown here.
  - Click  to start the configuration process.
- See [Content Delivery Network Metrics](#) for more details about CDN statistics.

## 4.2 Security Scans

There are three types of security scan you can run on your site:

- Remote Scan** – An automatic scan that runs immediately after you add a site to cWatch. Remote scans require no configuration and are a fast and convenient way to identify threats.

The scan searches front-end pages for threats, blacklist status, missing security headers, SSL errors, javascripts and more. You can also run remote scans on-demand at any time.

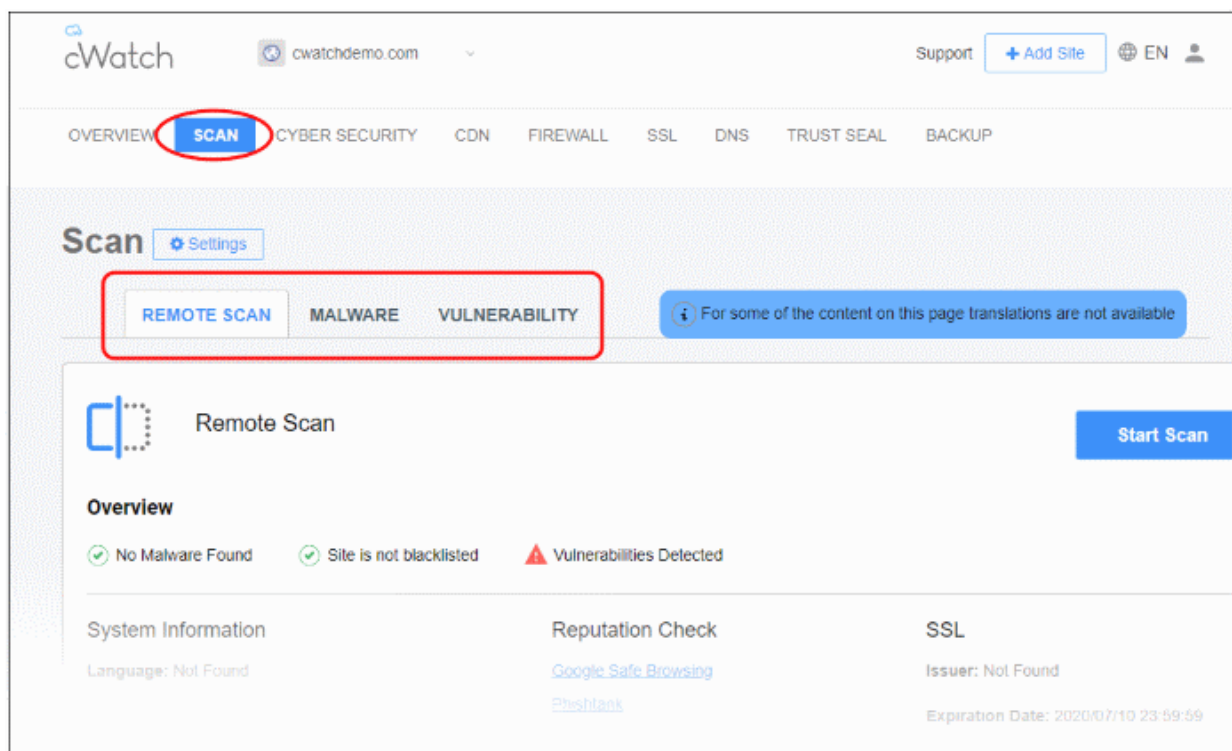
The remote scan checks the site's front-end pages, but the malware scan is much more thorough. The malware scan checks both front-end and back-end files, including items like perl, php, asp.net and SQL.

Also, you must use a malware scan if you want to schedule recurring scans and automatic clean-ups.

- Malware Scan** – An in-depth scan of your site for known malware and viruses. You can schedule repeat scans to run at a time of your choice, and have any discovered malware automatically removed. You need to upload the cWatch agent to your server to enable this type of scan.
- Vulnerability Scan** – A scan for content management system (CMS) vulnerabilities and for top ten

vulnerabilities published by the Open Web Application Security Project (OWASP).

Select a website from the drop-down and choose 'Scan'

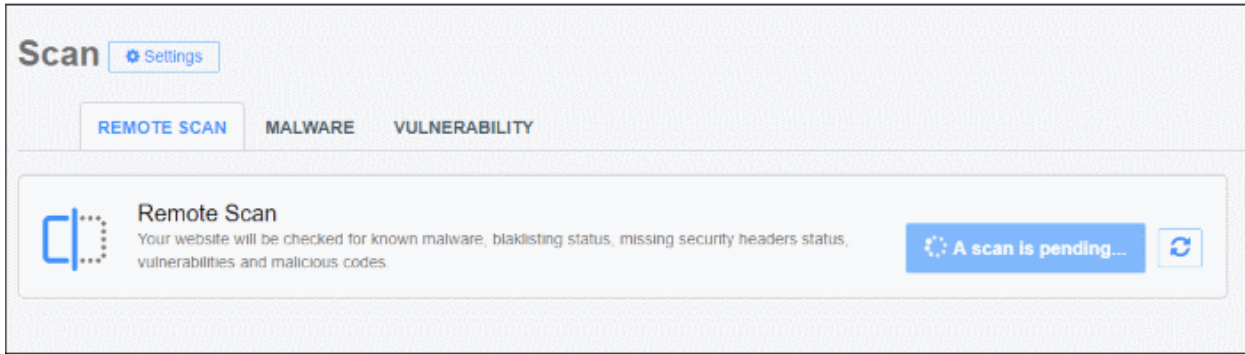


Click the following for more information about each scan:

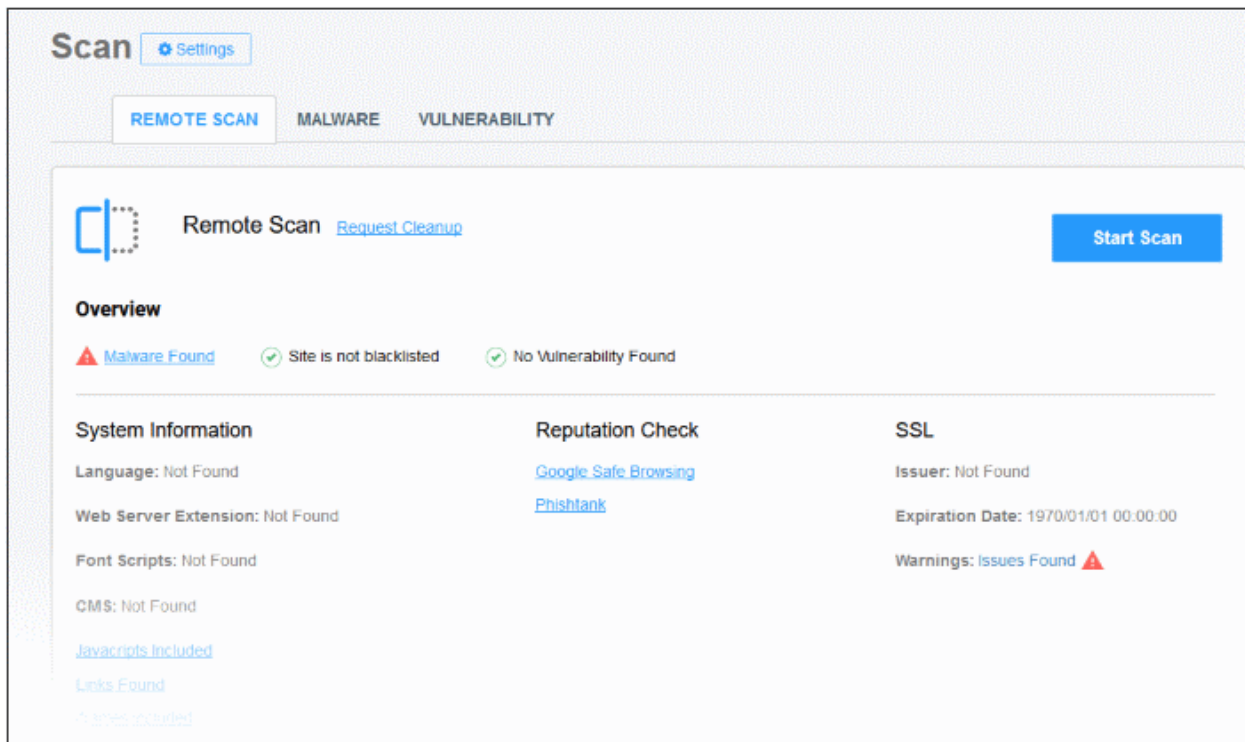
- [Remote Scans](#)
- [Malware Scans](#)
- [Vulnerability Scans](#)

#### 4.2.1 Remote Scans

- The remote scan checks your front-end webpages for errors, vulnerabilities and known malware.
- The scan is a good, 'first-level' check for threats to your site. However, you must enable the full malware scanner for long-term protection.
- Remote scans check the following:
  - Safe browsing status (blacklist status)
  - SSL certificate errors
  - Content Management (CMS) errors
  - HTTP errors and missing security headers
  - Javascripts, iframes and malicious links
- The remote scan starts automatically right after you add a website:



- The results are shown at the end of the scan:



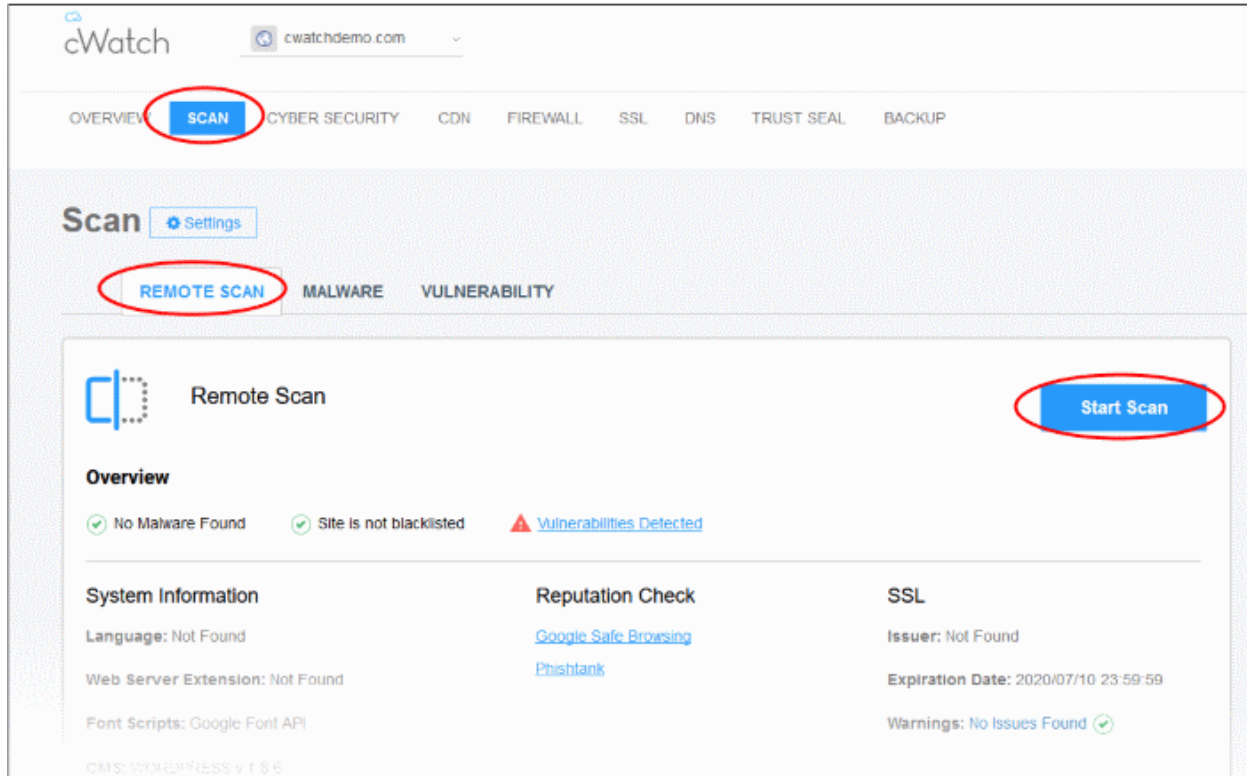
See '[Run Remote Scans and View Results](#)' for information about remote scan results.



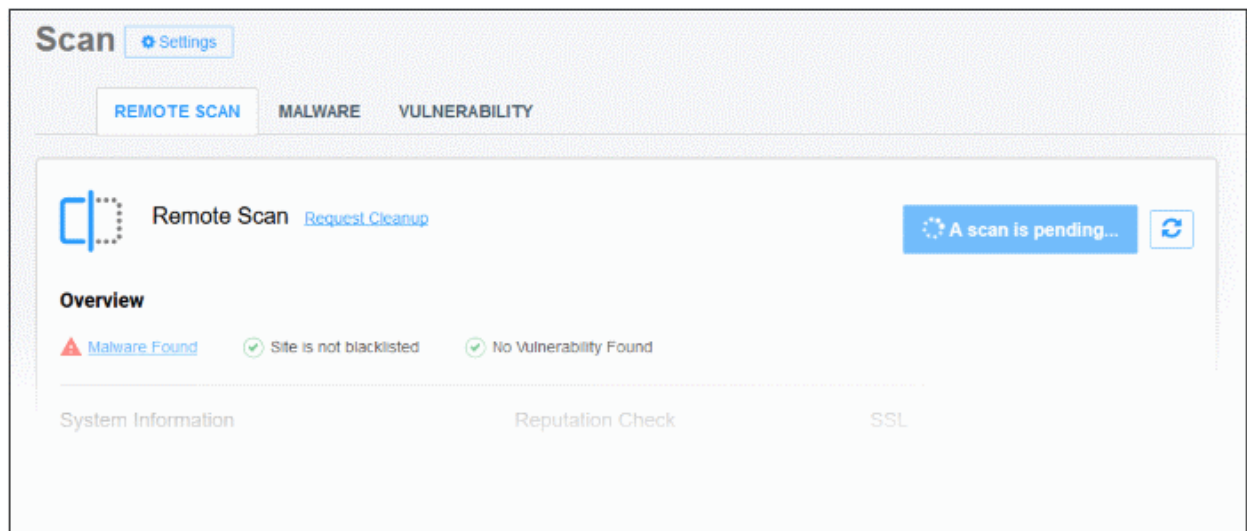
## 4.2.1.1 Run Remote Scans and View Results

You can run a manual remote scan every two hours.

- Select a website at top-left then choose 'Scan'
- Open the 'Remote Scan' tab
- Click 'Start Scan':



- The scan may take a few minutes to complete:



- Any vulnerabilities are shown at the end of the scan. The results list any missing headers and warns you about SSL errors and any blacklists on which your site appears:

Scan Settings

REMOTE SCAN
MALWARE
VULNERABILITY

### Remote Scan [Request Cleanup](#)

Start Scan

**Overview**

▲ Malware Found
✔ Site is not blacklisted
✔ No Vulnerability Found

<p><b>System Information</b></p> <p>Language: Not Found</p> <p>Web Server Extension: Not Found</p> <p>Font Scripts: Not Found</p> <p>GMS: Not Found</p> <p><a href="#">JavaScripts Included</a></p> <p><a href="#">Links Found</a></p> <p><a href="#">iFrames Included</a></p>	<p><b>Reputation Check</b></p> <p><a href="#">Google Safe Browsing</a></p> <p><a href="#">PhishTank</a></p>	<p><b>SSL</b></p> <p>Issuer: Not Found</p> <p>Expiration Date: 1970/01/01 00:00:00</p> <p>Warnings: Issues Found <span style="color: red;">▲</span></p>
--	---	---

**HTTP Security Headers**

Headers

✗ content-security-policy

✗ x-ss-protection

✗ x-content-security-policy

✗ x-content-type-options

✗ x-webkit-csp

✗ frame-options

✗ x-frame-options

✔ content-type

✗ content-security-policy-report-only

✔ pragma

**Raw HTTP Headers ▲**

```

http code : 200
date : Mon, 12 Aug 2019 06:25:12 GMT
server : Microsoft-IIS/7.5
content-length : 493
expires : -1
x-aspnet-version : 4.0.30319
client-peer : 50.63.202.46.60
client-date : Mon, 12 Aug 2019 06:25:13 GMT
pragma : no-cache
client-response-num : 1
x-powered-by : ASP.NET
content-type : text/html; charset=utf-8
connection : close
cache-control : no-cache
age : 1
                    
```

**Missing HTTP Security Headers**

content-security-policy	Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
x-ss-protection	This header enables the Cross-site scripting (XSS) filter built into most recent web browsers. It's usually enabled by default anyway, so the role of this header is to re-enable the filter for this particular website if it was disabled by the user. This header is supported in IE 8+, and in Chrome (not sure which versions). The anti-XSS filter was added in Chrome 4. Its unknown if that version honored this header
x-content-security-policy	Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
x-content-type-options	The only defined value, 'nosniff', prevents Internet Explorer and Google Chrome from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions. This reduces exposure to drive-by download attacks and sites serving user uploaded content that, by clever naming, could be treated by MSIE as executable or dynamic HTML files
x-webkit-csp	Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
frame-options	The use of 'X-Frame-Options' allows a web page from host B to declare that its content (for example, a button, links, text, etc.) must not be displayed in a frame (<frame> or <iframe>) of another page (e.g., from host A). This is done by a policy declared in the HTTP header and enforced by browser implementations
x-frame-options	The use of 'X-Frame-Options' allows a web page from host B to declare that its content (for example, a button, links, text, etc.) must not be displayed in a frame (<frame> or <iframe>) of another page (e.g., from host A). This is done by a policy declared in the HTTP header and enforced by browser implementations
content-security-policy-report-only	Like Content-Security-Policy, but only reports. Useful during implementation, tuning and testing efforts

**Additional Information**

content-type	In practice, resource owners do not always properly configure their origin server to provide the correct Content-Type for a given representation, with the result that some clients will examine a payload's content and override the specified type. Clients that do so risk drawing incorrect conclusions, which might expose additional security risks like privilege escalation etc
pragma	Caches expose additional potential vulnerabilities, since the contents of the cache represent an attractive target for malicious exploitation

- **Request Cleanup** – Create a ticket for Comodo security experts to fix all issues found by the scan. The link takes you to support page where you can create a ticket. See '**Get Support**'
- **Malware Found** - Click the 'Malware Found' link to start a deep virus scan on your web server. All malware will be removed at the end of the scan.

See '**Run Malware Scans and View Results**' for more information.

Note – you need to **configure the malware scanner** if you haven't yet done so.

- **Site is blacklisted** – The site was flagged as suspicious by Google's 'Safe Browsing' service. Click the link to view the full reasons on Google's transparency report page.
- **Vulnerabilities Detected** - Security holes were found on your website. Click the link to run a CMS and OWASP Top 10 scan on the site. The results of these scans contain mitigation advice to help you fix the issues. See '**Vulnerability Scans**' for more details.

### System Information

- **Language** – The programming language used in the site. For example, PHP, Python and so on.
- **Web Server Extension** – Optional module used in the website. For example, OpenSSL, mod\_ssl, Google PageSpeed and so on.
- **Font Scripts** – Shows fonts used on your web pages.
- **CMS** – The content management system (CMS) tool used on the site.
- **JavaScripts Included** – Click the link to view details of JavaScripts used on site pages.
- **Links Found** - Click the link to view internal and external hyperlinks used on site pages.
- **Iframes Included** - Click the link to view internal and external inline frames (iframes) used in site pages. Iframes can be vulnerable to attack.

### Reputation Check

- **Google Safe Browsing** – Opens <https://transparencyreport.google.com/safe-browsing/>. Use this site to check whether any of your sites have been flagged as harmful.
- **Phishtank** – Opens the PhishTank website at <https://www.phishtank.com/>. Use this site to run to see if any of your sites are listed as fraudulent.

### SSL

- **Issuer** - The certificate authority that issued the certificate to your site.
- **Expiration Date** - Date on which the certificate expires. Please remember to replace certificates that are nearing expiry. Google Chrome and other browsers will show error messages to your visitors if your certificate is not valid.
- **Warnings** – Click the 'Issues found' / 'No issues found' link to visit <https://www.sslshopper.com/ssl-checker.html>. The checker runs a deep inspection of your SSL configuration and identifies any errors. The page also has plenty of remediation advice to help you fix any issues.

### HTTP Security Headers

HTTP security headers are used to protect your website against attacks such as XSS, clickjacking, code injection and so on. cWatch reports which security headers are missing from your site.

## HTTP Security Headers

### Headers

✘ content-security-policy
✘ x-xss-protection
✘ x-content-security-policy
✘ x-content-type-options
✘ x-webkit-csp
  
✘ frame-options
✘ x-frame-options
✔ content-type
✘ content-security-policy-report-only
✔ pragma

### Raw HTTP Headers ▼

### Missing HTTP Security Headers

<b>content-security-policy</b>	Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
<b>x-xss-protection</b>	This header enables the Cross-site scripting (XSS) filter built into most recent web browsers. It's usually enabled by default anyway, so the role of this header is to re-enable the filter for this particular website if it was disabled by the user. This header is supported in IE 8+, and in Chrome (not sure which versions). The anti-XSS filter was added in Chrome 4. Its unknown if that version honored this header
<b>x-content-security-policy</b>	Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
<b>x-content-type-options</b>	The only defined value, 'nosniff', prevents Internet Explorer and Google Chrome from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions. This reduces exposure to drive-by download attacks and sites serving user uploaded content that, by clever naming, could be treated by MSIE as executable or dynamic HTML files
<b>x-webkit-csp</b>	Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
<b>frame-options</b>	The use of 'X-Frame-Options' allows a web page from host B to declare that its content (for example, a button, links, text, etc.) must not be displayed in a frame (<frame> or <iframe>) of another page (e.g., from host A). This is done by a policy declared in the HTTP header and enforced by browser implementations
<b>x-frame-options</b>	The use of 'X-Frame-Options' allows a web page from host B to declare that its content (for example, a button, links, text, etc.) must not be displayed in a frame (<frame> or <iframe>) of another page (e.g., from host A). This is done by a policy declared in the HTTP header and enforced by browser implementations
<b>content-security-policy-report-only</b>	Like Content-Security-Policy, but only reports. Useful during implementation, tuning and testing efforts

### Additional Information

<b>content-type</b>	In practice, resource owners do not always properly configure their origin server to provide the correct Content-Type for a given representation, with the result that some clients will examine a payload's content and override the specified type. Clients that do so risk drawing incorrect conclusions, which might expose additional security risks like privilege escalation etc
<b>pragma</b>	Caches expose additional potential vulnerabilities, since the contents of the cache represent an attractive target for malicious exploitation

## 4.2.2 Malware Scans

- Select the target website from the drop-down at top-left
- Click 'Scan' > '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 agent to your site.
  - Click 'Scan' > 'Malware' > 'Overview'
  - Click 'Enable Scanner'
  - Choose 'Automatic' in the 'Enable Malware Scanner' tile
  - Enter your web-server FTP details.
  - Click 'Test Connection'
  - Click 'Save' after the connection is established
  - You will see the message - 'Malware scanner is enabled'
    - See **Automatic configuration** for more information.
2. **Manually** - Download the agent and copy it to your site. The agent is a .php file.
  - Click 'Scan' > 'Malware' > 'Overview'
  - Click 'Enable Scanner'
  - Choose 'Manual' in the 'Enable Malware Scanner' tile.
  - Click the purple 'PHP' icon to download the file
  - Upload the file to a publicly accessible location on your site
  - Enter the URL of the file in the space provided
  - Click 'Test and Save'. The scanner will be enabled if the test is successful.
    - See **Manual Configuration** for guidance on this.

Once 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 license type. You can manage automatic malware removal in **malware settings** page.
- Automatic malware removal is not included with 'Basic' licenses. If you enable automatic malware removal in **malware settings** page, you will be prompted to upgrade your license.
- The frequency of the scheduled scans depends on your license type:
  - Basic – One scan per day
  - Pro – Two scans per day
  - Premium - Four scans per day
- Both scheduled and manual scans count against your number of scans per day. For example, if you have a premium license, and run two manual scans, then only two scheduled scans will run that day.

### Open the 'Malware' interface

- Select the website from the menu at top-left of the dashboard
- Click the 'Scan' tab then 'Malware'

- The malware overview page shows threats on the site.
- The malware history page shows the last ten 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.
- If enabled, you will receive a notification email when malware is found.
- You can request Comodo technicians manually remove all threats from your site.

From the malware section you can:

- Upload the scanner agent to your site
- Start a manual scan
- View malware scan results
- Submit malware cleanup requests
- Configure automatic cleanup requests
- Configure email notifications
- Start a scan and request a cleanup in a single step

See the following section for more help on malware scans:

- [Configure Malware Scan Settings](#)
  - [Automatic configuration](#)
  - [Manual Configuration](#)
- [Run Malware Scans and View Results](#)
- [Configure Notification and Automatic Malware Removal](#)

#### 4.2.2.1 Configure Malware Scan Settings

You need to upload the cWatch scanner file to your site in order to run malware scans.

##### Upload the scanner file

- Select the target site from the menu at top-left of the dashboard
- Click the 'Scan' tab then 'Malware' > 'Overview'
  - Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'
- Click 'Enable Scanner':

The screenshot displays the Comodo cWatch Web Security dashboard. At the top, the navigation menu includes OVERVIEW, SCAN, CYBER SECURITY, CDN, FIREWALL, SSL, DNS, TRUST SEAL, and BACKUP. The 'SCAN' tab is selected and circled in red. Below the navigation, the 'Scan' section is active, with sub-tabs for REMOTE SCAN, MALWARE, and VULNERABILITY. The 'MALWARE' sub-tab is selected and circled in red. Under the 'MALWARE' sub-tab, there is an 'Overview' section with a warning icon and the message: 'Malware Scanner has not been activated. In order to enable malware detection, we need to connect to your site via FTP/SFTP and upload server side scan agent'. A red arrow points to the 'Enable Scanner' button, which is also circled in red. Below this, the 'Settings' modal is open, showing the 'Enable Malware Scanner' configuration. The 'Automatic' radio button is selected. The 'CONNECTION TYPE' dropdown is set to 'FTP'. There are input fields for 'FTP USERNAME', 'FTP PASSWORD', 'FTP HOSTNAME', 'FTP PORT' (set to 21), and 'FTP DIRECTORY'. A 'Test Connection' button is at the bottom. To the right, the 'Email Notifications' section is set to 'Whenever Malware Found' with a 'Save' button. Below that, the 'Automatic Malware Removal' section has a toggle switch for 'Switch On for automatic malware removal'.

See the following sections for help with:

- [Automatic configuration](#)
- [Manual Configuration](#)

#### 4.2.2.1.1 Automatic Configuration

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

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Malware' > 'Overview'
  - Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'
- Click 'Enable Scanner'
- Select 'Automatic' in the malware scanner box:

## ← Settings

### Enable Malware Scanner

Automatic  Manual

FTP USERNAME

FTP HOSTNAME

FTP DIRECTORY  
  
e.g., /public\_html/

CONNECTION TYPE

FTP PASSWORD

FTP PORT

### Email Notification

Whenever Malware is detected

### Automatic Malware Scanner

When enabled when automatic scanning is performed.

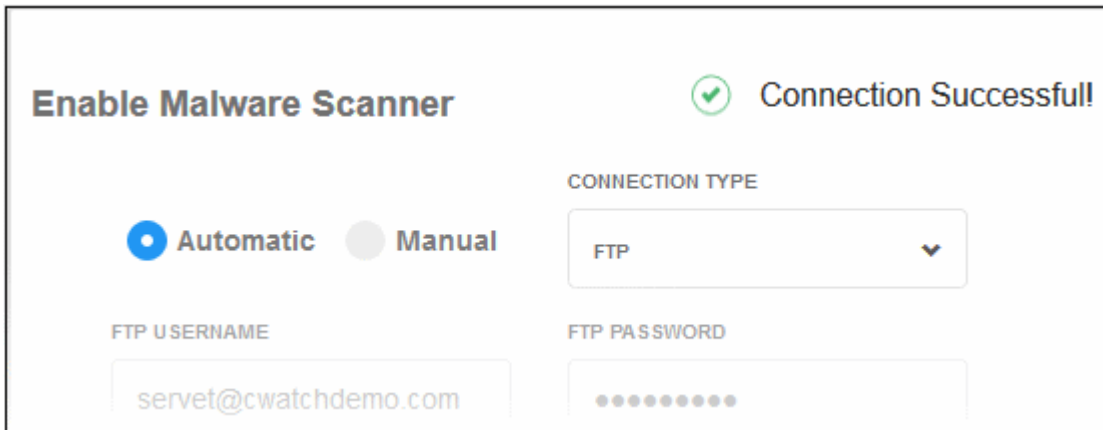
Switch On for automatic scanning

FTP / sFTP Settings - Table of Parameters

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

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

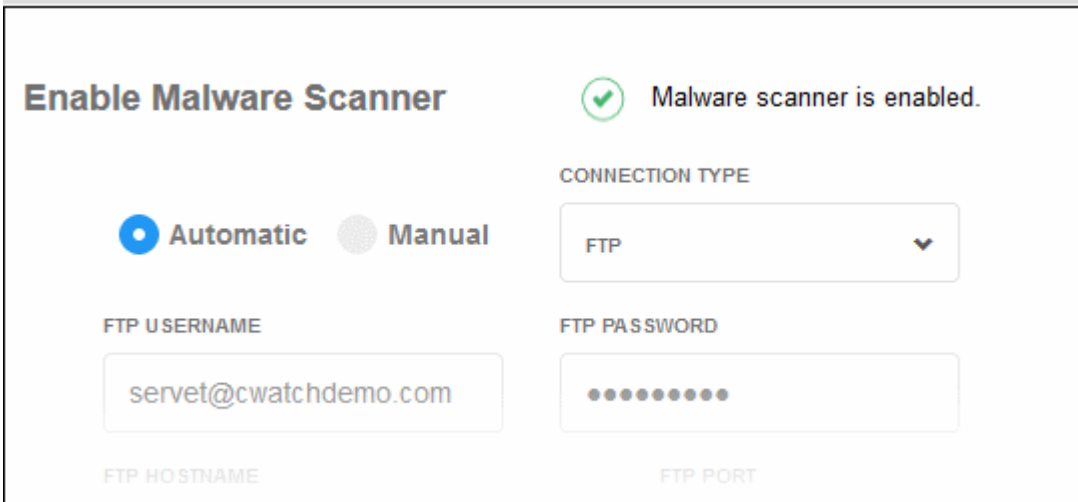




The screenshot shows the 'Enable Malware Scanner' configuration interface. At the top right, a green checkmark icon is followed by the text 'Connection Successful!'. Below this, there are two radio buttons: 'Automatic' (selected) and 'Manual'. To the right is a dropdown menu for 'CONNECTION TYPE' with 'FTP' selected. Below these are two input fields: 'FTP USERNAME' containing 'servet@cwatchdemo.com' and 'FTP PASSWORD' which is masked with dots. The interface is clean and modern with a white background and grey text.

- Click 'Save'

cWatch will upload the agent to your site. You will see 'Malware scanner is enabled' at the upper-left of the box if everything is successful:



This screenshot shows the same 'Enable Malware Scanner' configuration page, but now the status at the top right has changed to 'Malware scanner is enabled.' with a green checkmark icon. The configuration options remain the same: 'Automatic' is selected, 'CONNECTION TYPE' is 'FTP', 'FTP USERNAME' is 'servet@cwatchdemo.com', and 'FTP PASSWORD' is masked. Additionally, 'FTP HOSTNAME' and 'FTP PORT' fields are visible at the bottom of the form, though they are currently empty.

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


#### 4.2.2.1.2 Manual Configuration

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

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Malware' > 'Overview'
  - Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'
- Click 'Enable Scanner'
- Select 'Manual' in the malware scanner box:

### Enable Malware Scanner

Automatic  Manual

1.) Download this file. 

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

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

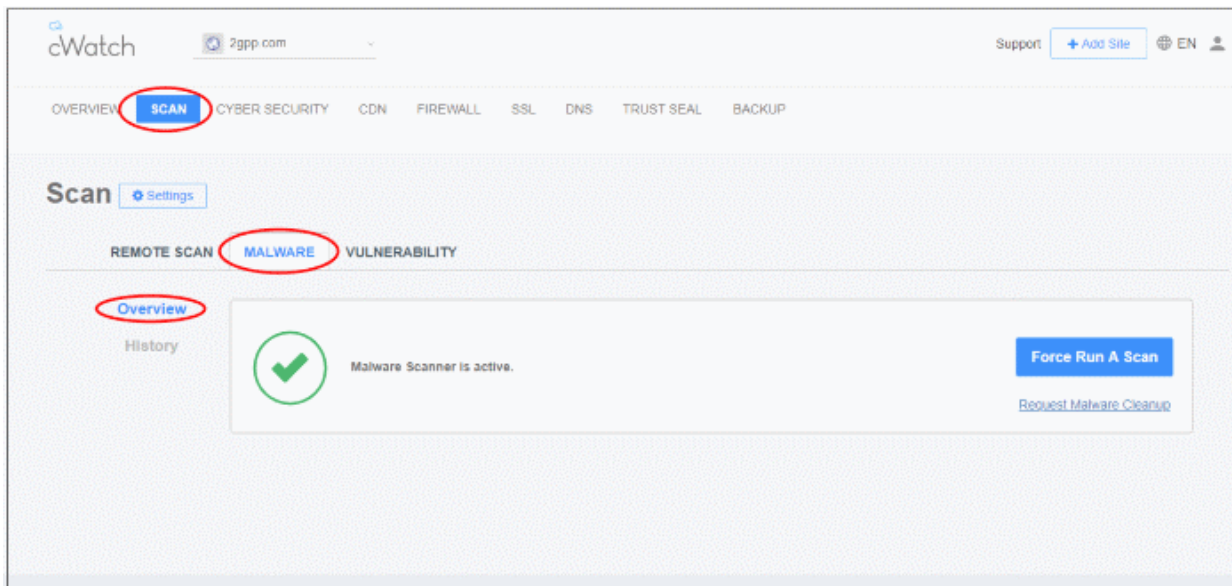
We will try to access the file at:

- Download the PHP file in step 1
- Upload the file to the root folder of your website. The file should be publicly accessible.
- Enter the URL of the uploaded file in the text field.
- Click 'Test and Save' to run the check.
- Malware scans will begin on your site if the check is successful.

#### 4.2.2.2 Run Malware Scans and View Results

- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Scan' tab then 'Malware' > 'Overview'
  - Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'

**Note** - Make sure you have uploaded the scanner file to the site. See [Configure Malware Scan Settings](#) if you haven't yet done this.



- The overview page shows details about any malware found on the site. Click the history link to view current and previous scan results.

From this interface you can:

- **Start a manual scan**
- **Submit a malware cleanup request**
- **Start a scan and request a cleanup in a single step**
- **View malware scan results**

### Start a manual scan

- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Scan' tab then 'Malware' > 'Overview'
  - Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'
- Click the 'Force Run a Scan' button:



Any malware found is shown in the results table at the end of the scan:

**Malware Scanner is active.**

[Force Run A Scan](#)  
[Request Malware Cleanup](#)

---

!

## Malware Found

#	FILE VERDICT	FILE PATH	SHA1
1	Backdoor.2867	./crayonweb.site/wp-includes/wp-tmp.php	58aa9e41a5f1cd8c58571bf8c677d8e3438921e
2	1.TrojWare.3458	./crayonweb.site/wp-content/themes/twentyseventeen/functions.php	33b5f73418a309ceca720e3aff584c91a17d2b7b
3	1.TrojWare.3458	./wp-content/themes/twentyseventeen/functions.php	5000fec709fb42d5e6ac1c4a903a9186a562bb7b
4	9.1.9.ApplicUwnt.2139	./crayonweb.site/wp-content/plugins/ol_scrapes/classes/class-ol-scrapes.php	0d865f0f9bfa3e5a4e5742c44d959e5b5fc76489
5	1.TrojWare.3458	./crayonweb.site/wp-content/themes/twentyfifteen/functions.php	466bd9573cedf18bd626247e44828994063b246c
6	1.TrojWare.3458	./crayonweb.site/wp-content/themes/twentsixteen/functions.php	b3fa57f19468e9eedf4e5587a82cec865f6da3

**File Verdict** – Name of the malicious item

**File Path** – Location of the item on your webserver

**SHA1** – File hash of the malicious item. Hash values are used by Comodo, and every other antivirus company, to identify malicious files.

- Click the history link to view the results of past malware scans:

**Scan**
[Settings](#)

REMOTE SCAN
MALWARE
VULNERABILITY

Overview

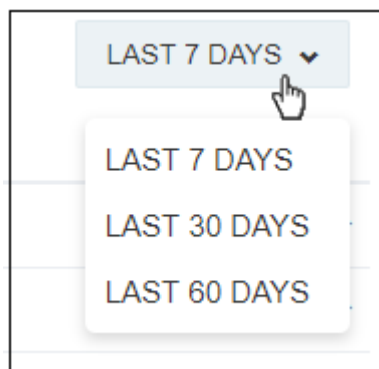
History

LAST 7 DAYS

DATE	SCAN RESULT
Aug 12	Malware Found
Aug 12	Malware Found
Aug 11	Malware Found
Aug 11	Malware Found
Aug 10	Malware Found
Aug 10	No malware found.
Aug 9	Malware Found
Aug 9	Malware Found
Aug 8	Malware Found
Aug 8	Malware Found

First Previous 1 2 Next Last

- Select the result period at top-right:



- Click a row to expand and view malware scan details:

#	FILE VERDICT	FILE PATH	SHA1
1	Backdoor.2863	./assets/backup/index.php	e2e5857e5dcdcf1182c13467347d078b14eb8331
2	9.1.9.TrojWare.5848	./assets/plugins/forgotmanagerlogin/efe94786.ico	4b20cda2836ee00a99ab8add4d23b569c438afd5
3	9.1.9.TrojWare.5842	./manager/media/rss/extlib/jercqvh.php	b398f0048c92b651a3f401b8d5066cc7b65ffdbf
4	Backdoor.2387	./scripts/index.php	6e09e83cbf21e834b1bc4510c172fcd77ec48c7
5	Backdoor.2387	./tours/cgi-bin/index.php	97e33809b9aad714bccb29bdd982dfca52109e1
6	Backdoor.2387	./manager/actions/index.php	076d0049f15ab5d8358bb0b05d5d80cd425f8aec
7	Backdoor.2387	./index.php	b0d32e4f0388beb0b9bb1e693785238c970c9100

- Click the row again to collapse the details.
- Request Malware Cleanup - Instruct Comodo technicians to remove the malware. See the next section for more on this.

### Submit a malware cleanup request

- You can request Comodo technicians professionally remove any malware found by a cWatch scan.
- The request form lets you pick the exact issue, or issues, you would like us to deal with
  - You can also tell cWatch to auto-create a clean up request whenever malware is found. See **'Configure Notification and Automatic Malware Removal'**.

### Request malware removal

- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Scan' tab then 'Malware' > 'Overview'
  - Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'
- Click the 'Request Malware Cleanup' link:

Overview

History

Malware Scanner is active.

**Force Run A Scan**  
**Request Malware Cleanup**

**Malware Found**

#	FILE VERDICT	FILE PATH	SHA1
1	Backdoor 1252	/images/stories/hrd.gif	a32d6677602a7d8a8c2e6f8f6d73f34b0409afa7
2	Backdoor 2338	/ccadence.com/limesurvey/framework/yilife.php	e02ea6426b10a6435e305870a572327a7b50e012
3	Backdoor 2319	/libranes/joomla/event/list.ctg	098bbcb376a96e51d7a6d7645463fab0666574
4	9.1.9 ApplicUnw nt.2140	/log/jhackguard-log.php	8edfd9200b116d2cd70e15fd45ca51c7bf671ec5

1

You will be taken to the support page to create a ticket:

**Support**

Your 'malware requests' would be listed here.  
Currently there are none in queue.

**Submit Malware Cleanup Request**

The screen above is shown if you have not yet submitted any requests.

- Click 'Submit Malware Cleanup Request'
- OR
- Click the '+' button:

**Support**

ALL OPEN TICKETS CLOSED TICKETS

**+**

ID	TYPE	DOMAIN	DESCRIPTION	STATUS
5938620	MRR	laghoo.com	Malware Report found 1 9.5.9...	CLOSED

First Previous 1 Next Last

This opens the removal request form:

### ← New Malware Removal Request

I'm having trouble with:

- Blacklisted site
- Google warning detected
- Sitecheckers uncovered an issue
- Unauthorized emails are being sent
- Hosting provider has detected malware on my site
- I see unknown strange files
- Unauthorized redirects
- Site does not load
- Want to perform a site health check
- After your cleanup my website stopped working

Domain:

Details:

Some files may be modified, removed, added, updated during the malware removal(clean up). We may access your admin panels and database. Submitting this request authorizes us to do all of the above.

- Select all issues affecting your site (optional)
- Enter any further information you feel is important in the 'Details' box
- Click 'Submit'.
- A request ID is created. Our technicians will access your site to remove the malware and remediate the issues.
  - Click 'Request ID' if you want to message the technician while the clean is in progress:

You will see the following when the cleanup is complete:

### ← 5551463(COMPLETED)

[Download Cleanup Report Progress](#)

**i** This ticket is closed. Please request new malware cleanup if you are still experiencing issues.

- **Download Cleanup Report** – Obtain 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

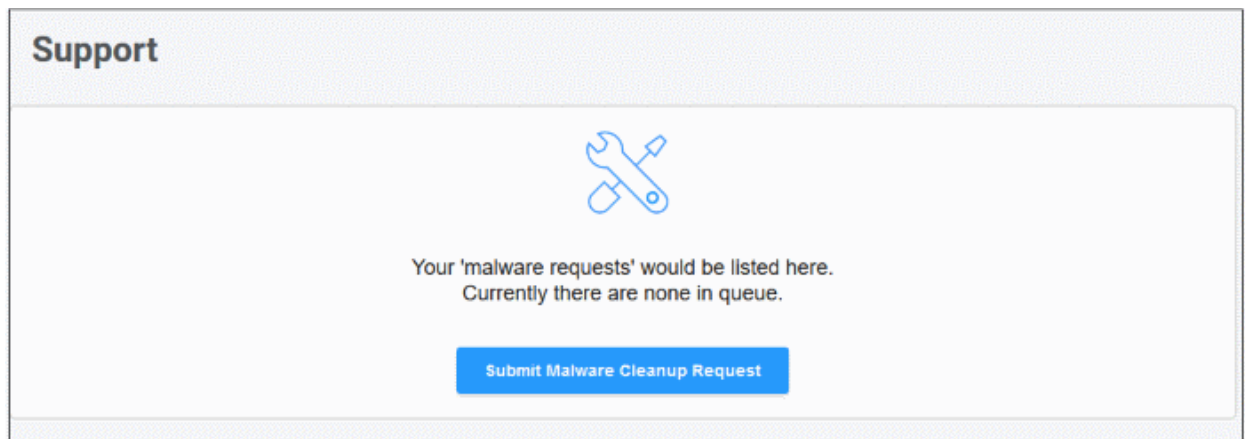
- You can initiate an on-demand malware scan and clean operation in one step.
- You can also configure the site for malware scans by uploading the malware scanner agent if the site is not pre-configured to enable scans.
- The malware removal request is submitted automatically if any threats are found at the end of the scan.

### Start a scan and submit malware cleanup request

- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Scan' tab then 'Malware' > 'Overview'
  - Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'



- Click 'Request Malware Cleanup'
- You will be taken to the support page to create a ticket:




The screen above is shown if you have not yet submitted any requests.

- Click 'Submit Malware Cleanup Request'
- OR
- Click the '+' button:



**Support**

ALL    OPEN TICKETS    CLOSED TICKETS



ID	TYPE	DOMAIN	DESCRIPTION	STATUS
5938620	MRR	laghoo.com	Malware Report found 1 9.5.9...	CLOSED

First   Previous   1   Next   Last

This opens the removal request form:

**← New Malware Removal Request**

I'm having trouble with:

- Blacklisted site
- Google warning detected
- Sitecheckers uncovered an issue
- Unauthorized emails are being sent
- Hosting provider has detected malware on my site
- I see unknown strange files
- Unauthorized redirects
- Site does not load
- Want to perform a site health check
- After your cleanup my website stopped working

Domain:

Details:

Some files may be modified, removed, added, updated during the malware removal(clean up). We may access your admin panels and database. Submitting this request authorizes us to do all of the above.

- Select all issues affecting your site
- Enter your message to the technician in the 'Details' text box
- If the website has already been enabled for malware scan, click 'Submit Request'.
  - The scan will start immediately.
  - 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.
  - View the cleanup report after the completion of cleaning as described **above**.
- If malware scanning has not been enabled on the site then you need to upload the scanner agent to the

site. Note - The following option only appears if malware scanning is not enabled, or if the FTP credentials have changed.

CONNECTION TYPE: FTP

FTP HOSTNAME: [ ] FTP PORT: [ ]

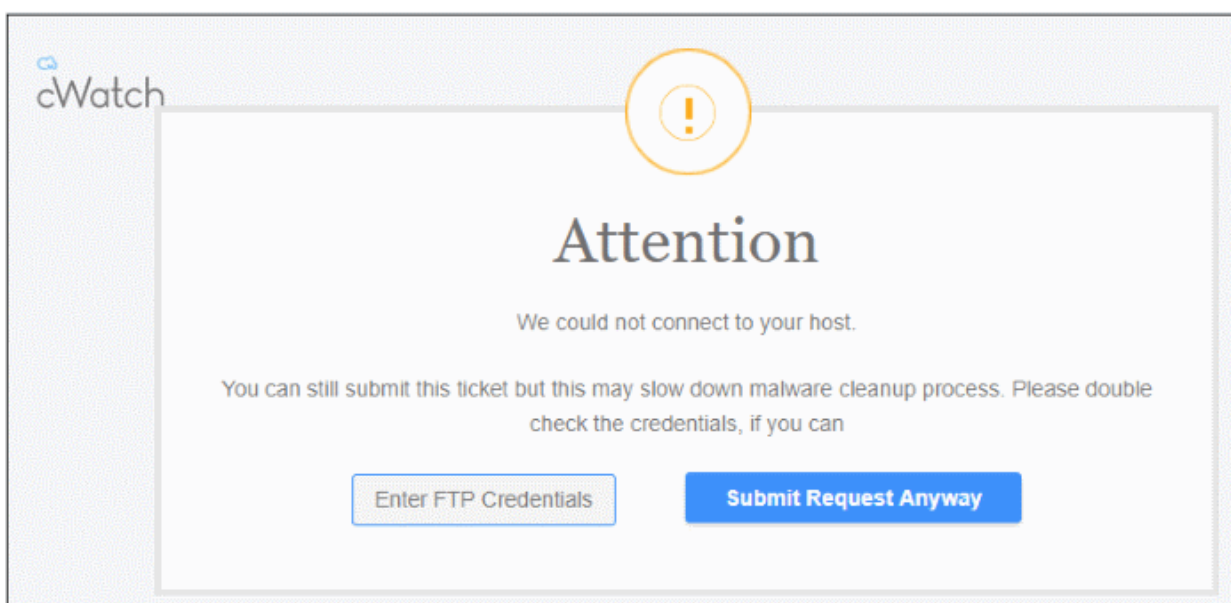
FTP USERNAME: [ ] FTP PASSWORD: [ ] FTP DIRECTORY: [ ]

Some files may be modified, removed, added, updated during the malware removal(clean up). We may access your admin panels and database. Submitting this request authorizes us to do all of the above.

Buttons: Cancel, Submit

- Enter your website's FTP details then click 'Submit'
- You can configure the FTP settings in the malware page or upload the agent manually. See '**Automatic Configuration**' and '**Manual Configuration**' for help with malware scanner configuration.

The following alert is shown if you submit the request without providing FTP details:



Comodo recommends you provide FTP details for quicker resolution of the request.

- Click 'Submit Request Anyway'. Note – This will slow down the malware cleanup process.

### 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.

### View the malware scan results

- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Scan' tab then 'Malware' > 'Overview'

- Or click the hamburger button then 'Scan' > 'Malware' > 'Overview'

**Malware Scanner is active.**

Force Run A Scan

[Request Malware Cleanup](#)

---

## Malware Found

#	FILE VERDICT	FILE PATH	SHA1
1	Backdoor.2867	./crayonweb.site/wp-includes/wp-tmp.php	58aa9e41a5f1cd8c58571bf8c677d8e3438921e
2	1.TrojWare.3458	./crayonweb.site/wp-content/themes/twentyseventeen/functions.php	33b5f73418a309ceca720e3aff584c91a17d2b78
3	1.TrojWare.3458	./wp-content/themes/twentyseventeen/functions.php	5000fec709f842d5e6ac1c4a903a9186a562bb7b
4	9.1.9.Applic.Unwnt.2139	./crayonweb.site/wp-content/plugins/ol_scrapes/classes/class-ol-scrapes.php	0d865f0f9bfa3e5a4e5742c44d959e5b5fc76489
5	1.TrojWare.3458	./crayonweb.site/wp-content/themes/twentyfifteen/functions.php	466bd9573cedf18bd626247e44828994063b246c
6	1.TrojWare.345	./crayonweb.site/wp-content/themes/twentsixteen/functions.php	b3fa57f19468e9eedef4e6587a82cec865f5da3

**File Verdict** – Name of the malicious item

**File Path** – Location of the item on your webserver

**SHA1** – File hash of the malicious item. Hash values are used by Comodo, and every other antivirus company, to positively identify malicious files.

- Click the history link to view results of past malware scans:

**Scan**
[Settings](#)

REMOTE SCAN
MALWARE
VULNERABILITY

Overview

History

LAST 7 DAYS ▾

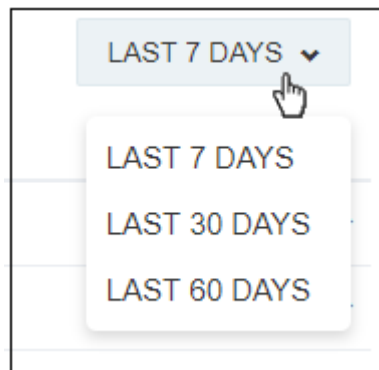
DATE	SCAN RESULT
Aug 12	Malware Found
Aug 12	Malware Found
Aug 11	Malware Found
Aug 11	Malware Found
Aug 10	Malware Found
Aug 10	No malware found.
Aug 9	Malware Found
Aug 9	Malware Found
Aug 8	Malware Found
Aug 8	Malware Found

First Previous 1 2 Next Last

- Select the result period at top-right:

Comodo cWatch Web Security - Website Administrator Guide | © 2019 Comodo Security Solutions Inc. | All rights reserved.

59



- Click a row to expand and view malware scan details:

Overview  
History

REMOTE SCAN MALWARE VULNERABILITY

LAST 7 DAYS

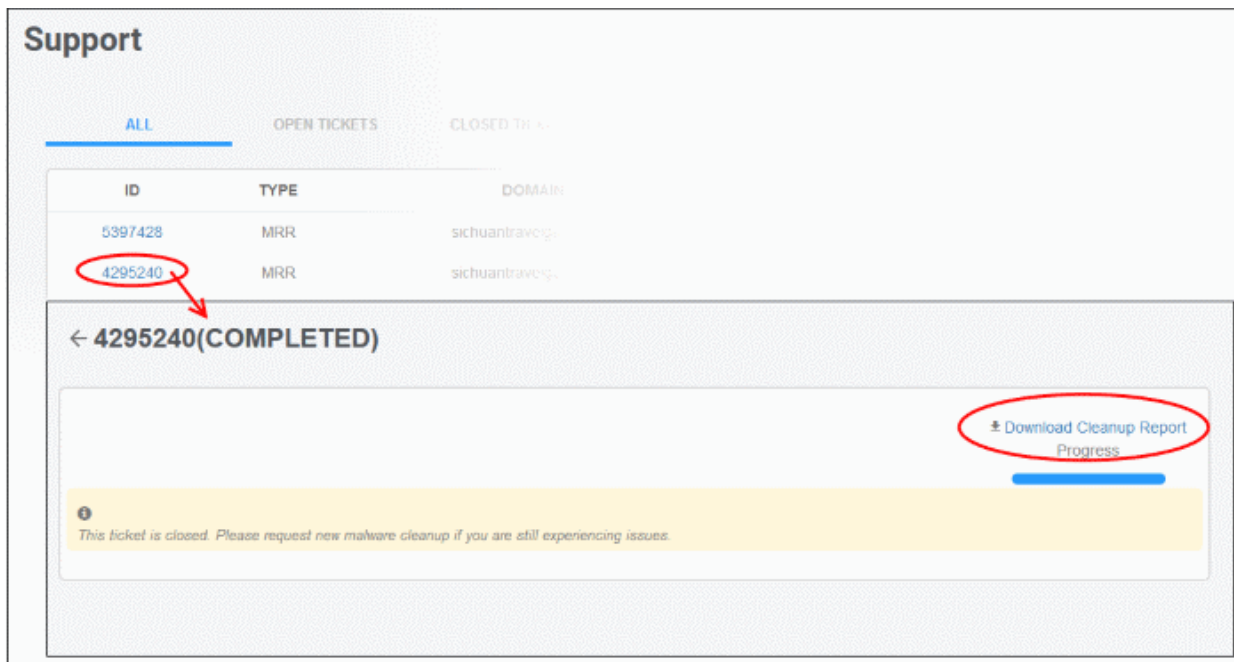
DATE SCAN RESULT

Aug 12 Malware Found

#	FILE VERDICT	FILE PATH	SHA1
1	Backdoor.2863	/assets/backup/index.php	e2e6857e5dcdcf1182c13467347d078b14eb8331
2	9.1.9.TrojWare.5848	/assets/plugins/forgotmanagerlogin/efe94786.ico	4b20cda2836ee00a99ab8add4d23b569c438afd5
3	9.1.9.TrojWare.5842	/manager/media/rss/extlib/jercqvh.php	b398f0048c92b651a3f401b8d5066cc7b65fddf
4	Backdoor.2387	/scripts/index.php	6e09e83cbf21e834b1bc4510c172fcd77ec48c7
5	Backdoor.2387	/tours/cgi-bin/index.php	97e33809b9aad714bccb29bdd982dbfca52109e1
6	Backdoor.2387	/manager/actions/index.php	076d0049f15ab5d8358bb0b05d5d80cd425f8aec
7	Backdoor.2387	/index.php	b0d32e4f0388beb0b9bb1e693785238c970c9100

1

- Click the row again to collapse the details.
- Click 'Request Malware Cleanup' in the overview screen to instruct Comodo technicians to remove the malware.
- To download a cleanup report, go to support page then click the request ID:



**Support**

ALL OPEN TICKETS CLOSED TICKETS

ID	TYPE	DOMAIN
5397428	MRR	sichuantravel.com
4295240	MRR	sichuantravel.com

← 4295240(COMPLETED)

Download Cleanup Report Progress

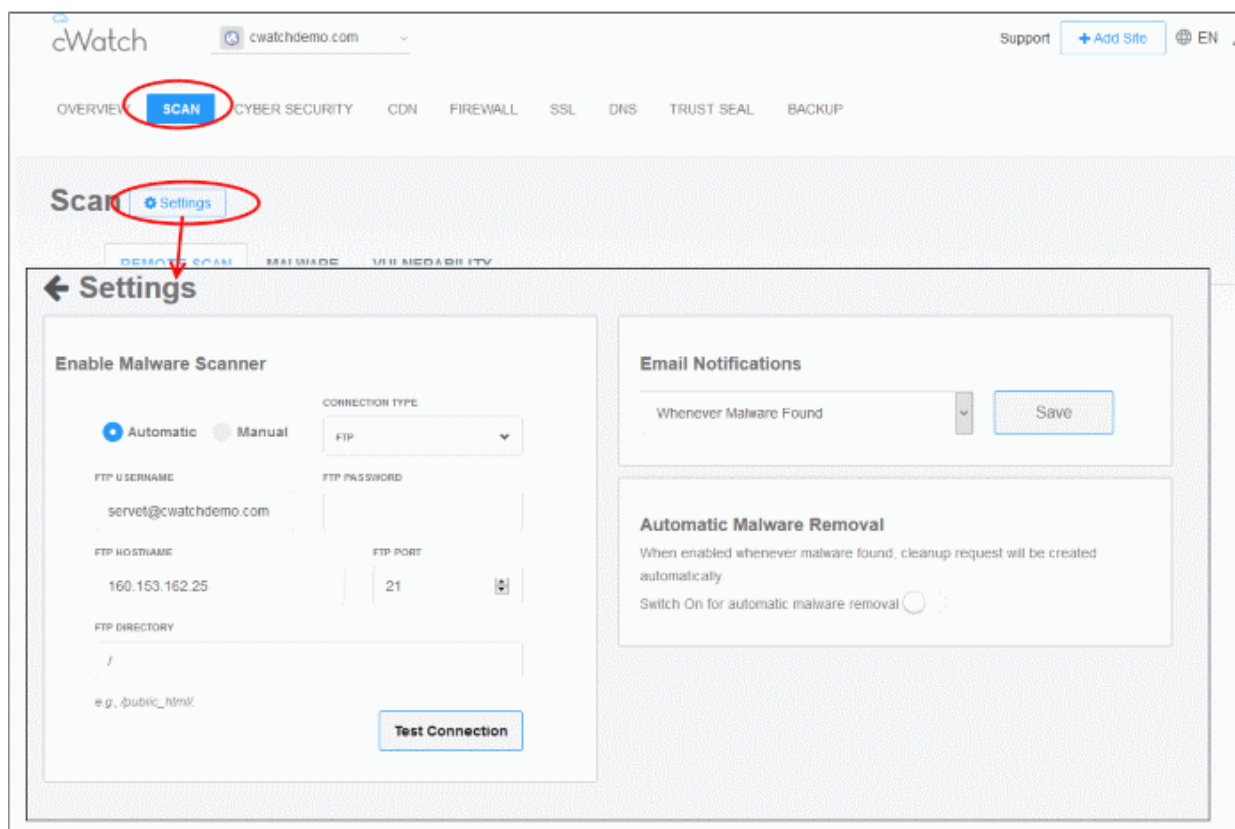
**i**  
This ticket is closed. Please request new malware cleanup if you are still experiencing issues.

- Click 'Download Cleanup Report' and save the file. See '**Get Support**' for more details.

#### 4.2.2.3 Configure Notifications and Automatic Malware Removal

cWatch sends alerts if malware is found after a scan. You can also tell cWatch to auto-submit a clean up request if malware is found.

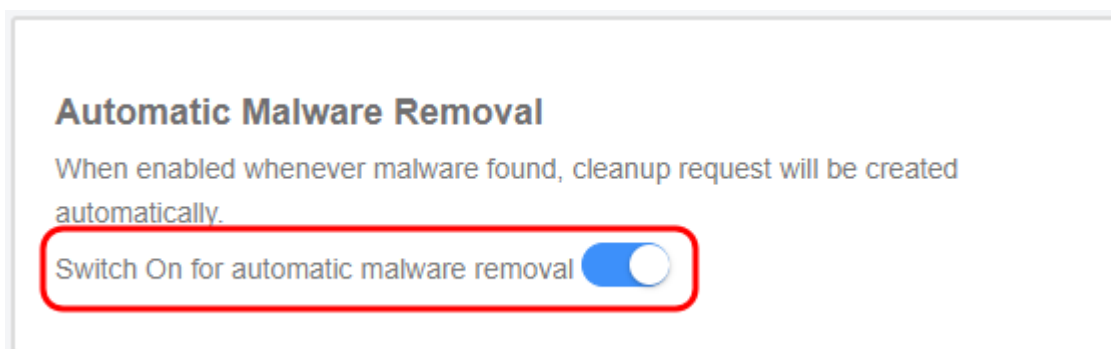
- Open the cWatch dashboard
- Select a website from the menu at top-left and choose 'Scan'
- Click 'Settings'



**Enable Malware Scanner** – See '[Configure Malware Scan Settings](#)'

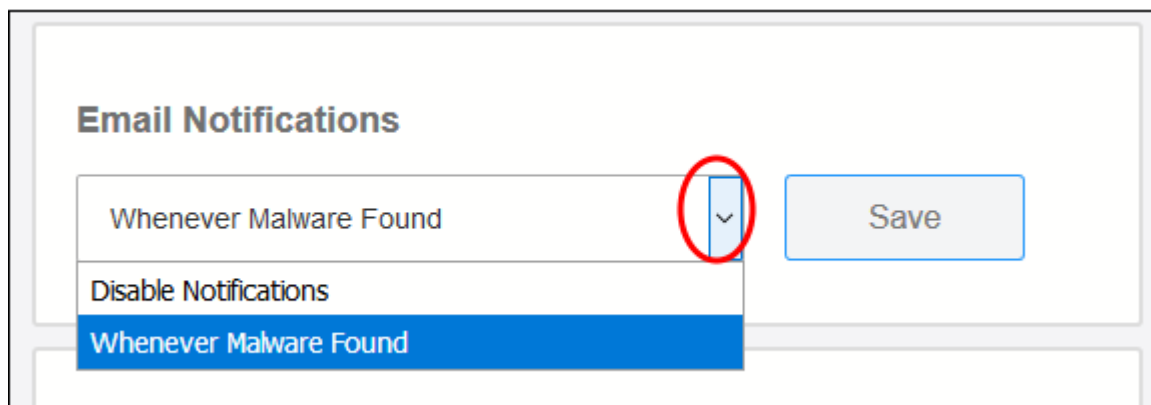
#### Automatic Malware Removal:

- You can configure cWatch to auto-submit a malware removal request if threats are discovered. You can enable this setting on a per-website basis.
- Auto-removal is enabled by default for 'Pro' and 'Premium' licenses. The scan and cleanup automatically takes place according to your schedule.
- Auto-removal is not included with basic licenses. If you enable automatic removal, you will be prompted to upgrade your license for the website
- You can enable/disable auto-removal requests with the switch highlighted below:



#### Email Notifications

Email notifications are enabled by default for all license types. The notifications are sent to the registered email address for the account.



- **Whenever Malware Found** – Alerts are sent if malware is detected by a scan. We recommend you keep this setting.
- **Disable Notifications** – No alerts are sent. You will need to log into cWatch to view security information about your sites.
- Click 'Save' to apply your changes

### 4.2.3 Vulnerability Scans

- Select a website from the drop-down at top-left
- Click 'Scan' > 'Vulnerability'

cWatch can perform two types of vulnerability scans:

- CMS vulnerabilities
- OWASP Top Ten threats

#### **CMS Vulnerabilities**

- A scan that searches for known weaknesses 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 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. From here, you can also:

- Run on-demand scans on a site
- 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](#)

#### 4.2.3.1 CMS Vulnerability Scans

- Select a website from the drop-down at top-left
- Click 'Scan' > 'Vulnerability'
- 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

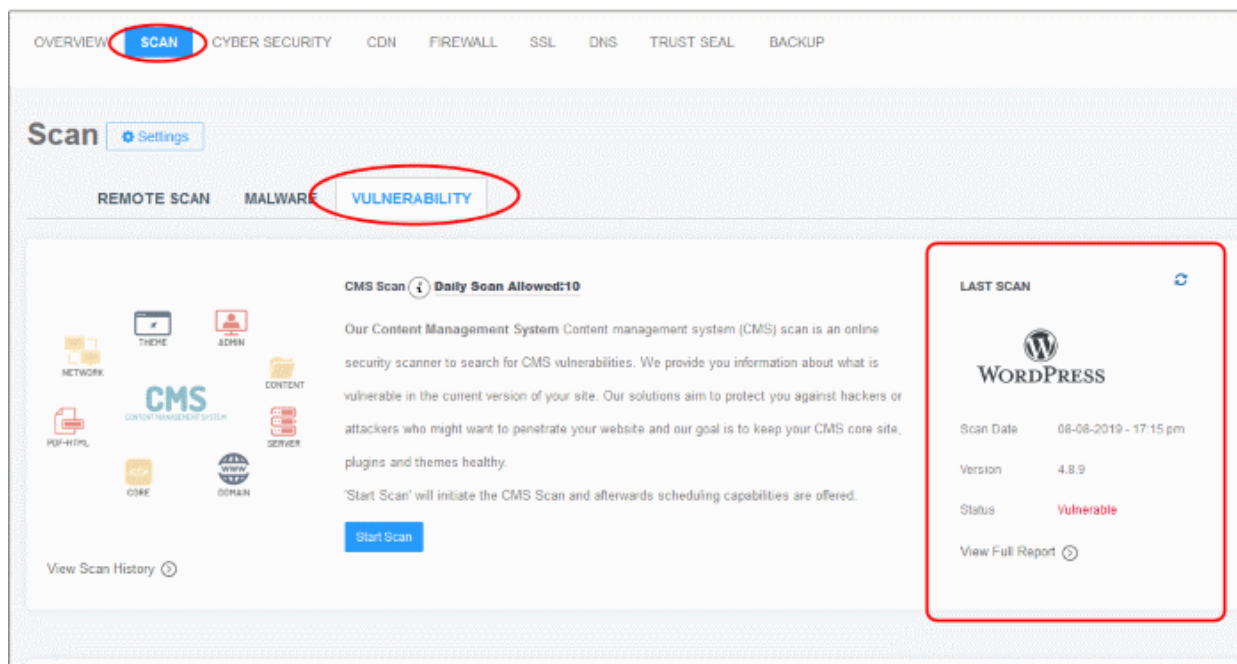
You can run manual CMS scans and view the results from the last ten scans.

Note – Remote scan also detects CMS vulnerabilities. Clicking the 'Vulnerabilities Detected' link in the remote scan overview section leads to this page. See ['Remote Scans'](#)

##### Run a CMS scan

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





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

- **Scan Date** - When the most recent discovery was run.
- **Version** - The version number of the 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 format not identified' - 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.

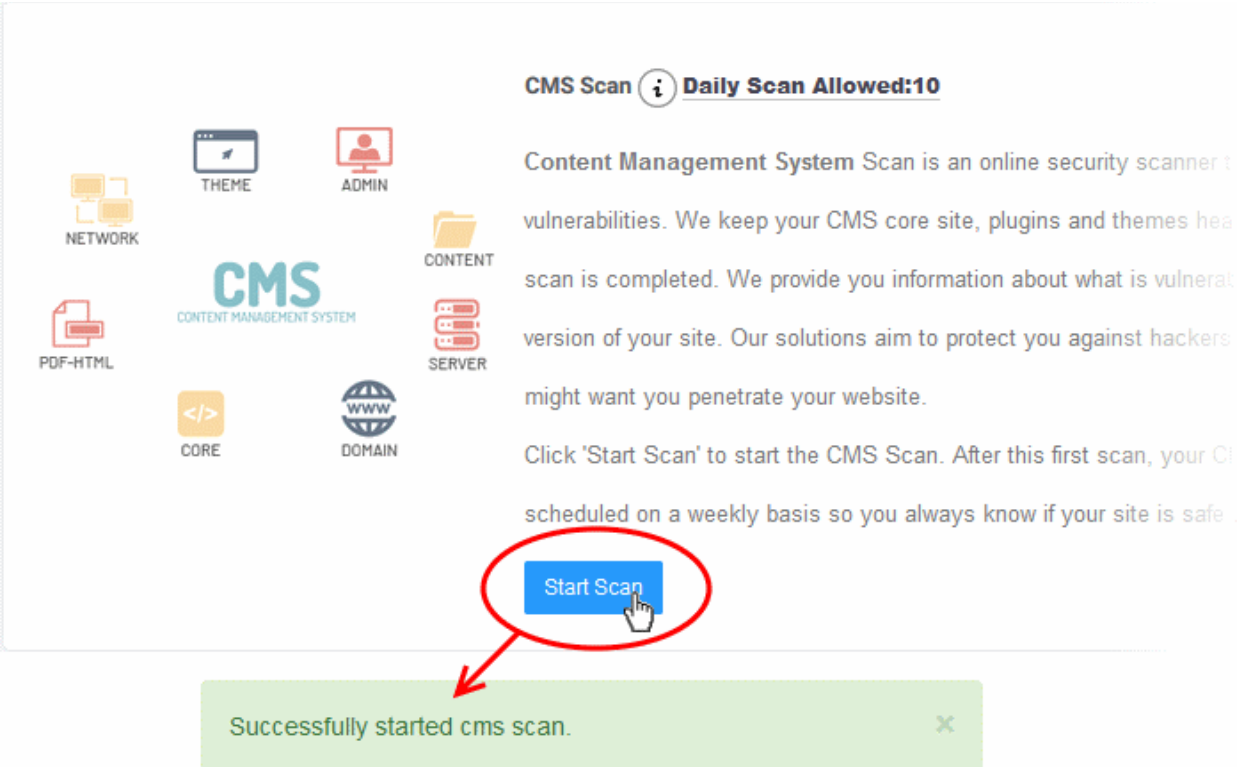
The pane lets you:

- **Run an on-demand scan**
- **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:

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



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

Content Management System Scan is an online security scanner that checks for vulnerabilities. We keep your CMS core site, plugins and themes healthy. Once the scan is completed. We provide you information about what is vulnerable in the current version of your site. Our solutions aim to protect you against hackers who might want you penetrate your website.

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

Start Scan

Successfully started cms scan. X

- 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.

### View detailed results

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability'
  - Or click the hamburger button and select 'Scan' > 'Vulnerability'
- Click 'View Full Report' under 'Last Scan' in the CMS scan pane as shown below:

The screenshot displays the 'LAST SCAN' section for a WordPress website. The scan date is 08-03-2019 - 02:56 am, the version is 5.1, and the status is 'Not Vulnerable'. A red circle highlights the 'View Full Report' link, with a red arrow pointing to the 'CMS Scan History' section below. The 'CMS Scan History' section shows a table of scan dates for March 2019, with the 23rd highlighted. A blue notification box states 'Translations for the vulnerabilities are not available.' Below the table, there are tabs for 'CORE', 'PLUGIN', and 'THEME'. A '+' icon is visible next to the WordPress logo.

March 23 2019	March 16 2019	March 09 2019	March 09 2019	March 08 2019

WordPress Scan Date: 23-03-2019 19:38 pm | Version: 5.1.1 | 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.

March  
23  
2019

March  
16  
2019

March  
09  
2019

March  
09  
2019

March  
08  
2019

CORE   PLUGIN   THEME

---

-

**WORDPRESS**

woocommerce

Scan Date: 23-03-2019 19:38 pm

Version: 3.4.2

Status: Vulnerable

VULNERABILITY	PATCH FIX ↕	REFERENCE ↕	FOUND IN ↕	LATEST VERSION ↕
XSS vulnerability in WordPress Plugin woocommerce before 3.5.1	3.5.1	<a href="https://www.ripstech.com/php-security-calendar-2018/#Day23">https://www.ripstech.com/php-security-calendar-2018/#Day23</a>	--	--
OBJECTINJECTION vulnerability in WordPress Plugin woocommerce before 3.4.5	3.4.5	<a href="https://woocommerce.wordpress.com/2018/08/29/woocommerce-3-4-5-security-fix-release-notes/">https://woocommerce.wordpress.com/2018/08/29/woocommerce-3-4-5-security-fix-release-notes/</a>	--	--
RCE vulnerability in WordPress Plugin woocommerce before 3.4.6	3.4.6	<a href="https://www.ripstech.com/php-security-calendar-2018/#day-3">https://www.ripstech.com/php-security-calendar-2018/#day-3</a> <a href="#">See More</a>	--	--
PRIVESC vulnerability in WordPress Plugin woocommerce before 3.4.6	3.4.6	<a href="https://woocommerce.wordpress.com/2018/10/11/woocommerce-3-4-6-security-fix-release-notes/">https://woocommerce.wordpress.com/2018/10/11/woocommerce-3-4-6-security-fix-release-notes/</a> <a href="#">See More</a>	--	--
OBJECTINJECTION vulnerability in WordPress Plugin woocommerce	3.4.6	<a href="https://medium.com/websec/woocommerce-and-azis-with-scoth-bc9d561377e1">https://medium.com/websec/woocommerce-and-azis-with-scoth-bc9d561377e1</a> <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.

- Select the target website from the menu at top-left

- Click the 'Scan' tab then 'Vulnerability'
  - Or click the hamburger button and select 'Scan' > 'Vulnerability'
- Click 'View Scan History' in the 'CMS Scan' pane

The screenshot shows the 'CMS Scan' section of the Comodo cWatch Web Security interface. The 'View Scan History' link is circled in red, with a red arrow pointing to the 'CMS Scan History' window below. The 'CMS Scan History' window displays a calendar for March 2019 with dates 23, 16, 09, 09, and 08. Below the calendar, there are tabs for 'CORE', 'PLUGIN', and 'THEME'. The 'CORE' tab is selected, showing a scan for 'WordPress' on '23-03-2019 19:38 pm' with a status of 'Vulnerable'. A blue notification bar at the top right of the history window states: 'Translations for the vulnerabilities are not available.'

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.

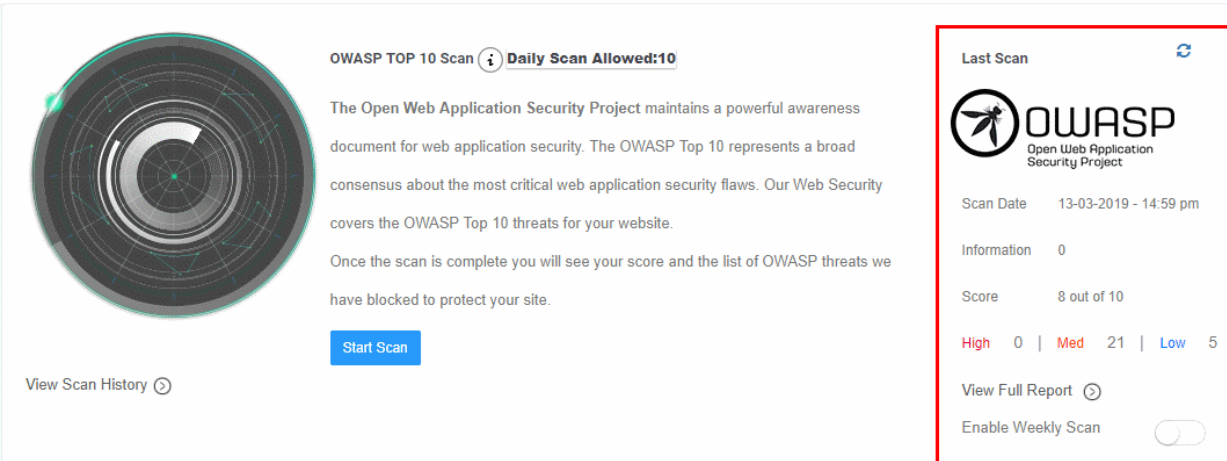
### 4.2.3.2 OWASP Top 10 Vulnerability Scans

- Select a website from the drop-down at top-left and choose 'Scan' > 'Vulnerability'
- 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 and shows 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

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

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



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


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

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

[Start Scan](#)

[View Scan History](#) ⓘ

**Last Scan** ⓘ

 **OWASP**  
Open Web Application Security Project

Scan Date 13-03-2019 - 14:59 pm

Information 0

Score 8 out of 10

High 0 | Med 21 | Low 5

[View Full Report](#) ⓘ

Enable Weekly Scan

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

- Scan Date - When the last WASP vulnerability 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.

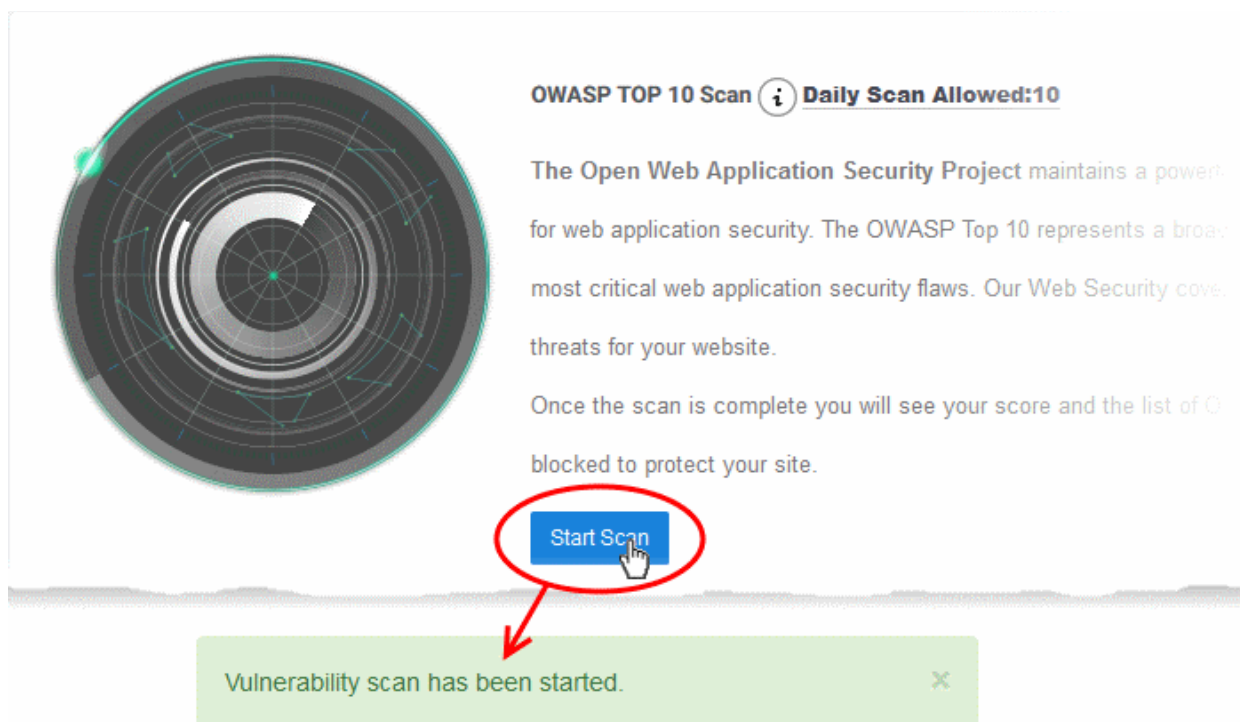
The pane lets you:

- **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:

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability'
  - Or click the hamburger button and select 'Scan' > 'Vulnerability'
- Click 'Start Scan' in the 'OWASP Top 10 Scan' pane:



- 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 OWASP scans on any of your websites

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability'
  - Or click the hamburger button and select 'Scan' > 'Vulnerability'
- Use the switch in the OWASP pane to enable the weekly scan, as shown in the screenshot below:

scan ⓘ **Daily Scan Allowed:10**

Application Security Project maintains a powerful awareness of application security. The OWASP Top 10 represents a broad range of the most critical web application security flaws. Our Web Security tool identifies the Top 10 threats for your website. After the scan is complete you will see your score and the list of OWASP threats we detected on your site.

**Last Scan**

**OWASP**  
Open Web Application Security Project

Scan Date 13-03-2019 - 14:59 pm

Information 0

Score 8 out of 10

High 0 | Med 21 | Low 5

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

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability'
  - Or click the hamburger button and select 'Scan' > 'Vulnerability'
- Click 'View Full Report' under 'Last Scan' in the 'OWASP Top 10' Scan pane

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



**Daily Scan Allowed:10**

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

complete you will see your score and the list of OWASP threats we protect your site.

Last Scan ↻

Scan Date 13-03-2019 - 14:59 pm

Information 0

Score 8 out of 10

High 0 | Med 21 | Low 5

[View Full Report](#) ➤

Enable Weekly Scan

---

← OWASP Scan History

March 13 2019

March 08 2019

Translations for the vulnerabilities are not available.

---

Scan Date: 13-03-2019 - 14:59 pm

High 0 | Med 21 | Low 5

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 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 servers, web

## OWASP Top 10 Vulnerabilities - Column Descriptions

Column Header	Description
Rank	Severity, or criticality, of the attack category.
Vulnerabilities	Number of threats in this category that were found on your site. <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 <b>View Details of Identified Vulnerabilities</b> for more details</li> </ul>

Comodo cWatch Web Security - Website Administrator Guide | © 2019 Comodo Security Solutions Inc. | All rights reserved.

73

Description	A short explanation 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

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability'
  - Or click the hamburger button and select 'Scan' > 'Vulnerability'
- 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 OWASP Top 10 vulnerabilities. The 'A6' category is highlighted with a red circle and a hand icon. A red arrow points from this category to a detailed dialog box titled 'A6 VULNERABILITY DETAIL'. The dialog box contains a list of specific threat types found within that category:

Threat Type	Count
Unhandled error in web application	7
Code disclosure vulnerability	1

A 'Close' button is located in the bottom right corner of the dialog box.

The details dialog shows a list of specific threat types 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** 7

Vulnerabilities:

- Medium http://www.domain1.com/
- Medium http://www.domain1.com/wp-content/plugins/hello.php
- Medium http://www.domain1.com/PHPinfo.php
- Medium http://www.domain1.com/index.php
- Medium http://www.domain1.com/wp-login.php
- Medium http://www.domain1.com/INSTALL.php
- Medium http://www.domain1.com/test.php

**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 with their risk level.
- 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.

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability'
  - Or click the hamburger button and select 'Scan' > 'Vulnerability'
- 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 aware document for web application security. The OWASP Top 10 represents a bi consensus about the most critical web application security flaws. Our Web Security covers the OWASP Top 10 threats for your website.

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

[Start Scan](#)

[View Scan History](#) ⓘ

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

March	March	March	March	March
<b>21</b>	18	13	13	13
2019	2019	2019	2019	2019

**OWASP SAFE** Scan Date: 21-03-2019 - 14:46 pm High 0 | Med 0 | Low 8 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

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

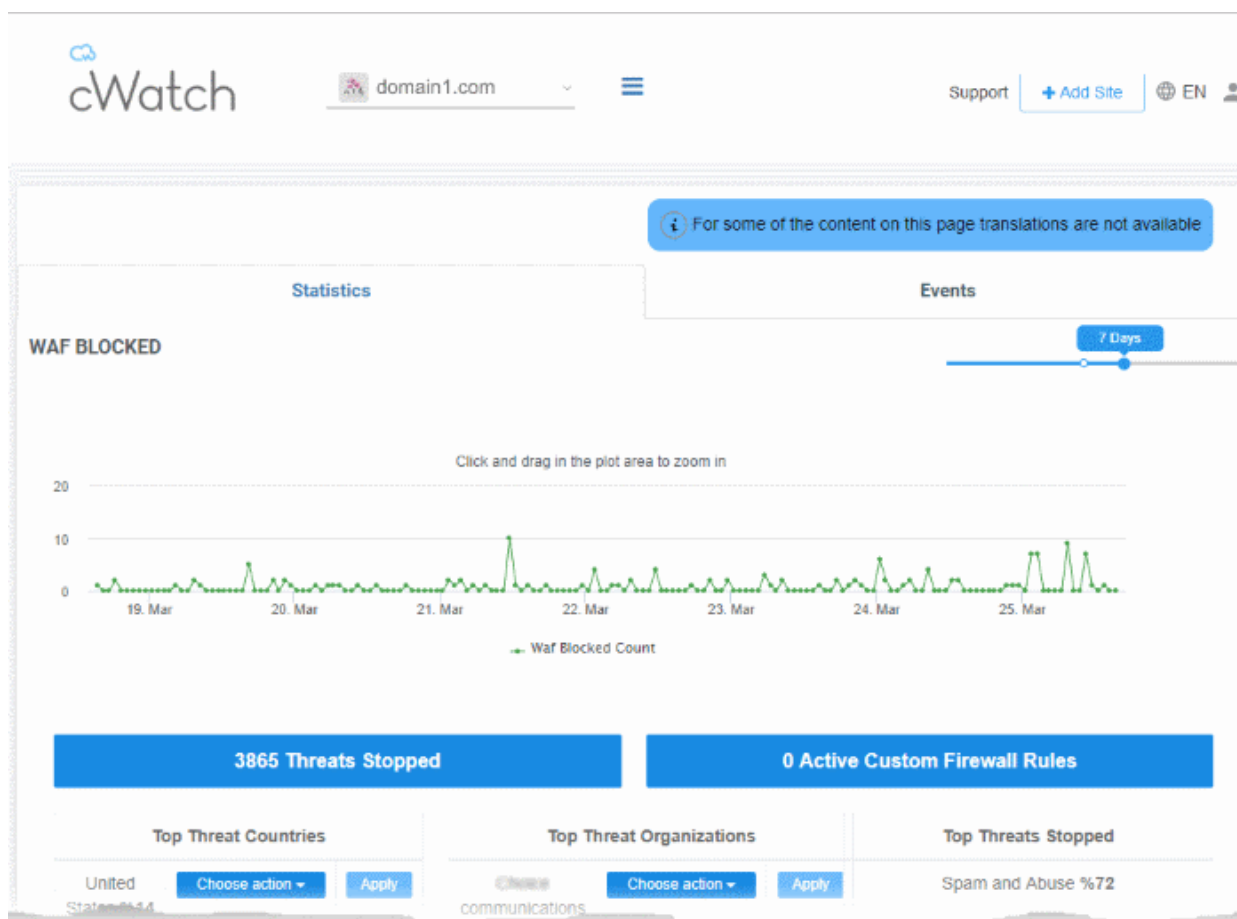
See **View detailed results of the last scan** if you need more help with this.

## 4.3 Cyber Security Operation Center Results

- Select a website from the drop-down at top-left and choose 'Cyber Security'
- The Cyber Security Operation Center (CSOC) is a dedicated team of Comodo technicians who investigate and remove threats discovered by cWatch.
- The team monitors events on customer websites in real-time. Using this information, they constantly update security rules on the site to deliver unrivaled protection.
- 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 in the future.

### Open CSOC page of a website

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



The 'Cyber Security Operation Center' 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.

### 4.3.1 WAF Statistics

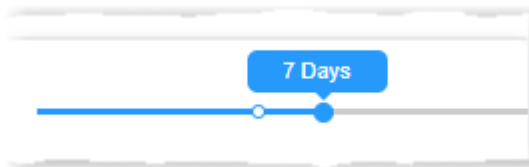
- Choose a website from the drop-down at top-left
- Click 'Cyber Security' > 'Statistics' tab
- The statistics page shows attacks identified and blocked by the Web Application Firewall (WAF). This includes the top 5 attack types and top 5 attack sources.
- You can also choose the action taken on future threats from the same source. cWatch updates your WAF rules accordingly.

#### Important Notes:

- The web application firewall is only available for 'Pro', 'Premium' and 'WAF Starter' licenses.
- To enable WAF protection, you need to change the authoritative DNS of the site to Comodo Secure DNS. You can also enable this by adding a CNAME entry to your DNS records. See [DNS Configuration](#) for help on this.

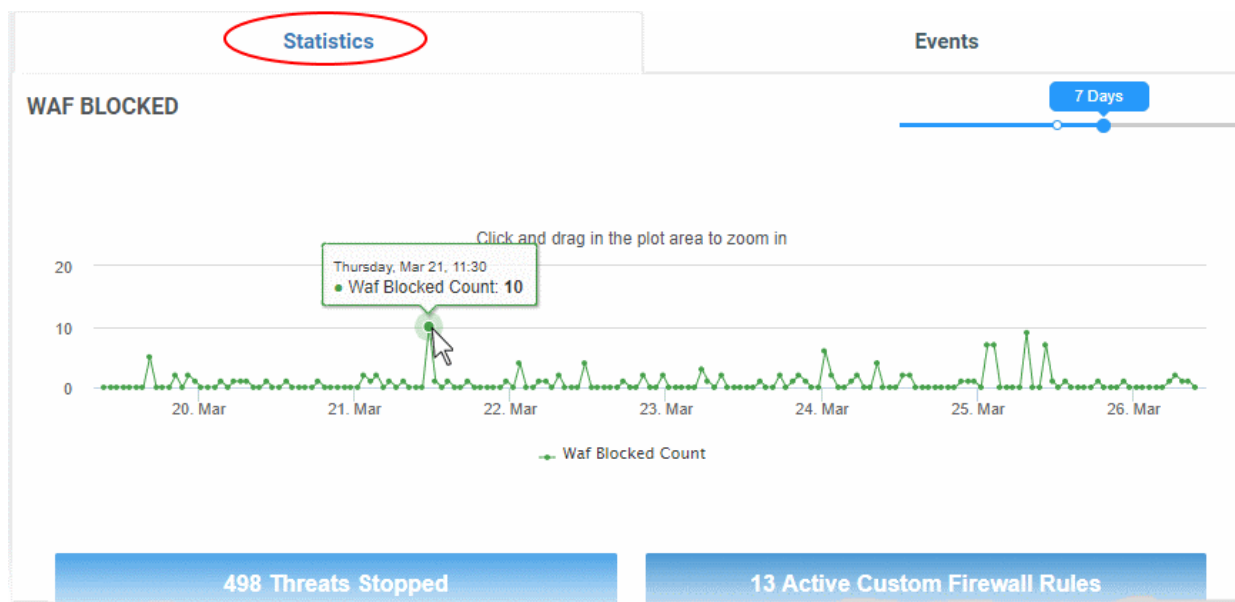
#### View WAF statistics

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Cyber Security' tab
  - Or click the hamburger button and select 'Cyber Security'
- Open the 'Statistics' tab if not already open
- Select the period for which you want to view statistics from the slider at top-right:



#### WAF Blocked

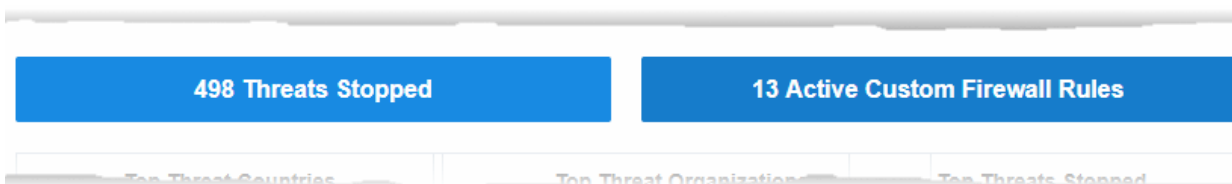
A timeline of attacks blocked by the web application firewall (WAF). The WAF is constantly and automatically updated with new rules to combat the latest threats.



- 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.



- **<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 **Manage Custom Firewall Rules** for more details.

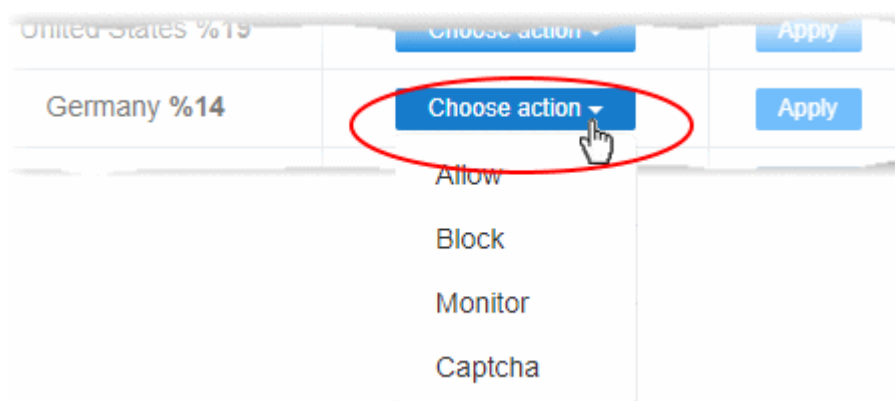
## Top Countries

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

Top Threat Countries		
India %35	Choose action ▾	Apply
United States %19	Choose action ▾	Apply
Germany %14	Choose action ▾	Apply
Belgium %4	Choose action ▾	Apply
Viet Nam %3	Choose action ▾	Apply

**Choose action** - Specify how to deal with future traffic from the country:

- The action you choose here will create a custom firewall rule for traffic from the country.
- Note - Custom firewall rules require a 'Premium' license for the website.



- **Allow** - All traffic from the country is permitted. This includes legitimate traffic, bots, malicious

traffic 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 establish what kind of traffic will be affected and so avoid creating a rule that might negatively impact users.
- **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 your choices:

- Edit the rule name and conditions if required
- Click 'Add Condition' if you want to append more conditions to the rule
- Click 'Save' to add the rule.

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



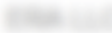


RULE ID	RULE NAME	TYPE	DETAILS	ACTION
1222040	Monitor Germany	Country	DE	Monitor

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

### Top Organizations

The 5 companies, networks or other entities from which most attacks originated. You can also see the percentage of all attacks that came from the entity.



Top Threat Organizations		
 %35	Choose action ▾	Apply
 %10	Choose action ▾	Apply
 %10	Choose action ▾	Apply
 %4	Choose action ▾	Apply
 %2	Choose action ▾	Apply

**Choose action** - Specify how to deal with future traffic from the organization / entity.

- The rest of the process is similar to creating a rule for a country. See the [explanation above](#).
- See [Manage Custom Firewall Rules](#) for help with custom firewall rules.

### Top Threats

The top 5 attack types blocked by WAF:

Top Threats Stopped
Spam and Abuse %35
Traffic Via Proxy Networks %34
Traffic From Hosting Services %16
CSRF %11
Invalid User Agent Prevention %1

### 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.

### 4.3.2 WAF Events

- Choose a website from the drop-down at top-left
- Click 'Cyber Security' > 'Events'
- The events page lists all access attempts intercepted by the Web Application Firewall (WAF) rules. This includes both built-in rules and any custom 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 how to deal future incidents of the same type from the same source . cWatch updates your WAF rules automatically.

#### Notes

- The web application firewall is only available for 'Pro', 'Premium' and 'WAF Starter' licenses.
- To enable WAF protection, you need to change the authoritative DNS of the website to Comodo Secure DNS. You can also enable this by adding a CNAME entry to your DNS records. See [DNS Configuration](#) for help on this.

#### View WAF Events

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

- Or click the hamburger button and select 'Cyber Security'
- Open the 'Events' tab

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 captcha verification
IP	The IP address of the source of the access request
Country	The country from which the access request came
Date	The date and time of the access request

### Sorting and Filtering options:

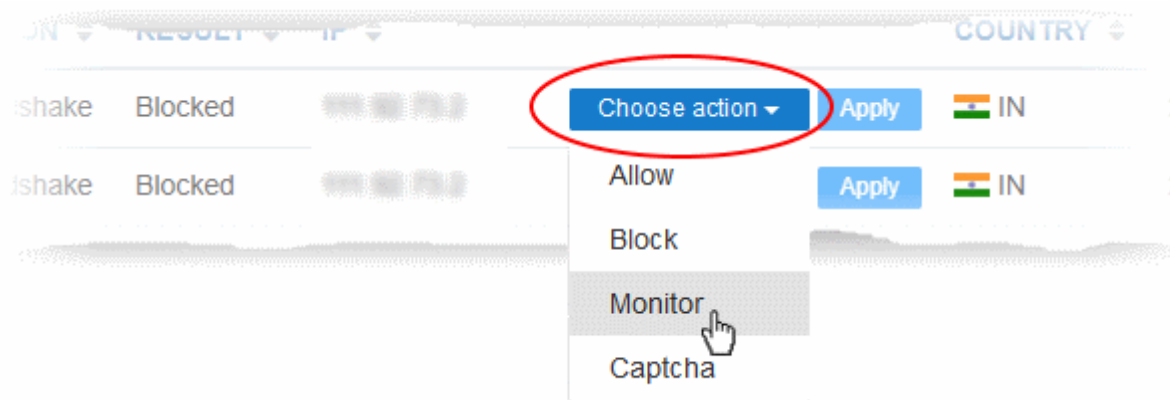
- Use the buttons along the top to filter events by action taken on the traffic

- 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

- **Choose an action** - Specify how to deal with future traffic from the IP address.
  - The action you choose here will create a custom firewall rule for traffic from the IP:



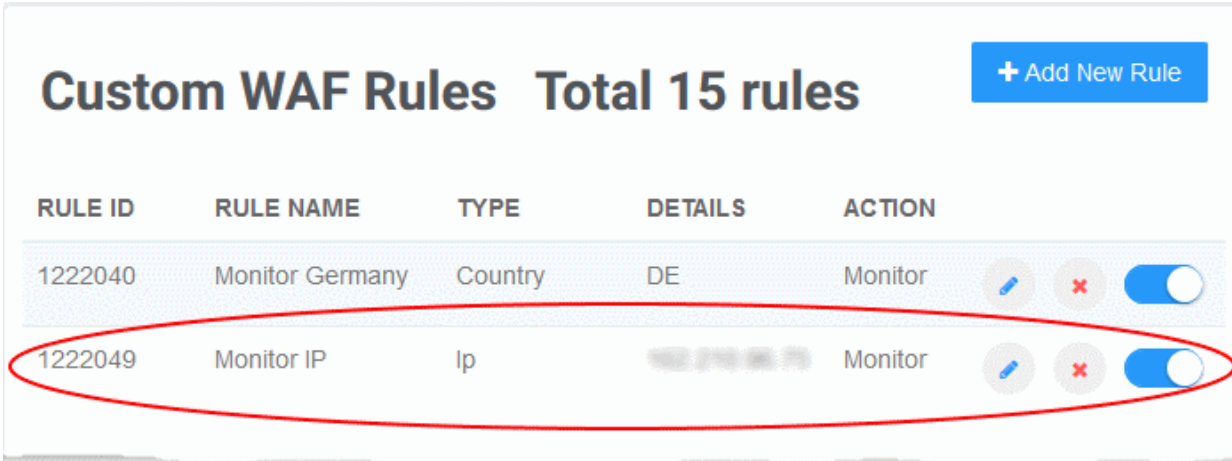
- **Allow** - All traffic from the IP is permitted. This includes legitimate traffic, bots, malicious traffic etc.
  - **Block** - No traffic is allowed from the IP. An error message is shown to users.
  - **Monitor** - Traffic from the IP is recorded. This action is particularly useful for testing out potential 'Captcha' and 'Block' rules. You can establish what kind of traffic will be affected and so avoid creating a rule that might negatively impact users.
  - **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 your choices:






 A screenshot of the 'ADD NEW RULE' dialog box. The title bar is blue with the text 'ADD NEW RULE' and a close button 'X'. The main area has a white background. There is a text input field for 'Enter Rule Name:' containing 'Monitor IP'. Below that is a condition field: 'If: IP = 192.168.1.1'. The 'Then the action is:' dropdown is set to 'Monitor'. At the bottom right, there are two buttons: '+ Add Condition' and 'Save'.

- Edit the rule name and conditions if required
- Click 'Add Condition' if you want to append more conditions to the rule
- 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 15 rules + Add New Rule

RULE ID	RULE NAME	TYPE	DETAILS	ACTION	
1222040	Monitor Germany	Country	DE	Monitor	  
1222049	Monitor IP	Ip	192.168.1.1	Monitor	  

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

## 4.4 Content Delivery Network

- Select a website from the drop-down at top-left
- Choose 'CDN'
- Your cWatch license includes a content delivery network (CDN) for your websites. The service will improve page load-times for your customers and improve the reliability/uptime of your site.
- You can 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 'CDN' > 'Settings' > 'Activation'. The CNAME entry is generated by cWatch. See [Activate CDN for a Website](#) for more details.

Once activated and configured, the CDN service will:

- Accelerate performance by delivering site content from data centers closest to your visitor's location.
- Forward event logs to the Comodo CSOC team who will monitor the traffic for unusual 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.

See the following sections for more help on CDN configuration:

- [Activate CDN for a Website](#)
- [Configure CDN Settings](#)
- [View CDN Metrics](#)

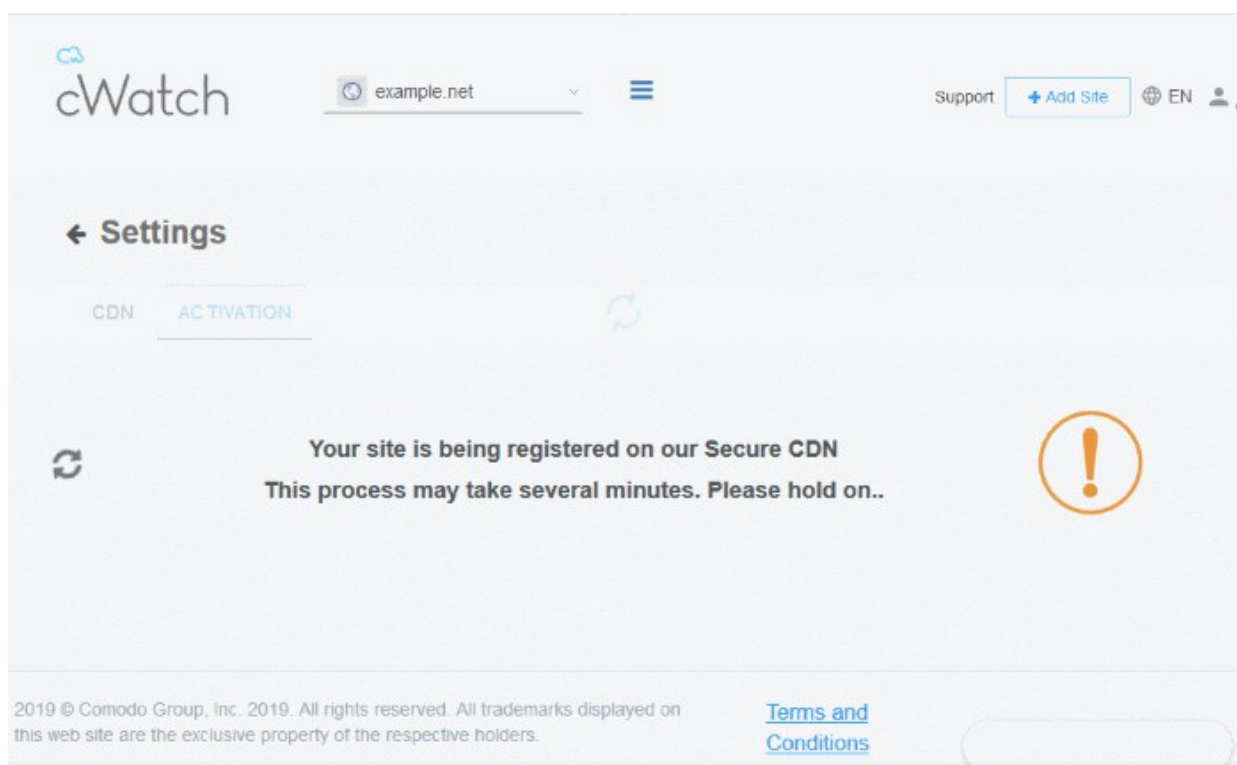
### 4.4.1 Activate CDN for a Website

- Select a website from the drop-down at top-left
- Click 'CDN' > 'Settings' > 'Activation'
- You need to change your site's authoritative DNS server to Comodo DNS in order to activate the content delivery network.
- Alternatively, you can add a CNAME entry to your DNS records.
  - The CDN activation page has both authoritative name server (NS) and CNAME records for your site. You can use these to configure DNS.

#### Configure DNS settings of your website

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

cWatch first registers your site with the CDN service:



The NS records are generated after site registration:

← Settings

CDN **ACTIVATION**

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 Name Servers (NS)
- B) Enter DNS records explicitly

**A) CHANGE YOUR NAME SERVERS (NS)**

i. Go to 'DNS' page and click 'Next'

	TYPE	VALUE
ii. If the first step is completed, change nameservers(ns) to our Authoritative DNS	NS	ns1.dnsbycomodo.net ns2.dnsbycomodo.net ns3.dnsbycomodo.net ns4.dnsbycomodo.net

for DNS changes to be processed globally. There will

**B) ENTER DNS RECORDS EXPLICITLY**

You can configure your DNS using the instructions given below.

	TYPE	NAME	VALUE	STATUS
i. In order to set up <a href="#">www.example.net</a> please create a CNAME record with the value shown below.	CNAME	www	examplenet-1553659357-givkjgav4ntofwivqlm.stagings.ecurecdn.com	Not yet configured!
ii. In order to configure <a href="#">example.net</a> please create an A Record with the value shown below.	A	@	151.139.240.18	Not yet configured!

- There are two ways to configure your site to use our DNS:
  - **Change your domain's authoritative DNS servers to Comodo DNS**
  - **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.

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

Name server (NS) details are shown in the 'CDN' > 'Settings' > 'Activation' page:

**A) CHANGE YOUR NAME SERVERS (NS)**

**i. Go to 'DNS' page and click 'Next'**

	TYPE	VALUE
<b>ii. If the first step is completed, change nameservers(ns) to our Authoritative DNS</b>	NS	ns1.dnsbycomodo.net ns2.dnsbycomodo.net ns3.dnsbycomodo.net ns4.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 servers. Throughout this switch your site will remain available.*

*Once you have made the change to your nameservers, you will manage your DNS Records via our web portal.*

*This is locate once you login in the settings and manage DNS.*

*Not sure how to change nameservers? Try:*

**<https://support.google.com/domains/answer/3290309?hl=en>**

*Still need a help? Please contact our support professionals.*

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

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

- Select the target website from the menu at top-left
- Click the 'CDN' tab
  - Or click the hamburger button and select 'CDN'
- Click 'Settings'
- Select the 'Activation' tab
- Look at option 'A) Change nameservers to...':



**A) CHANGE NAMESERVERS(NS) TO OUR AUTHORITATIVE DNS**

		STATUS	
i. Go to 'DNS' page and click 'Next'		✔	
	TYPE	VALUE	STATUS
ii. If the first step is completed, change nameservers(ns) to our Authoritative DNS	NS	ns1.dnsbycomodo.net ns2.dnsbycomodo.net ns3.dnsbycomodo.net ns4.dnsbycomodo.net	✔

Name servers are set

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

**Note:**

- After changing to Comodo DNS, you have to use cWatch to manage your DNS settings.
- For example, changes to your MX records must be done in cWatch, not in your web host's DNS management page.

See '**Manage DNS Records**' in **DNS Configuration** for more information.

**Option B - Enter DNS records explicitly**

- The CNAME and A records for your site are shown in 'CDN' > 'Settings' > 'Activation':

**B) ENTER DNS RECORDS EXPLICITLY** 


You can configure your DNS using the instructions given below.



	TYPE	NAME	VALUE	STATUS
i. In order to set up <code>www.example.net</code> please create a CNAME record with the value shown below.	CNAME	www	examplenet-1553659357-givkjgav4ntofwivqlm.stagingsecurecdn.com	 Not yet configured!
ii. In order to configure <code>example.net</code> please create an A Record with the value shown below.	A	@	151.139.240.18	 Not yet configured!

- 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 to add '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 provider.
- 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.

- Select the target website from the menu at top-left
- Click the 'CDN' tab
  - Or click the hamburger button and select 'CDN'
- Click 'Settings' to open the 'CDN Settings' page
- Select the 'Activation' tab and scroll down to option 'B - Enter DNS Records Explicitly'

**B) ENTER DNS RECORDS EXPLICITLY** 

TYPE	NAME	VALUE		STATUS
CNAME	www	examplenet-1553659357-givkjgav4ntofwivqlm.stagingsecurecdn.com		Configured.
A	@	151.139.240.18		Configured.

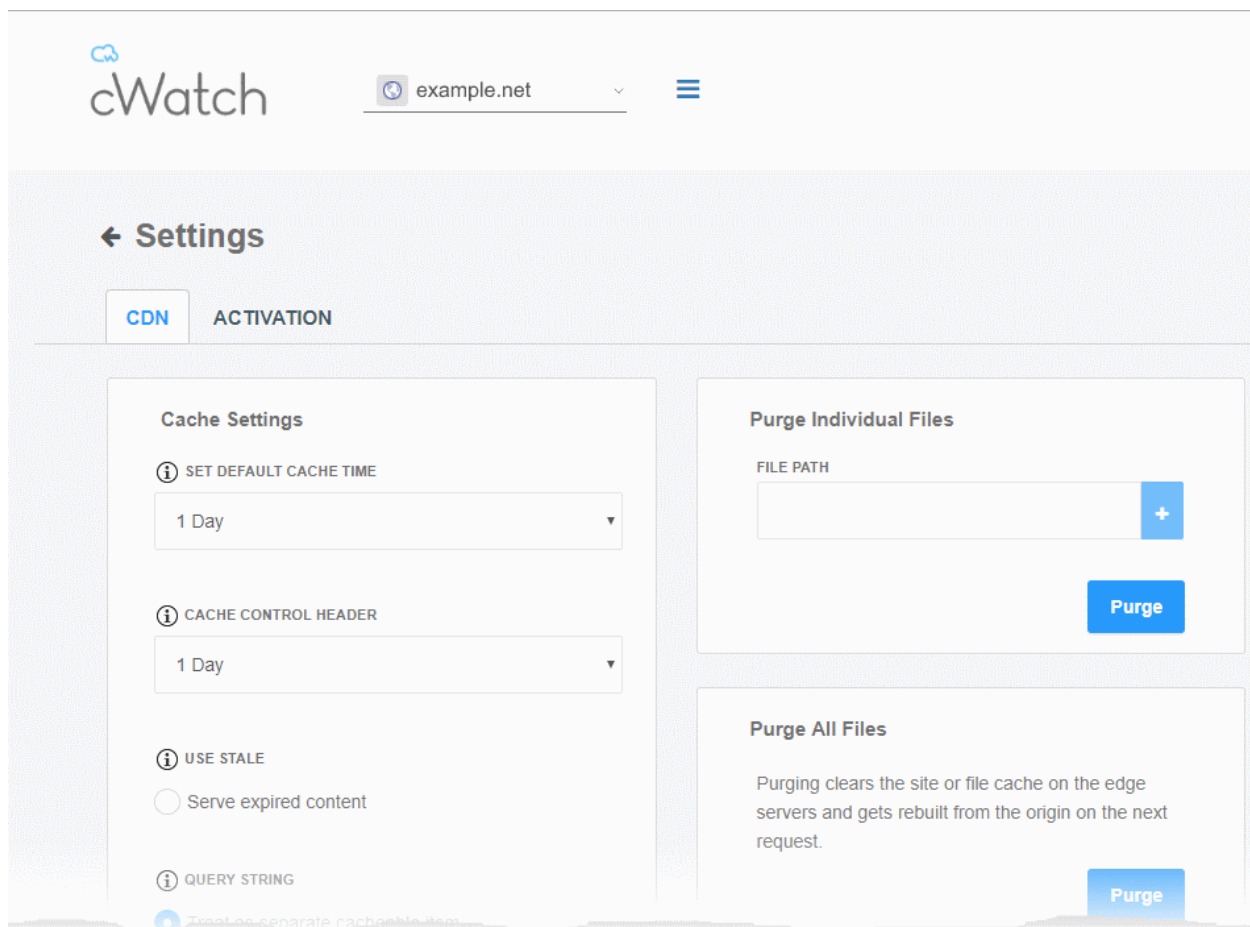
- You can view the confirmation under the 'Status' column.

## 4.4.2 Configure CDN Settings

- Choose a website from the drop-down at top-left and select 'CDN'
- Click 'Settings' > 'CDN'

The settings page lets you configure how website data is cached and rendered by the CDN edge servers.

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



## Cache Settings

### Cache Settings

**(i) SET DEFAULT CACHE TIME**

1 Day ▼

**(i) CACHE CONTROL HEADER**

1 Day ▼

**(i) USE STALE**

Serve expired content

**(i) QUERY STRING**

Treat as separate cacheable item

**(i) IGNORE CACHE CONTROL**

Ignore max age set by the origin

Update  
Cache  
Settings

Cache Settings - Table of Parameters

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

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

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

## Purge Files

**Purge Individual Files**

FILE PATH

+

Purge

---

**Purge All Files**

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

Purge

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

## Site Settings

### Site Settings

**i** ORIGIN IP RESOLUTION

ORIGIN IP

**i** CUSTOM HOST HEADER

**i** ORIGIN PROTOCOL

**Update**

Site Settings	
Origin IP Resolution	<p>Choose whether or not the CDN should use DNS servers to resolve the IP address of your web server.</p> <p>Whether you enable this option depends on whether your server uses a static or dynamic IP.</p> <ul style="list-style-type: none"> <li>• <b>Static IP</b> - Enable 'Origin IP Resolution'. The CDN will fetch your IP address by domain look-up, and display it in the 'Origin IP' field. The CDN will use this IP to fetch and cache files from your web server.</li> <li>• <b>Dynamic IP</b> – Disable 'Origin IP Resolution'. The CDN will use DNS services to resolve your IP address.</li> </ul>
Custom Host Header	Enter the custom host header in this field if the host header for your site is different to the domain name.
Origin Protocol	Choose whether the CDN should use website with SSL certificate or not.

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

## Edge Settings

**Edge Settings**

**ⓘ GZIP COMPRESSION**

Serve compressed files with GZip

**ⓘ CONTENT DISPOSITION**

Force files to download

**ⓘ REMOVE COOKIES**

Ignore cookies in requests

**ⓘ PSEUDO STREAMING**

Enable pseudo stream seeking

**ⓘ ADD XFF HEADER**

Add X-Forwarded-For HTTP Header

**ⓘ ADD CORS HEADER**

Allow Cross Origin Resource Sharing

**ⓘ ENABLE WEBP**

Allow separate caching for WebP files

## Edge Settings - Table of Parameters

Parameter	Description
Gzip Compression - Server compressed files with GZip	Reduces the size of files for faster network transfers. Optimizes bandwidth usage and increases transfer speeds to browsers.
Content Disposition - Force Files to download	Forces the files to download instead of showing the content in the browser
Remove Cookies - Ignore cookies in requests	CDN ignores header cookies
Pseudo Streaming - Enable pseudo stream seeking	Plays media files (FLV and MP4 files only with H.264 encoding)
Add XFF Header - Add X-Forwarded for HTTP Header	The CDN identifies the actual IP address of the client connecting to the website. This is used to render location based content, logging and more.
Add CORS Header - Allow Cross Origin Resource Sharing	Appends 'Access-Control-Allow-Origin' header to responses
Enable WebP - Allow separate caching for WebP files	Currently being developed by Google, WebP is an image format that provides both lossy and lossless compression. If enabled, cWatch will have separate cache for these files.

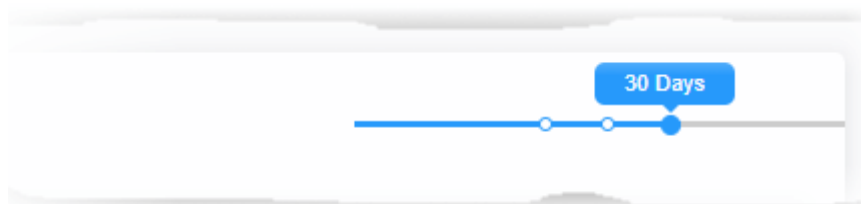
- Click 'Update' for your settings to take effect.

### 4.4.3 View CDN Metrics

- Select a website from the drop-down at top-left and choose 'CDN'
- The metrics page shows your site's traffic usage, the origins of your traffic, and page error/status codes.

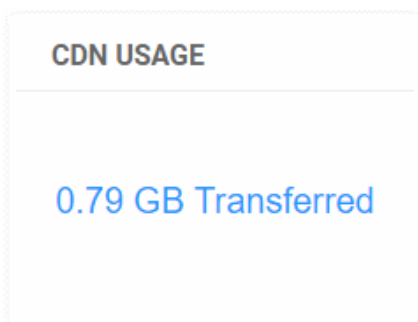
#### View CDN metrics

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'CDN' tab
  - Or click the hamburger button and select 'CDN'
- Select the period for which you want to view the metrics from the slider at top-right:



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

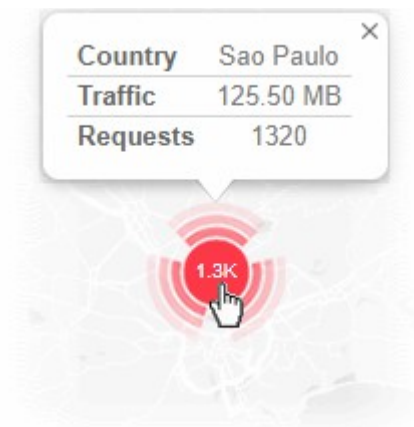
The request and bandwidth map shows the regions from which your traffic originated. You can also view the number of access requests from each region.



## REQUEST AND BANDWIDTH BY EDGE LOCATION

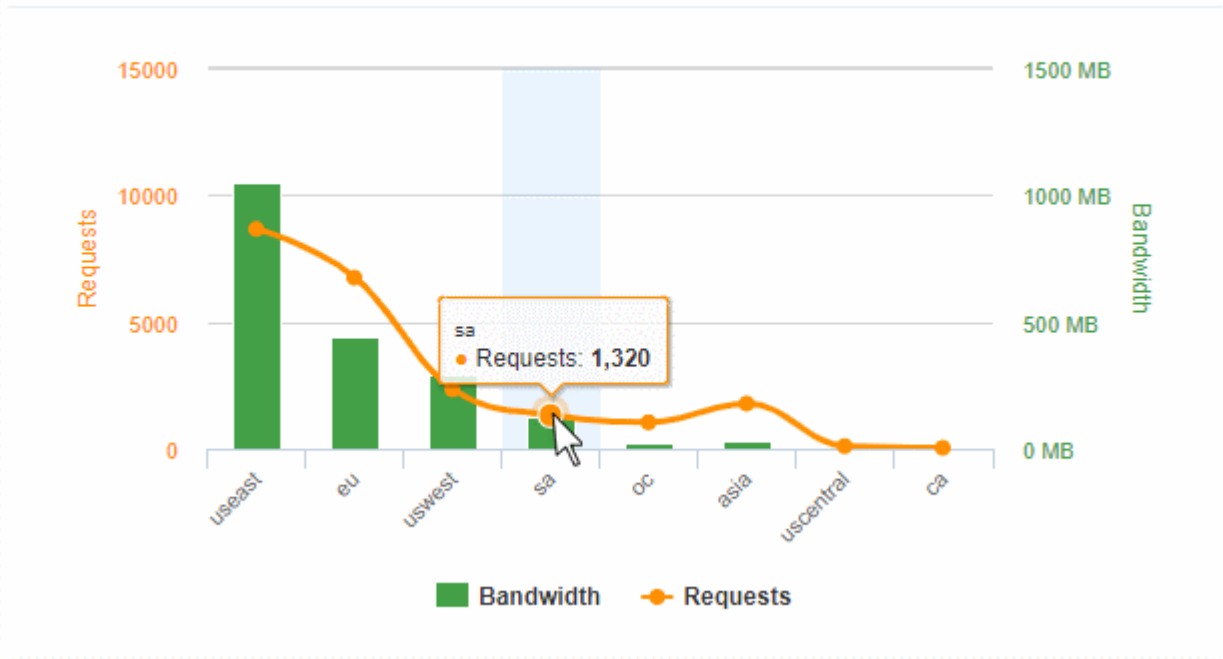


- Click on an regional hot-spot to view the traffic and number of access requests from that area.

**Request and Bandwidth by Region**

Shows the number of site requests and the amount of data downloaded by each continent.

### REQUEST AND BANDWIDTH BY REGION

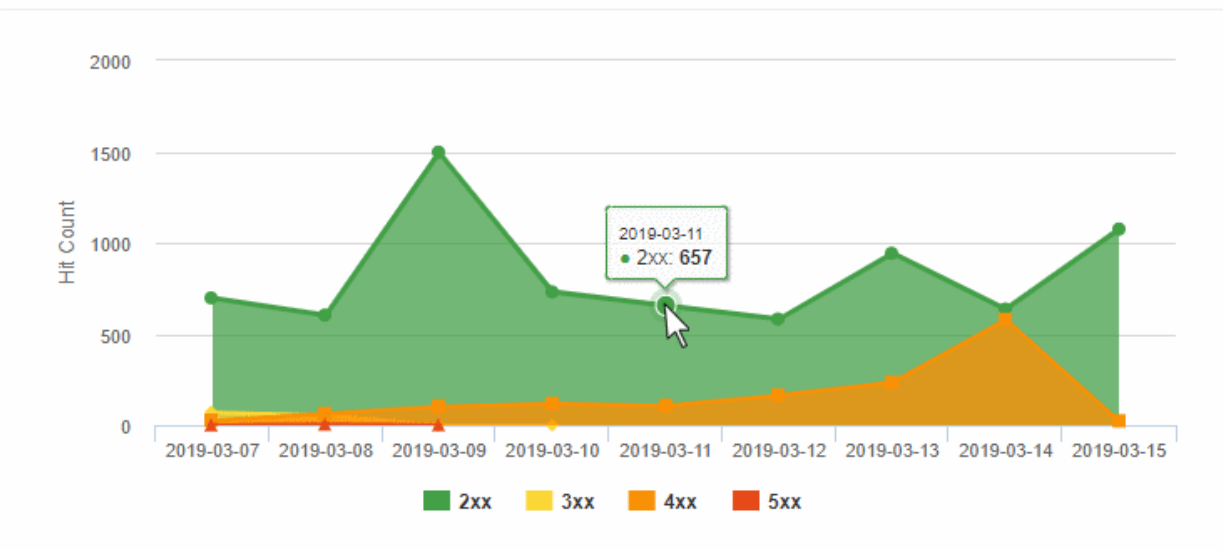


- Select a portion of the graph to zoom-in
- The yellow line graph shows the number of requests from different continents
  - Place your mouse on the line to view the number of requests from the respective continent
- The green bar graph shows the bandwidth usage from different continents
  - Place your 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

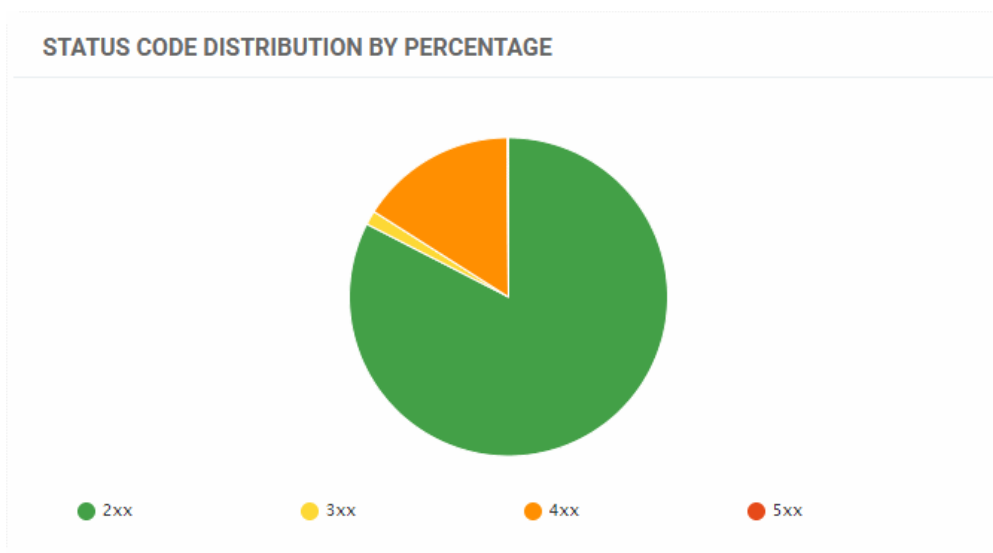
- 3xx = Redirection
- 4xx = Client errors
- 5xx = Server errors
- You can choose the time period using the slider at top-right.
- You can choose the time period using the slider at top-right.
- Select a portion of the graph to zoom-in
- Place your mouse on the graph to view the number of responses of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

### Status Code Distribution by Percentage

- The percentage of HTTP response status codes generated by your site within the set time period.

HTTP status codes are as follows:

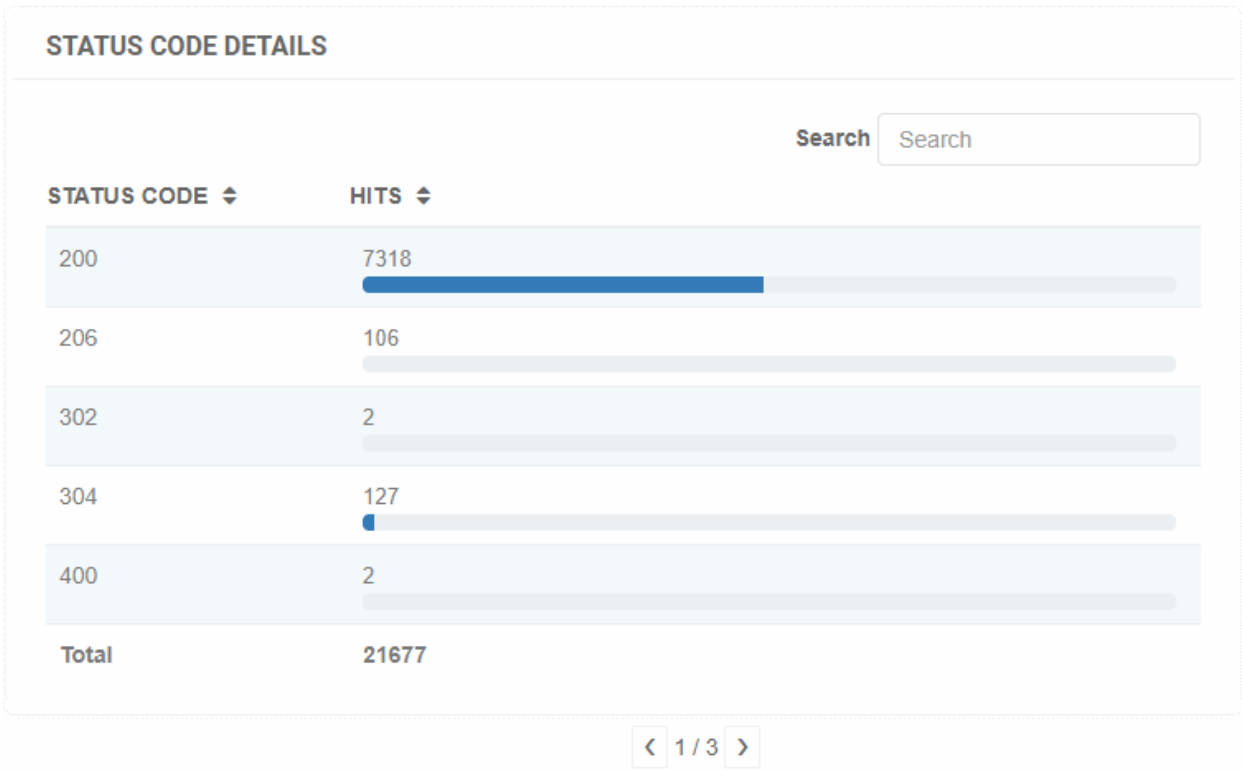
- 1xx Informational responses.
- 2xx Success.
- 3xx Redirection.
- 4xx Client errors.
- 5xx Server errors.



- Place your mouse on a sector the to view the number of responses of that type

### Status Code Details

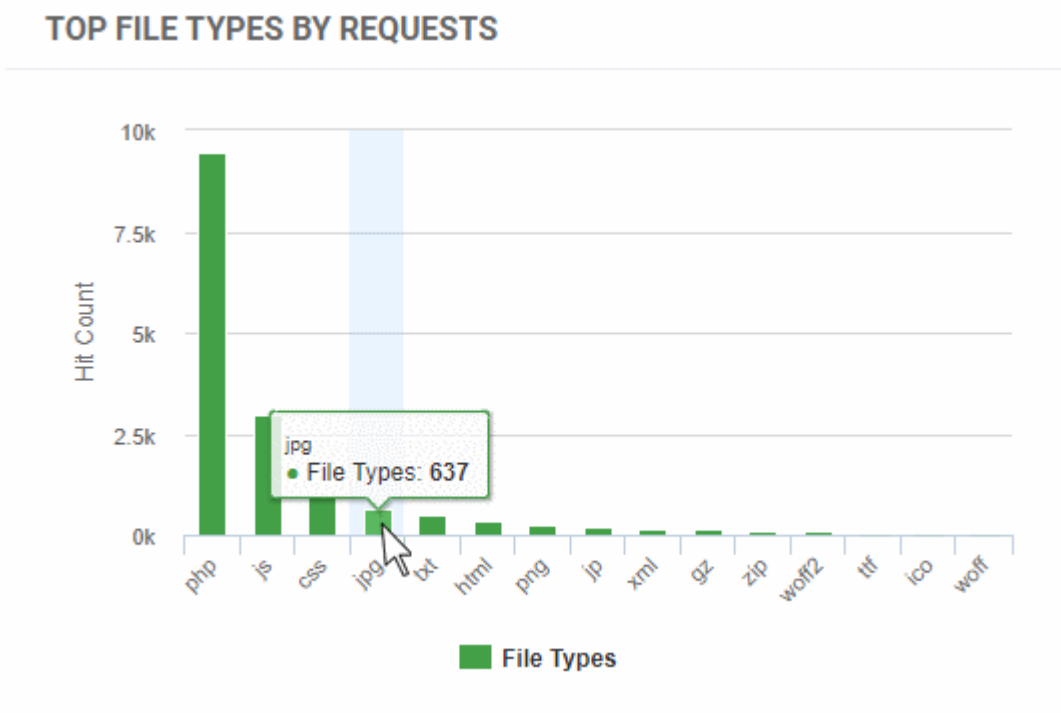
- Lists how many of each HTTP response code were shown in the selected time period.
  - '200' class codes - Success. Page displayed correctly/The server was able to fulfil the request
  - '300' class codes - Redirection. The user requested a page but was redirected to a different page.
  - '400' class codes – Errors. The requested page could not be provided for some reason.
- A more 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).



- 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.
- Use the arrows at the bottom to navigate to successive pages

### Top File Types by Requests

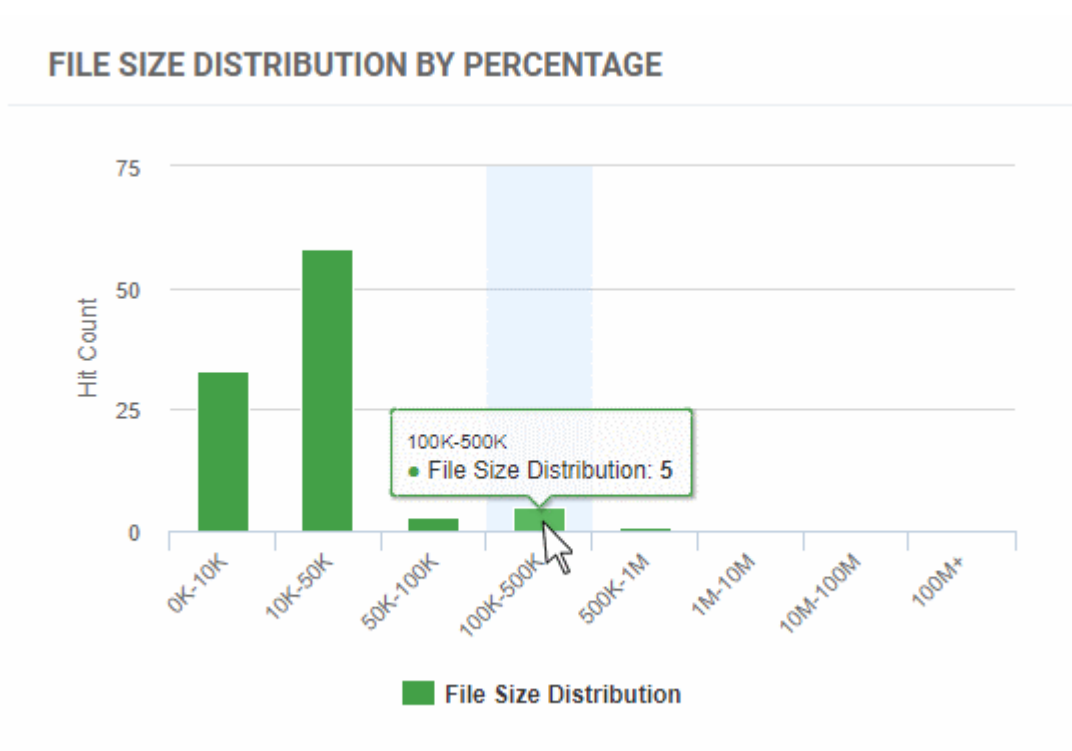
- Shows the different file types requested by your website visitors, and the quantities of each that were downloaded.



- 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

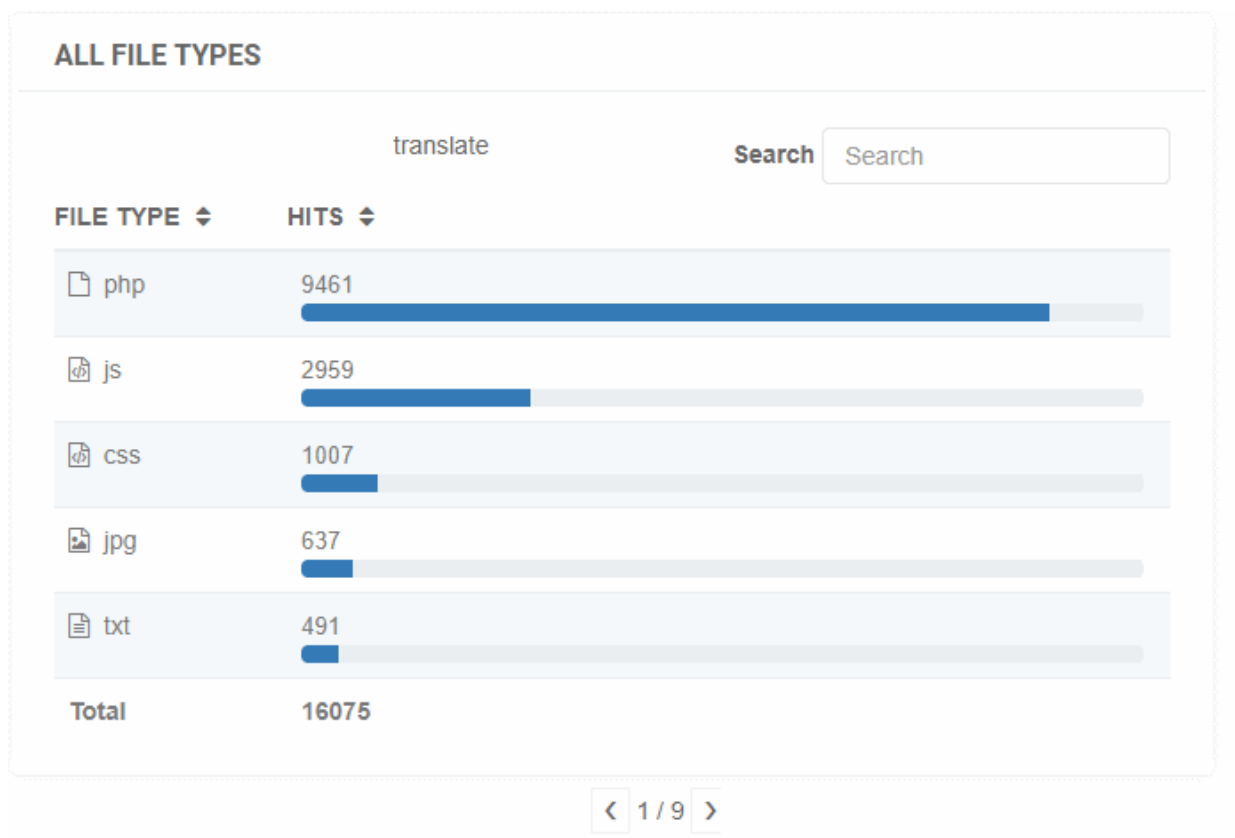
- Shows the number of files in a specific size-range that were requested by your visitors



- 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

Show the quantity of different file types downloaded by your visitors:



- 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.
- Use the arrows at the bottom to navigate to successive pages

## 4.5 Firewall Rules

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

### Pre-defined Policies

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.

### Custom Firewall Rules

You can define custom rules to block, allow, monitor or challenge specific types of traffic.

- Custom rules can be defined for for specific IPs, IP ranges, countries, organizations and more.
- Each rule can have multiple conditions. 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'.

### Notes:

- The web application firewall is only available for 'Pro', 'Premium' and 'WAF Starter' licenses.
- Custom firewall rules are only available on 'Premium' licenses.

See the following sections for more help on predefined and custom firewall rules:

- [Configure WAF Policies](#)
- [Manage Custom Firewall Rules](#)

## 4.5.1 Configure WAF Policies

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

### Configure WAF settings

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

**Firewall** [Settings](#)

**Custom WAF Rules Total 2 rules**

### ← Settings

#### WAF SETTINGS

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

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

#### WAF POLICIES

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



## WAF Settings

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

### WAF SETTINGS

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

**WAF Status**  WAF is enabled

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

### WAF POLICIES

**Note** - If you disable WAF protection then no firewall policies will be applied. Any custom firewall rules will also be disabled. See [Manage Custom Firewall Rules](#) for more information.

## WAF Policies


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

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

- Name** - Label of the built-in WAF policy.
- Status** - Indicates whether the firewall is enabled or not. 'Passive' indicates the firewall is disabled.

## Enable / disable firewall rule(s)

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

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

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

## 4.5.2 Manage Custom Firewall Rules

- Select a website from the drop-down at top-left
- Choose 'Firewall'
- The firewall page lets you construct custom rules to block, allow, monitor, or challenge specific types of traffic.
- You can create custom rules for specific IPs, IP ranges, countries, organizations, and more.
- Each rule can have multiple conditions. 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 list. 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.

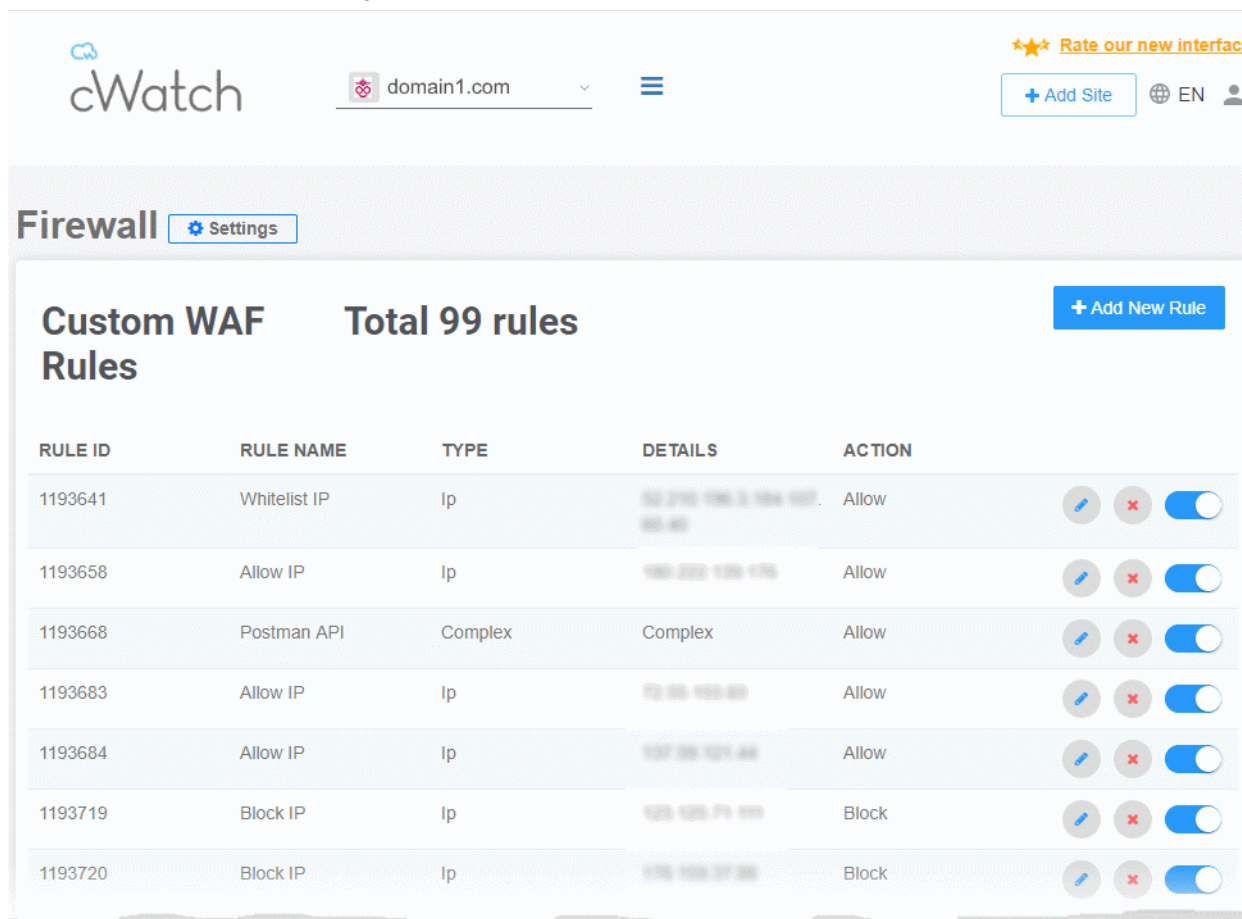
For example, suppose a piece of traffic is covered by three separate rules:

- 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 interface

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



Custom WAF Rules - Column Descriptions	
Column Header	Description
Rule ID	An auto-generated identity number for the rule
Rule Name	The label of the rule.
Type	The origin 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. Possible values are: <ul style="list-style-type: none"> <li>• Allow</li> <li>• Block</li> <li>• Monitor</li> <li>• Captcha</li> </ul>
Controls	 - Edit the firewall rule  - Remove the rule  - Enable / disable the rule

The 'Firewall' interface allows you to:

- **Add a new custom WAF rule**
- **Edit a rule**
- **Enable / Disable a rule**
- **Remove a rule**

#### Add a new WAF rule


- Select the target website from the menu at top-left
- Click the 'Firewall' tab
  - Or click the hamburger button and select 'Firewall'
- Click 'Add New Rule' at the top right

The screenshot shows the 'Add New Rule' modal form. The form has a blue header with the text 'ADD NEW RULE' and a close button 'X'. Below the header, there are three main sections:


- Enter Rule Name:** A text input field with the placeholder text 'Rule Name'.
- If:** A dropdown menu with 'IP' selected, followed by an equals sign, and a text input field containing 'IP1, IP2, etc. (example: 92.92.168.2.1, 192.168.2.2)'. There is a copy icon to the right of the input field.
- Then the action is:** A dropdown menu with 'Allow' selected.

At the bottom right of the form, there are two buttons: '+ Add Condition' and 'Save'.

- **Rule Name** - Type a label which describes the rule.
- **Condition 'If'** - Choose the source of the traffic:
  - **IP** - Enter specific IP address(es). For example, 192.168.2.1,192.168.2.2
  - **IP Range** - Enter start and end IP addresses of the IP range to be covered in the 'From' and 'To' fields
  - **URL** - Enter the name of the domain you want to specify for the condition, in part or full.
    - The rule will apply for traffic from all domains whose domain name partially matches with the value entered here.
    - Select 'Exact Match' if you have entered the domain name in full. The rule will only apply to requests from the specific domain.
  - **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 entity 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** - Choose how the traffic or access request from the selected source should be dealt with. The available options are:
  - **Allow** - All traffic from the source is permitted. This includes legitimate traffic, bots etc.
  - **Block** - No traffic is allowed from the selected source. An error message is shown to users.
  - **Monitor** - Traffic from the source 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.

## Edit a WAF rule

- Select the target website from the menu at top-left
- Click the 'Firewall' tab
  - Or click the hamburger button and select 'Firewall'
- Click the  icon beside the rule to be edited


The screenshot shows the 'Custom WAF Rules' interface. At the top, it says 'Total 99 rules' and has a '+ Add New Rule' button. Below is a table with columns: RULE ID, RULE NAME, TYPE, DETAILS, and ACTION. Two rules are visible: 'Whitelist IP' (ID 1193641) and 'Allow IP' (ID 1193658). Each rule has an edit icon (pencil), a delete icon (X), and a toggle switch. A red circle highlights the edit icon for the 'Whitelist IP' rule, with a red arrow pointing to the 'EDIT RULE' modal form below. The modal form has a blue header and contains the following fields:

- Enter Rule Name:** A text input field containing 'Whitelist IP'.
- If:** A dropdown menu set to 'IP', followed by an equals sign and a text input field containing '192.168.1.100-10.10.10.10'. A duplicate icon is to the right.
- Then the action is:** A dropdown menu set to 'Allow'.
- At the bottom right, there are two buttons: '+ Add Condition' and 'Save'.

- The 'Edit Rule' dialog is similar to the 'Add Rule' dialog
- See the explanation **above** for the description of parameters
- Edit the parameters and conditions and click Save for the changes to take effect


### Enable / Disable a firewall rule

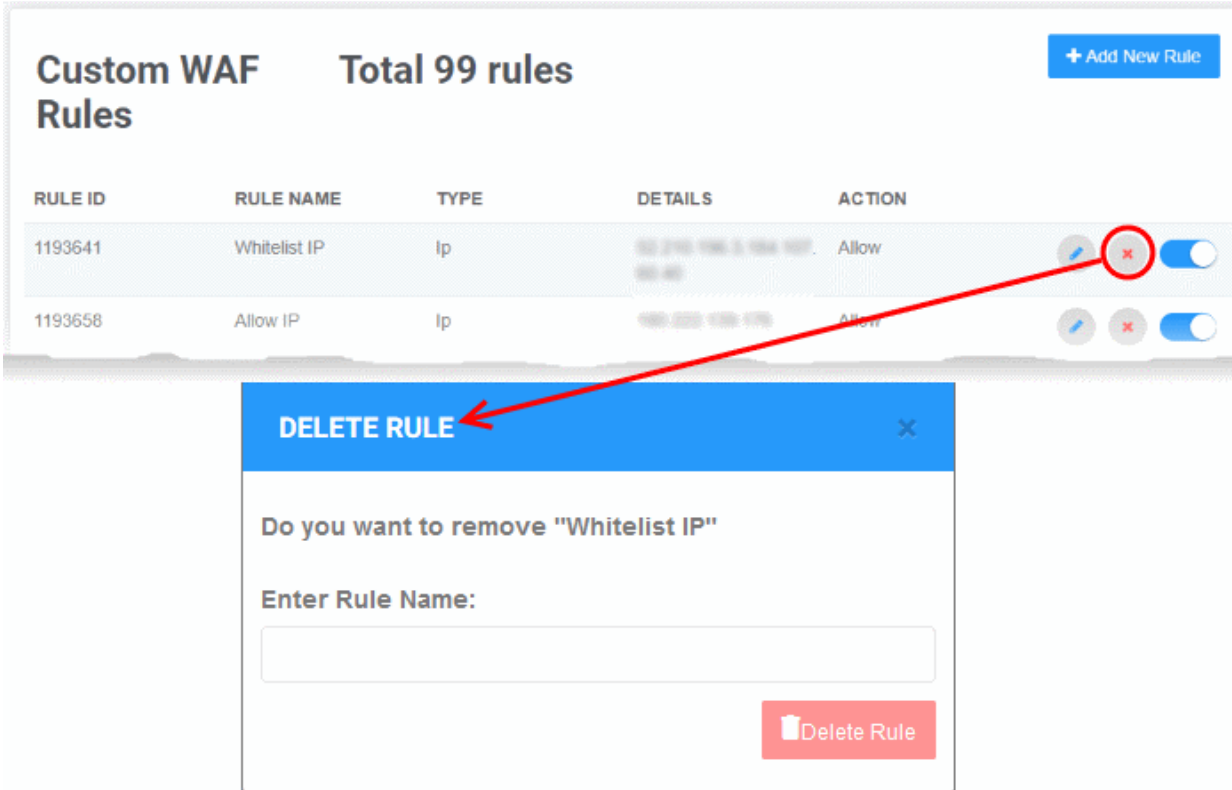
Any new custom firewall rule is enabled by default when added. Rules that need not be triggered can be disabled temporarily and can be enabled when required.

- Select the target website from the menu at top-left
- Click the 'Firewall' tab
  - Or click the hamburger button and select 'Firewall'
- Use the  switch beside the rule to enable or disable it.







### Remove a firewall rule

Custom firewall rules that are no longer needed can be removed from the website.

- Select the target website from the menu at top-left
- Click the 'Firewall' tab
  - Or click the hamburger button and select 'Firewall'
- Click the  icon beside the rule to be edited



The screenshot displays the 'Custom WAF Rules' interface. At the top, it shows 'Total 99 rules' and a '+ Add New Rule' button. Below is a table with columns: RULE ID, RULE NAME, TYPE, DETAILS, and ACTION. Two rules are visible: 'Whitelist IP' (ID 1193641) and 'Allow IP' (ID 1193658). Each rule has an edit icon, a delete icon (circled in red), and a toggle switch. A red arrow points from the delete icon of the 'Whitelist IP' rule to a 'DELETE RULE' dialog box. The dialog box has a blue header with 'DELETE RULE' and a close button. The main text asks 'Do you want to remove "Whitelist IP"'. Below this is a text input field labeled 'Enter Rule Name:' and a red 'Delete Rule' button.

RULE ID	RULE NAME	TYPE	DETAILS	ACTION
1193641	Whitelist IP	Ip	192.170.198.3, 1984.107.192.40	Allow   
1193658	Allow IP	Ip	192.222.198.178	Allow   

- Enter the label of the rule in the confirmation dialog and click 'Delete Rule'

## 4.6 SSL Configuration

- Select a website from the drop-down at top-left and choose 'SSL'
  - SSL/TLS certificates identify a website's owner, and encrypt all data that passes between the site and a visitor's browser.
  - Sites that use an 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.

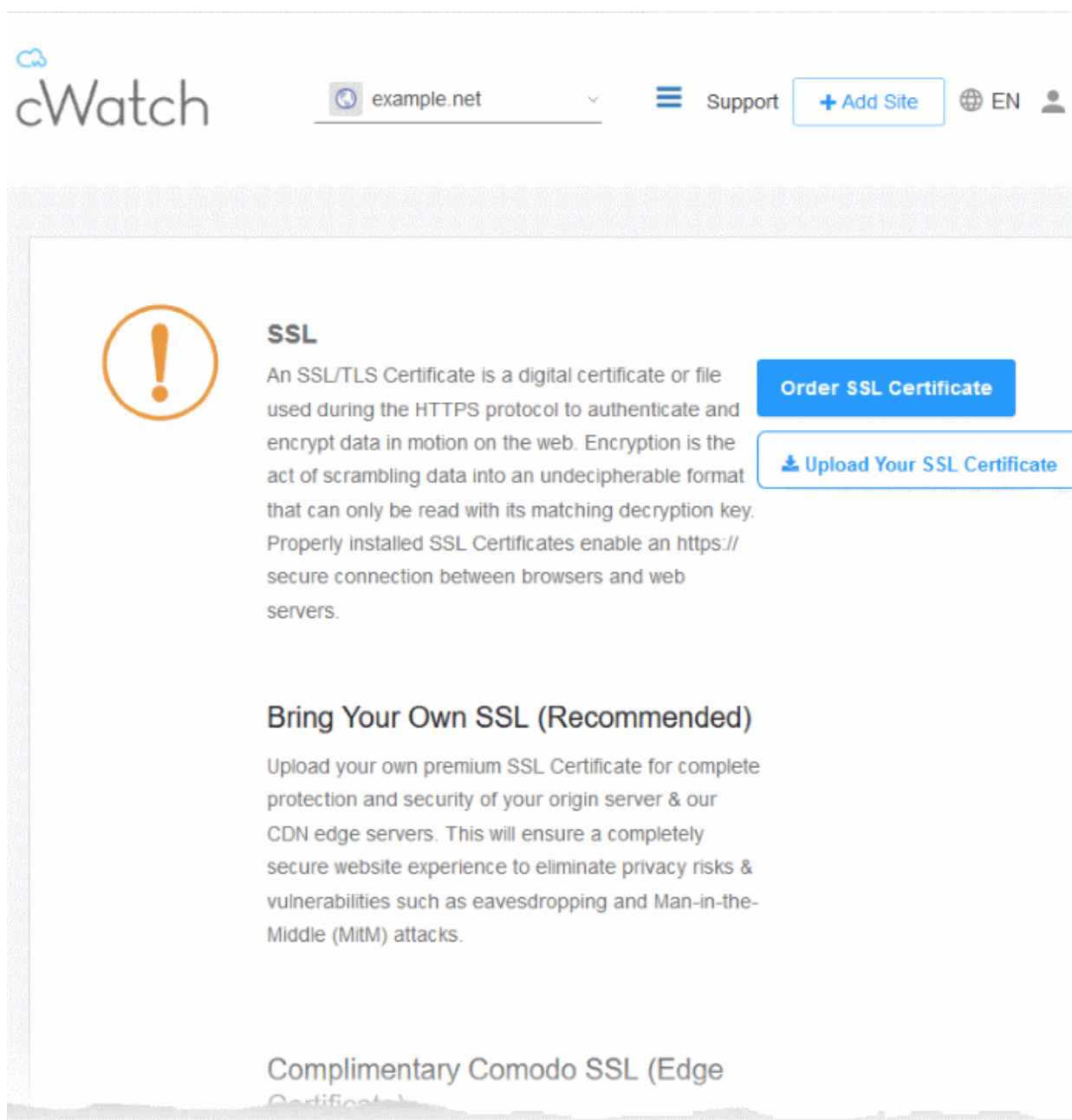
There are two ways to deploy a certificate with cWatch Web:

- **Bring your own SSL**
  - Upload your site's existing certificate to the cWatch CDN edge servers. Recommended for most customers.
  - This will secure the traffic between your site (the origin server) and the cWatch CDN.
  - See [Upload your own SSL Certificate](#) to find out how to deploy your certificate
- **Complimentary Comodo SSL**
  - Get a free SSL from Comodo deployed on the CDN Edge servers. Again, this will encrypt traffic between your site and the CDN.
  - You need to configure your site to use Comodo DNS in order to get the free SSL certificate. There are two ways you can do this:
    1. Change your domain's authoritative DNS servers to Comodo DNS
    2. Enter DNS records explicitly
      - Help to configure DNS is available in [Activate CDN for a Website](#).
      - See [Install Complementary SSL Certificate](#) for help to deploy your free certificate

### Upload your own SSL Certificate

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





The screenshot shows the cWatch website administrator interface. At the top left is the cWatch logo. To its right is a dropdown menu showing 'example.net'. Further right are a hamburger menu icon, the word 'Support', a '+ Add Site' button, a globe icon with 'EN', and a user profile icon. The main content area features a large orange warning icon (an exclamation mark inside a circle). To the right of the icon is the heading 'SSL' followed by a paragraph: '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.' To the right of this text are two buttons: a blue 'Order SSL Certificate' button and a white 'Upload Your SSL Certificate' button with a download icon. Below this is the heading 'Bring Your Own SSL (Recommended)' followed by a paragraph: '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.' At the bottom of the section is the heading 'Complimentary Comodo SSL (Edge Certificate)'.

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



### SSL

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

[Order SSL Certificate](#)

[Upload Your SSL Certificate](#)



#### UPLOAD YOUR CERTIFICATE

**📘 Certificate**

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

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	<p>Paste the content of your certificate. The content you are looking for is something like this:</p> <pre> -----BEGIN CERTIFICATE----- MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGE wJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA 1UECXMCMC VU4xFDASBgNVBAMTC0hlcm9uZyBZYW5nMB4XDTA1MDcxNTIxMTk0N1oXD TA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAGTA1BOMQswCQYDV QQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTA1VOMRQwEgYDVQQDEwtIZXJvb mcgWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBe wKE/B7j V14qeysl nr26xZUssVko36ZnhiaO/zbMOoRcKk9vEcGmtcLFuQTWD13RA gMBAAGj gbEwga4wHQYDVR0OBYYEFFFFI70krXeQDxZgbaCQoR4jUDncEMH8GA1UdI wR4MHaA FFFFI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMQswCQYDVQQGEwJDTjELM AkGA1UE CBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECXMCMV U4xFDAS BgNVBAMTC0hlcm9uZyBZYW5nggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIh vcNAQEE BQADQQA/ugzBrjjK9jcWnDVfGHlk3icNRq0oV7Ri32z/ +HGX67aRfgZu7KWdI+Ju Wm7DCfrPNGVwFWUQOmsPue9rZBgO -----END CERTIFICATE----- </pre>
SSL Chain Certificate	If your certificate contains an intermediate certificate then paste it here. If not, leave this field blank.
Certificate Key	Private key of your certificate

- Click 'Upload Your SSL Certificate'

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



## SSL

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

[Order SSL Certificate](#)

### Bring Your Own SSL (Recommended)

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

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

[Uninstall](#)

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

### Install Complementary SSL Certificate

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

## Complimentary Comodo SSL (Edge Certificate)

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

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

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

You have two options to enable the free certificate:

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

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

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

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


See **Activate CDN for a Website** and **DNS Configuration** for more details.

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

### Option A - Change your domain's authoritative DNS

[> Click for more details](#)

Activate Basic SSL Now

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

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

### Create CNAME record pointed back to us

[> Click for more details](#)

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

## Complimentary Comodo SSL (Edge Certificate)

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

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

Uninstall

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

### Option B - Create a CNAME record which points to Comodo

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

## Complimentary Comodo SSL (Edge Certificate)

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

### Option A

Change your domain's authoritative DNS servers to Comodo

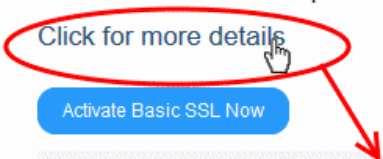

[Click for more details](#)

### Option B

Create CNAME record pointed back to Comodo

[Click for more details](#)

[Activate Basic SSL Now](#)

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


- Click the 'Activate Basic SSL Now' button:




## Option B

Create CNAME record pointed back to Comodo

[Click for more details](#)

Activating 

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

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

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

**CNAME KEY:**

`_32cba9664abf865b2fafcc9a13ce99d4`

**CNAME VALUE:**

`2b62240e2e92177963e113516c4bba0c.3a43f61c206dce84bb456d6ac4a41964.comodoca.com`

cWatch generates a CNAME record for domain control validation.

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

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

## Complimentary Comodo SSL (Edge Certificate)

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

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

[Uninstall](#)

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

## 4.7 DNS Configuration

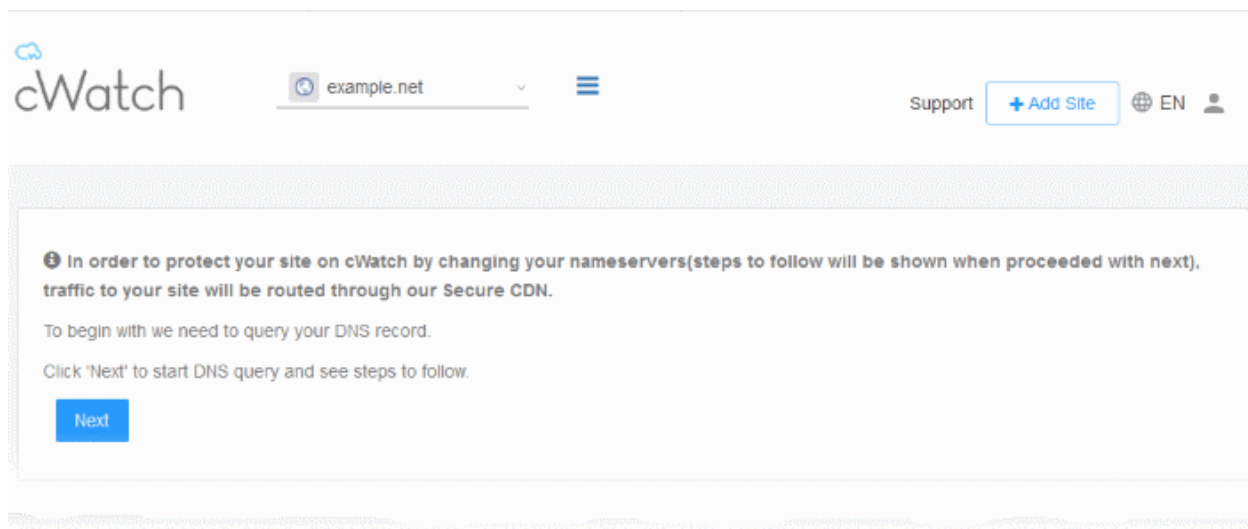
- Select a website from the drop-down at top-left then choose 'DNS'
- You need to change your site's authoritative DNS server to Comodo DNS to enable cWatch protection, the content delivery network, and the Web Application Firewall (WAF).
  - The DNS page shows the authoritative name servers (NS) for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

### Configure DNS settings on your site

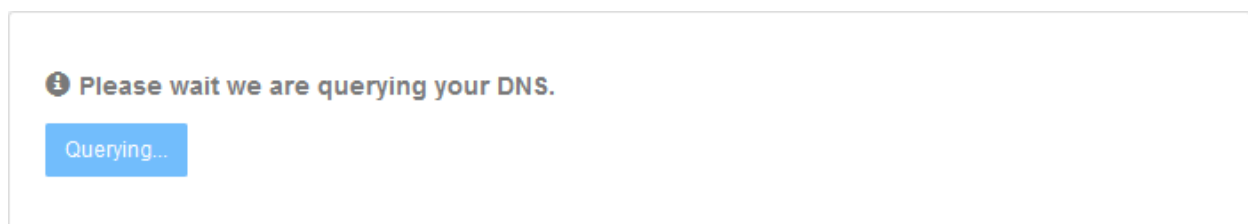
- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'DNS' tab

- Or click the hamburger button and select 'DNS'

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



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



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

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

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

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

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

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

## DNS Records

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

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

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

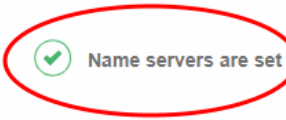
You can view whether the change was successful in the cWatch interface:

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

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

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

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

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

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

**Note:**

- You have to use the cWatch interface to manage your DNS records once you have pointed your name servers to Comodo DNS.
- 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**' below for more information.

**Manage DNS Records**

**Note** - you can only manage DNS records in cWatch if your nameservers are pointed to Comodo.

- This applies if you entered the NS values from the 'DNS' page as explained **above**, or chose **Option A - Change your domain's authoritative DNS servers to Comodo** in 'CDN' > 'Settings' > 'Activation'.
- If you selected '**Option B - Enter DNS records explicitly**' when **activating the CDN**, then you must use your web-host's tools to manage your DNS records. Any updates to DNS records that you make in this page will have no effect.

**Manage DNS records**

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'DNS' tab
  - Or click the hamburger button and select 'DNS'
- Scroll down to 'DNS Records' pane

The DNS records associated with the website are shown:

## DNS Records

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

TYPE	NAME	VALUE	TTL	
A	<input type="text" value="Name"/>	<input type="text" value="IPv4 Address"/>	Automatic TTL	<input type="button" value="Add Record"/>
<input type="text" value="Search DNS Record"/>				

TYPE	NAME	VALUE	TTL	STATUS	
TXT	@	"v=spf1 mx include:example.net include:t	Automatic TTL		
MX	@	Mail handled by: sgmail.examplegroup.cc	Automatic TTL		
A	@	178.208.81.208	1 hour		
A	wiki	91.188.212.100	1 hour		
A	www	178.208.81.208	1 hour		

**DNS Records - Table of Parameters**

Column Header	Description
Type	The kind of the DNS record.
Name	The label of the record
Value	The content of the record
TTL (Time To Live)	How long the record value can be served from the name server / local cache without refreshing the value from the site.
Status	<p>Whether the record is protected or not.</p> <ul style="list-style-type: none"> <li> - The record is protected.                             <ul style="list-style-type: none"> <li>Click the icon to remove the site from cWatch</li> </ul> </li> <li> - The record is not protected.                             <ul style="list-style-type: none"> <li>Click the icon to add the record to cWatch for protection</li> <li>See <b>Configure cWatch protection for a site</b> for guidance on this</li> </ul> </li> </ul> <p>Note - protection is available for CNAME and A records if not already enrolled to cWatch.</p>


### Add a DNS record

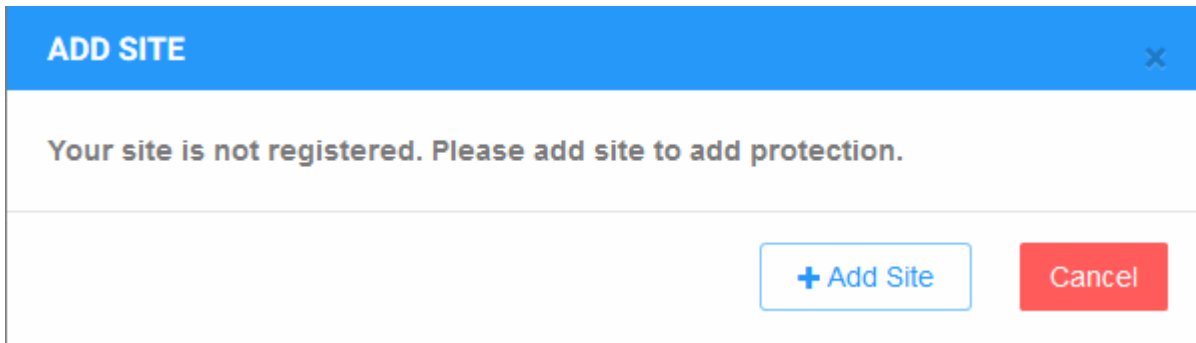
- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'DNS' tab
  - Or click the hamburger button and select 'DNS'
- Scroll down to the 'DNS Records' pane
- Configure the following items:
  - Type - Select the kind of the DNS record from the drop-down
  - Name - Enter an appropriate label for the record
  - Value - Enter an appropriate content 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' to save your changes

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 to change nameservers.

### Enable cWatch protection on 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 you need to register the record to cWatch.



- Click 'Add Site' to start the 'Add Websites' wizard.

The screenshot shows the 'ADD WEBSITES' interface with a progress bar at the top. Step 1, 'Add Website', is active and highlighted in blue. Step 2, 'Select License', and Step 3, 'Site Provisioning In Progress', are shown in gray. Below the progress bar, the text 'Step 1 - Enter Site Name' is followed by the instruction 'Please Enter your Site Name' and an information icon. A text input field contains the pre-populated value 'dfs.example.net'. A blue button labeled 'Continue Setup' with a right-pointing arrow is located at the bottom right.

The website name is pre-populated.

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

The screenshot shows the 'ADD WEBSITES' interface with the progress bar updated. Step 2, 'Select License', is now active and highlighted in blue. Step 1, 'Add Website', and Step 3, 'Site Provisioning In Progress', are shown in gray. Below the progress bar, the text 'Step 2 - Select License' is followed by the instruction 'Site will be added with selected license type'. A drop-down menu is open, showing three license options: 'Premium (1 Site / 23 days left)', 'Pro (1 Site / 23 days left)', and 'Basic (1 Site / Indefinite Usage)'. The 'Premium' option is selected and highlighted in blue. A red circle highlights the drop-down arrow icon on the right side of the menu. At the bottom, there are two blue buttons: 'Back' with a left-pointing arrow and 'Finish' with a right-pointing arrow.

- Click 'Finish' to apply the license. The site will be registered.
- cWatch will validate your request then show the following confirmation message:



The screenshot shows a progress bar with three steps: 1. Add Website, 2. Select License, and 3. Site Provisioning In Progress. Step 3 is currently active. Below the progress bar, the text reads: "Step 3 - Site Provisioning In Progress", "Congratulations your site provisioning is in progress now!", "This process may take several minutes", "While we are registering your site on our SecureCDN, you may already start malware and vulnerability scans.", and "Need help? Please contact with our support professionals on 'Live Chat'". A "★ Get Started" button is located at the bottom center.

- Click 'Get Started' to activate cWatch protection.
- If you do not have any licenses available then you will be asked to purchase a license:

The screenshot shows a progress bar with three steps: 1. Add Website, 2. Select License, and 3. Site Provisioning In Progress. Step 2 is currently active. Below the progress bar, the text reads: "You don't have license to register new domains. Click to buy a license." A "Buy a License" button is located in the center. At the bottom left, there is a "← Back" button, and at the bottom right, there is a "→ Finish" button.

- Click 'Buy a License'.
- You will be taken to the license purchase page:

X

1  
Select a plan

2  
Process Payment

3  
Finish

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** if you want to read more about the features of each license.
- Click 'Continue'

X

1  
Select a plan

2  
Process Payment

3  
Finish

### Payment Profile

Card Number

#

Cardholder Name

Name displayed on card

Total

USD\$24.90

License Period

Monthly

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

#### Order Summary

**\$24.90 / Monthly / PREMIUM plan / example.org**

	Subtotal
	\$24.90
	Savings
	\$0.00
	Total
	\$24.90

### Billing Address

Company Name

Phone Number

Address

Address 2

City

State

Country

Postal Code

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

**cWatch**  
Website Security

Need help? [Contact Support](#)

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

1 x PREMIUM Licenses	\$24.90 USD
Discount	\$0.00 USD
Domain: example.org	
Subscription: Monthly	
<b>Total</b>	<b>\$24.90 USD</b>

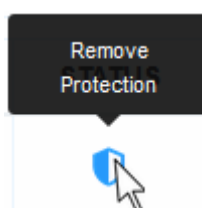
You'll receive an order checkout confirmation by email to teleramabw@gmail.com.

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

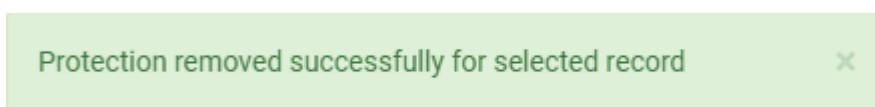
- The new license is added to your account and can be applied to the site in cWatch.
- Restart the process to add protection to the DNS record.

### Remove protection from a site

- Click the shield icon beside the record:

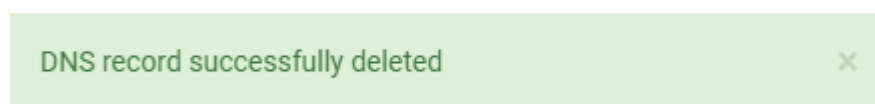


You will see the following confirmation message:



### Remove a DNS record

- You can remove a record that is not cWatch protected
- Click the trash can icon beside a record



## 4.8 Add Trust Seal to your Websites

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

### **Add the trust seal to your website**

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



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

Here are some sample scenarios:

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

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

## 4.9 Back up your Website

- cWatch backup is a robust disaster recovery solution which automatically creates a backup of your website at regular intervals. Using state of the art storage and security technologies, the service lets you quickly and easily restore your site in the event of catastrophic data loss.
- cWatch Backup includes:
  - Secure storage – Backups are encrypted and stored on heavily-protected AWS data-centers
  - Automatic full backups – Schedule daily, weekly, or monthly backup at a time that suits you
  - One-click restore – Get your site and your business back online in minutes
  - Incremental backups – Updates your backup in real-time whenever you make a change
  - Database backup – Your databases are stored separately, providing flexibility when you restore
  - On-demand backups – Instantly run a backup whenever you need to.
  - Integrated security – Each backup is scanned for malware, vulnerabilities, blacklist status and more
  - Full notifications – Get alerts after every successful or unsuccessful backup
  - Excluded paths and file types – Select exactly which items get backed up and which do not
  - Flexible plans – Choose 10 GB, 30 GB, or 50 GB storage limits

### Open the backup section

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

The screenshot shows the cWatch Backup dashboard. At the top, there's a navigation bar with tabs for OVERVIEW, SCAN, CYBER SECURITY, CDN, FIREWALL, SSL, DNS, TRUST SEAL, and BACKUP. The BACKUP tab is active. Below the navigation bar, there's a 'Backup' section with a 'Settings' link. The main content area is divided into two panels. The top panel shows 'Last Successful Backup' with a green checkmark icon, the date and time 'Jul 24th, 2019 / 8:00 UTC', and a file size of '74.07 MB'. There's a toggle switch for 'Disable Schedule Backup' and a 'Next Backup' section with the date and time 'Jul 25th, 2019 / 8:00 UTC' and a 'Backup Now' button. The bottom panel shows 'Backup Storage Usage' with a progress bar at 77%. It lists 'Files: 71.68 MB', 'Database: 2.38 MB', and 'Total Usage: 74.07 MB'. Below this, there's a table with tabs for months (JUL 2019, JUN 2019, MAY 2019, APR 2019). The table has columns for Date, Status, Files Added, Files Removed, Files Modified, Details, Download, and Restore History.

Date	Status	Files Added	Files Removed	Files Modified	Details	Download	Restore History
Jul 24	Backup Completed	2	1	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 23	Backup Completed	2	1	1	<a href="#">Check Details</a>	<a href="#">Restore</a>	<a href="#">View</a>
Jul 22	Backup Completed	2	0	2	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 21	Backup Completed	1	0	1	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 20	Backup Completed	1	1	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available

The top panel shows summary information about your latest backup, your current usage, and more:

This close-up screenshot shows the top panel of the backup dashboard. It features a green checkmark icon next to the text 'Last Successful Backup' and '74.07 MB'. Below this is a toggle switch for 'Disable Schedule Backup'. To the right, it shows 'Next Backup' with the date and time 'Jul 25th, 2019 / 8:00 UTC' and a 'Backup Now' button.

- **Last Successful Backup** – Date and time of the most recent backup operation.
  - The figure below the check-mark shows the total size of the files you have in your backup.
- **Disable Schedule Backup** – Activate or deactivate automatic backups. See '**Configure Backup Settings**'
- **Next Backup** – Date and time of the next scheduled backup



- **Backup Now** – Run a on-demand backup. You may want to do this prior to releasing a website updates. See '**On-Demand Backup**' if you need more help with this.
- **Backup Storage Usage** – The total size of the files you have in your backup. This includes individual files and databases.

The lower panel shows a list of all backup operations you have run over time:

Date	Status	Files Added	Files Removed	Files Modified	Details	Download	Restore History
Jul 24	Backup Completed	2	1	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 23	Backup Completed	2	1	1	<a href="#">Check Details</a>	<a href="#">Restore</a>	<a href="#">View</a>
Jul 22	Backup Completed	2	0	2	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 21	Backup Completed	1	0	1	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 20	Backup Completed	1	1	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available

From this pane you can:

- View backup details
- Restore website files and databases
- View restore history

### Settings

- Click the 'Settings' button to configure backup paths, FTP/SSH settings, schedules, exclusions, and more.

See the following sections for more on each:

- [Purchase a Backup License](#)
- [Configure Backup Settings](#)
- [On-Demand Backup](#)
- [View Backup Records](#)
- [Restore and Download Website Files](#)

## 4.9.1 Purchase a Backup License

- The backup service is an add-on available after you have bought a cWatch license. You must also have already configured your website to work with cWatch.
- Each license covers one site. You must purchase separate licenses for each site you want to backup.

### Open Backup section

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

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

	SMALL \$ 2.49 per month	MEDIUM \$ 6.49 per month	LARGE \$ 9.49 per month
Websites	1 site	1 site	1 site
Storage	10GB	30GB	60GB
Backup Retention	Until Storage is Full or 90 days	Until Storage is Full or 90 days	Until Storage is Full or 90 days
File System Backup	FTP/SFTP	FTP/SFTP	FTP/SFTP
Daily Automatic Backup	✓	✓	✓
Custom Scheduled Backup	✓	✓	✓
Backup Now	✓	✓	✓
Backup History	✓	✓	✓
Backup Status Notifications	✓	✓	✓
Alerts on Failure to Backup	✓	✓	✓
File Change Monitoring	File System	File System	File System
One Click Automatic Recovery	File System	File System	File System
Manual Restore(Download Zip)	✓	✓	✓
	LET'S TRY	LET'S TRY	LET'S TRY

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

**Medium**  
cWatch Backup Medium Package Monthly \$6.49

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

**Billing Info**

FULL NAME  
#

ADDRESS

CITY ZIP CODE

COUNTRY

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

**Credit Card Info**

CARD NUMBER #

CARDHOLDER NAME  
Name displayed on card

EXPIRE DATE  
MM YYY

CVV  
CVC

I'm not a robot reCAPTCHA Privacy - Terms

**Process Payment**

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

## 4.9.2 Configure Backup Settings

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

### Open the backup settings page

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

The screenshot shows the 'Settings' page for the 'BACKUP' tab in the Comodo cWatch interface. The page is for the site 'cwatchdemo.com'. It features two main configuration panels: 'Website Details' and 'Database Options'. Both panels include a warning about external IP addresses for backups and a form with the following fields:

- Website Details:** WEBSITE URL (cwatchdemo.com), CONNECTION TYPE (FTP), FTP USERNAME (servet@cwatchdemo.com), FTP PASSWORD (masked), FTP HOSTNAME (160.153.162.25), FTP PORT (21), and FTP DIRECTORY.
- Database Options:** DATABASE NAME (db\_cwatchdm), CONNECTION TYPE (Direct Connect), DATABASE USERNAME (mysql:cwatchdm), DATABASE PASSWORD (masked), DATABASE HOST (107.180.24.253), and PORT (3306).

See the following for details about each of the settings:

- [Website Backup Settings](#)
- [Database Backup Settings](#)
- [Schedule your Backup](#)
- [Notification Settings](#)
- [Backup Exclusions](#)

### Website Backup Settings

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

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

**Website Details** ✔ Your website backup enabled.

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

WEBSITE URL:  CONNECTION TYPE:  ▲

FTP USERNAME:  FTP PASSWORD:

FTP HOSTNAME:  FTP PORT:  ▼

FTP DIRECTORY:   
e.g., /public\_html/

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

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

**Website Details** ✔ Connection Successful!

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

- Click 'Save'

### Database Backup Settings

This settings is configured to back up your website database to cWatch servers

- Two connection types are available between your database server and cWatch backup server:
  - Direct Connect and SSH-KEY
  - For SSH-KEY authentication method, the details of the cWatch private key (pertaining to your account) will be available in the pane.

- You need to place the cWatch server private key (.../ssh/authorized\_keys) in your database server

### Database Options

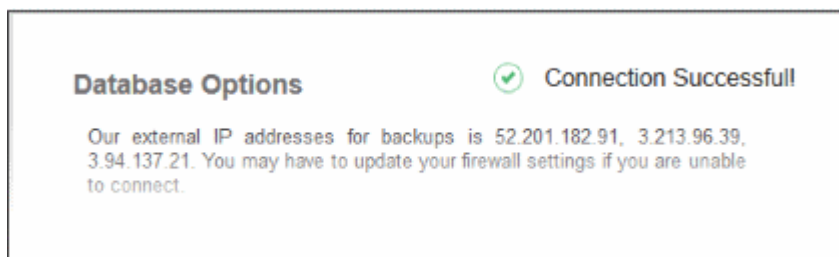
Your site databases are handled separately to the rest of the files on your site. Use this section to tell cWatch of the name, location and connection method of your database.

- Select the target website from the menu at top-left
- Click the 'Backup' tab
- Click 'Settings'
- Locate the 'Database Options' pane:

The screenshot shows the 'Database Options' configuration pane. At the top, it displays external IP addresses for backups: 52.201.182.91, 3.213.96.39, and 3.94.137.21, with a note that firewall settings may need to be updated. Below this, there are several input fields: 'DATABASE NAME' (db\_cwatchdm), 'CONNECTION TYPE' (Direct Connect), 'DATABASE USERNAME' (mysqlcwatchdm), 'DATABASE PASSWORD' (masked with dots), 'DATABASE HOST' (107.180.24.253), and 'PORT' (3306). A 'Test Connection' button is located at the bottom right of the pane.

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

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

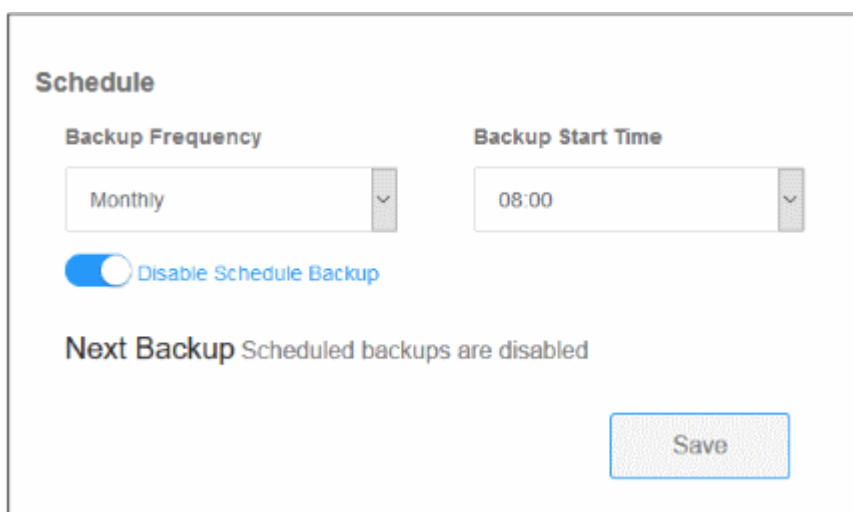


- Click 'Save'

## Schedule your Backup

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

- Select the target website from the menu at top-left
- Click the 'Backup' tab
- Click 'Settings'
- Locate the 'Schedule' pane:

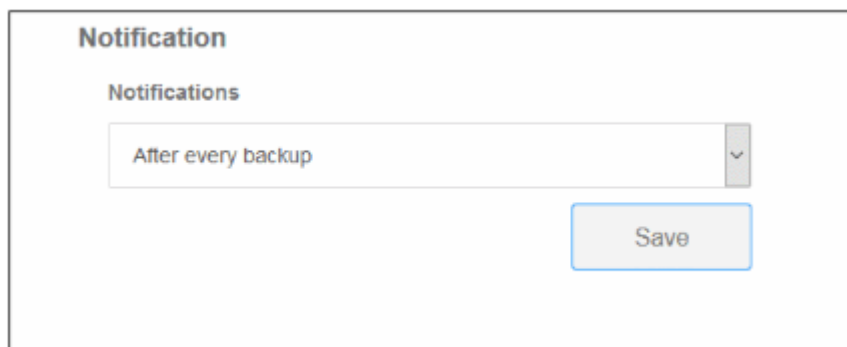


- **Backup Frequency** – Four options are available:
  - **Daily** - Backups start at the date/time shown in 'Next Backup', then run every day at the same time thereafter
  - **Every 2 days** - Backups start at the date/time shown in 'Next Backup', then run every other day thereafter.
  - **Weekly** – Backups start at the date/time shown in 'Next Backup', then run every 7 days thereafter.
  - **Monthly** - Backups start at the date/time shown in 'Next Backup', then run at the same date/time of every calendar month thereafter.
- **Backup Start Time** – Choose when the backup operation should begin
- Click 'Save'

## Notification Settings

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

- Select the target website from the menu at top-left
- Click the 'Backup' tab
- Click 'Settings'
- Locate the 'Notification' pane:



- Choose one of the following options:
  - **After every backup** – You receive a notification after each backup. The message states whether the operation was successful or not.
  - **Only on failure** – You only receive a notification when a backup fails
  - **Disable notifications** – No notification mails are sent
- Click 'Save'

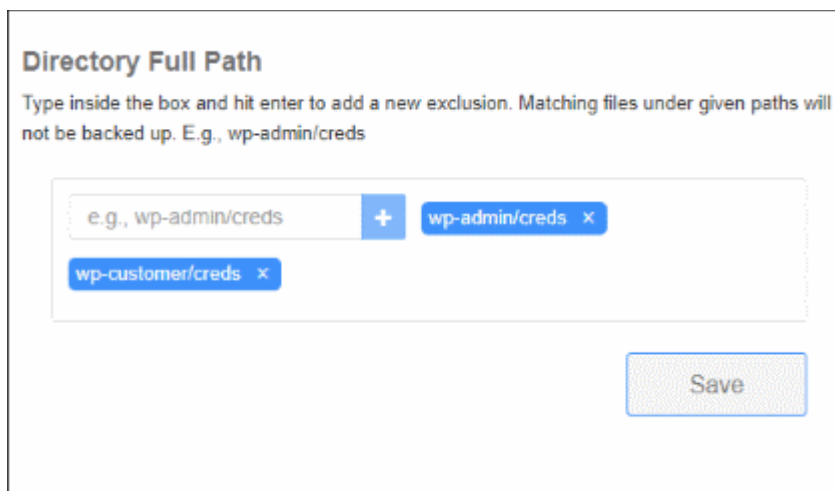
## Backup Exclusions

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

- Select the target website from the menu at top-left
- Click the 'Backup' tab
- Click 'Settings'
- There are two type of exclusion you can create
  - **Directory Full Path** – Exclude entire folders
  - **Extension Exclusions** – Exclude specific file extensions. For example, \*.psd will exclude any Photoshop source files.

### Directory Full Path

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



- Click 'Save'



## Extension Exclusions

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



**Extension Exclusions**

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

e.g., \*.jpeg + \*.txt x

Save

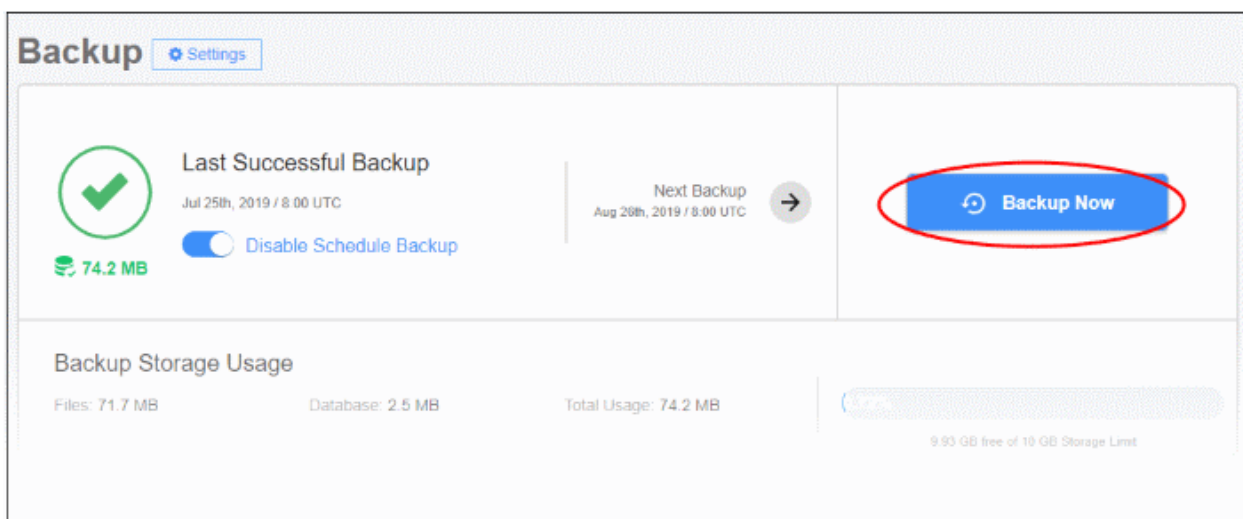
- Type the extension of the file that you want to exclude. You must prefix the extension with \*.
  - For example, \*.txt
- Click '+'.
- Repeat the procedure to add more file extensions.
- Click 'Save'

### 4.9.3 On-Demand Backup


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

Both website files and database are included. You can run two on-demand backups per-day.

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



**Backup** [Settings](#)

 **Last Successful Backup**  
Jul 25th, 2019 / 8:00 UTC  
74.2 MB

**Disable Schedule Backup**

Next Backup  
Aug 26th, 2019 / 8:00 UTC →

**Backup Now**

**Backup Storage Usage**

Files: 71.7 MB      Database: 2.5 MB      Total Usage: 74.2 MB

9.93 GB free of 10 GB Storage Limit

The progress of the backup is shown as follows:

The screenshot shows the 'Backup' page with a 'Settings' button. The main status is 'Backup In Progress...' with a 'Please Wait' message and a refresh icon. To the right, it says 'Next Backup Backing Up' with a right arrow. Below this, the 'Backup Storage Usage' section shows: Files: 71.7 MB, Database: 2.5 MB, Total Usage: 74.2 MB, and a progress bar at 72%. A 'Details' section below shows a left arrow and 'Backup In Progress' with a refresh icon.

The date of the 'Last Successful Backup' is updated when the backup operation finishes:

The screenshot shows the 'Backup' page with a 'Settings' button. The main status is 'Last Successful Backup' with a green checkmark icon, the date 'Jul 26th, 2019 / 9:42 UTC', and a '74.32 MB' storage indicator. There is a 'Disable Schedule Backup' toggle switch. To the right, it says 'Next Backup Aug 26th, 2019 / 8:00 UTC' with a right arrow and a 'Backup Now' button. Below this, the 'Backup Storage Usage' section shows: Files: 71.7 MB, Database: 2.62 MB, Total Usage: 74.32 MB, and a progress bar at 73%. At the bottom, it indicates '9.93 GB free of 10 GB Storage Limit'.

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

#### 4.9.4 View Backup Records and File Statistics

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

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

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

Files: 71.7 MB Database: 2.62 MB Total Usage: 74.32 MB							
9.93 GB free of 10 GB Storage Limit							
<a href="#">JUL 2019</a> <a href="#">JUN 2019</a> <a href="#">MAY 2019</a> <a href="#">APR 2019</a>							
Date	Status	Files Added	Files Removed	Files Modified	Details	Download	Restore History
Jul 26	<input checked="" type="checkbox"/> Backup Completed	1	1	0	<a href="#">Check Details</a>	<input type="button" value="Restore"/>	No restore available
Jul 25	<input checked="" type="checkbox"/> Backup Completed	2	1	0	<a href="#">Check Details</a>	<input type="button" value="Restore"/>	No restore available
Jul 24	<input checked="" type="checkbox"/> Backup Completed	2	1	0	<a href="#">Check Details</a>	<input type="button" value="Restore"/>	No restore available
Jul 23	<input checked="" type="checkbox"/> Backup Completed	2	1	1	<a href="#">Check Details</a>	<input type="button" value="Restore"/>	<a href="#">View</a>
Jul 22	<input checked="" type="checkbox"/> Backup Completed	2	0	2	<a href="#">Check Details</a>	<input type="button" value="Restore"/>	No restore available

Backup Records - Table of Parameters	
Parameter	Description
Date	When the backup was run
Status	Whether or not the backup was successful. Possible values are: <ul style="list-style-type: none"> <li>Backup Completed – Files backed up successfully.</li> <li>Backup Failed – The backup did not succeed for some reason. For example, the internet connection failed.</li> <li>Backup Completed Partially – Some files weren't copied because they were deleted between start and finish of the backup operation.</li> <li>Backup in Progress – Backup is running.</li> </ul>
Files Added	Number of new files added compared to the previous backup
Files Removed	Number of files removed compared to the previous backup
Files Modified	Number of files that were updated since the previous backup
Details	View the exact names of files added, removed or edited. <a href="#">Click here</a> for more details.
Download	Restore your website using the files/database in this record. See ' <a href="#">Restore and Download Website Files</a> '
Restore History	Details are shown here if your web site was restored using the backup on this row. Click 'View' to view the restore details. See ' <a href="#">Restore and Download Website Files</a> '

## View File Statistics

The 'Details' pane shows how many files were added, removed or modified during a backup operation. You can also

download the record to view the exact files that were involved.

- Click 'Check Details' in a backup record

Date	Status	Files Added	Files Removed	Files Modified	Actions	Notes
Jul 25	Backup Completed	2	1	0	<a href="#">Check Details</a> <a href="#">Restore</a>	No restore available
Jul 24	Backup Completed	2	1	0	<a href="#">Check Details</a> <a href="#">Restore</a>	No restore available
Jul 23	Backup Completed	2	1	1	<a href="#">Check Details</a> <a href="#">Restore</a> <a href="#">View</a>	
Jul 22	Backup Completed	2	0	2	<a href="#">Check Details</a> <a href="#">Restore</a>	No restore available

### ← Details

✓
Backup Completed

**FILE PROGRESS TRACKER**

- 2019-07-23 08:00:53.0 Backup request received
- 2019-07-23 08:03:41.0 File structure analysis being made
- 2019-07-23 08:05:34.0 File changes being analyzed
- 2019-07-23 08:05:37.0 Transferring files to our storage system
- 2019-07-23 08:07:35.0 File transfer completed
- 2019-07-23 08:07:47.0 All done!

**FILE STATS**

2  
FILES ADDED

1  
FILES REMOVED

1  
FILES MODIFIED

**DATABASE PROGRESS TRACKER**

- 2019-07-23 08:00:53.0 Backup request received
- 2019-07-23 08:02:13.0 All done!

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

	A	B	C
1	Status	File	Description
2	added	<u>cwatchdemo.com_1563846115.php</u>	
3	added	<u>cwatchdemo.com_1563867387.php</u>	
4	modified	<u>wp-content/themes/twentyfifteen/error_log</u>	
5	deleted	<u>cwatchdemo.com_1563780981.php</u>	
6			
7			
8			
9			
10			
11			

## 4.9.5 Restore and Download Website Files

- You can restore your site from any backup you have taken in the past.
- There are two steps to a full restore:
  - Restore your website files. Done automatically when you click 'Restore' > 'Auto-restore All Files'. This does not overwrite your current database.
  - Restore your database. You must do this manually. You can download the database from the 'Restore' options. You can get the database from a different backup-row if required.

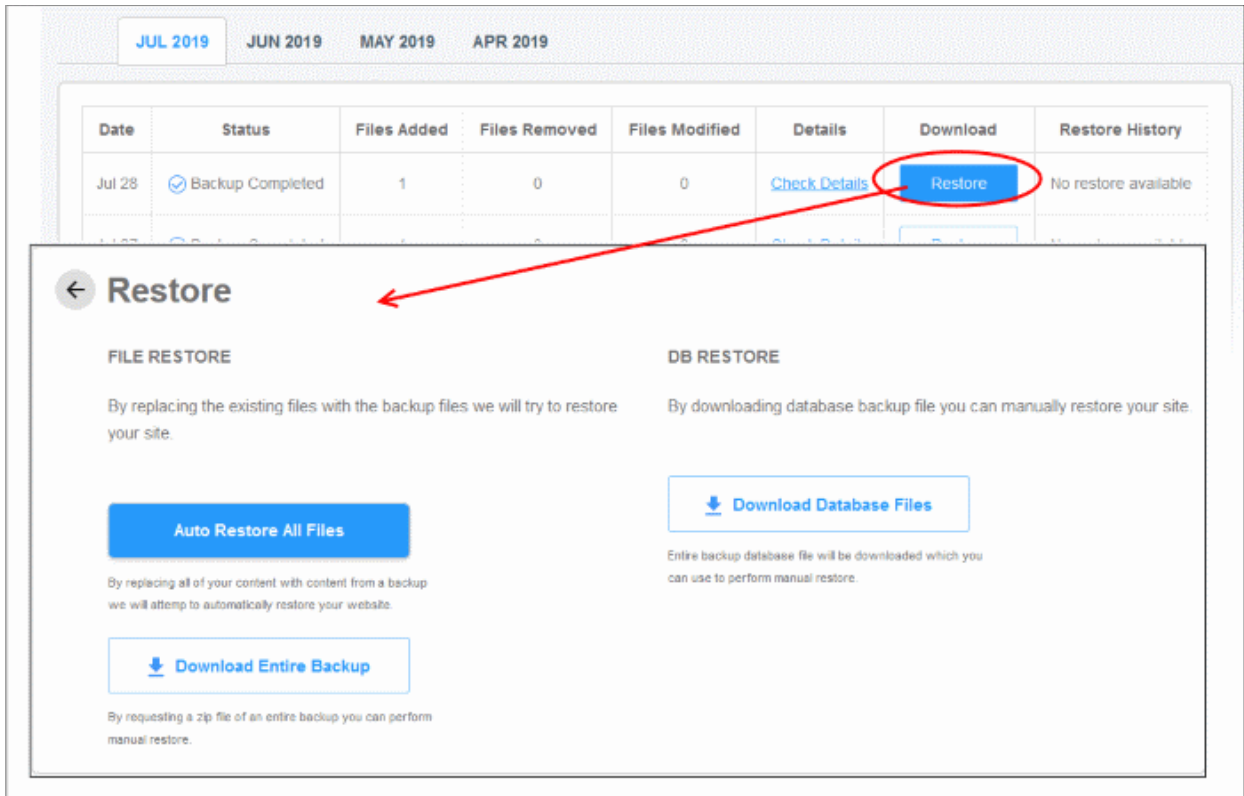
The options above offer you flexibility when restoring a website. For example, you can restore your site to the 'last-known-working' version, while keeping a database which has your most recent transactions.

### Run a restore operation

- Select the target website from the menu at top-left
- Click the 'Backup' tab
- Scroll down to the backup history table:

Files: 71.71 MB		Database: 2.86 MB		Total Usage: 74.57 MB		9.93 GB free of 10 GB Storage Limit	
JUL 2019		JUN 2019		MAY 2019		APR 2019	
Date	Status	Files Added	Files Removed	Files Modified	Details	Download	Restore History
Jul 28	Backup Completed	1	0	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 27	Backup Completed	1	0	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 26	Backup Completed	1	1	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 25	Backup Completed	2	1	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available
Jul 24	Backup Completed	2	1	0	<a href="#">Check Details</a>	<a href="#">Restore</a>	No restore available

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

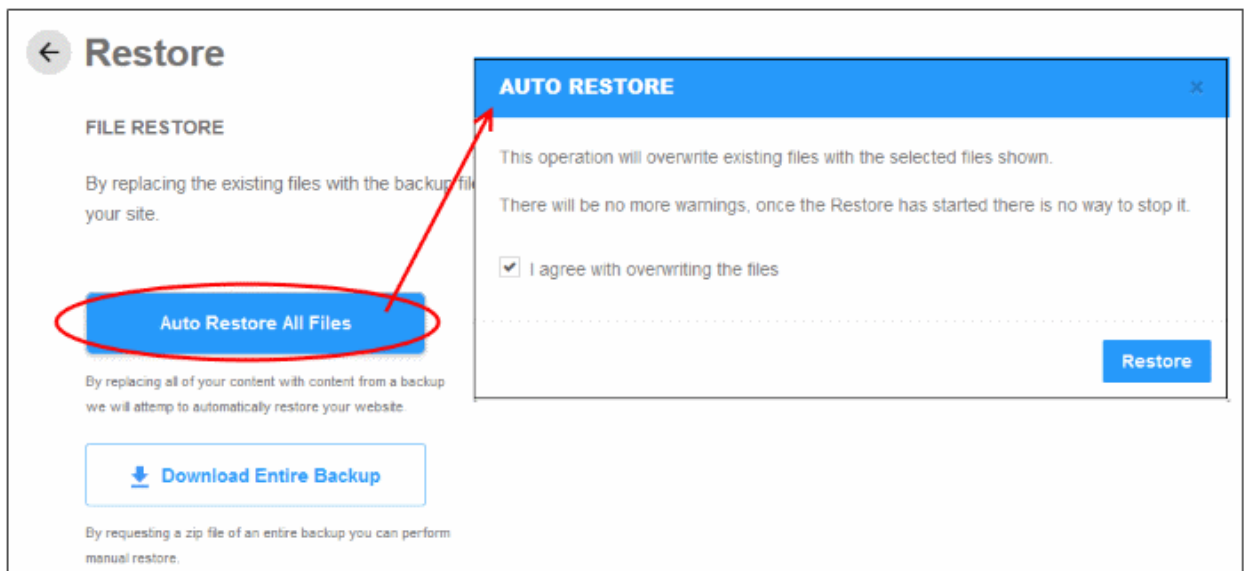


- **Auto-restore all files** - Start the restore process. Files in the destination will be replaced by those in the backup.
- **Download entire backup** - Download a .zip file of the backup. You can use this to manually restore files, or to run a partial restore, or to simply retrieve some lost / older versions of files.
- **Download Database Files** - Download a .zip file which contains all database records. You can manually unzip and restore the database as required.

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

## File Restore

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



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

The screenshot shows the 'Auto Restore In Progress' status with a circular progress indicator and a 'Please Wait' message. Below this, the 'Backup Storage Usage' section shows a progress bar at 0.73% with 9.93 GB free of a 10 GB storage limit. The 'Restore History' section contains a table with the following data:

Request Date	Request Type	Restore Status	Result
Jul 29	Auto Restore	In Progress	<a href="#">Download</a>

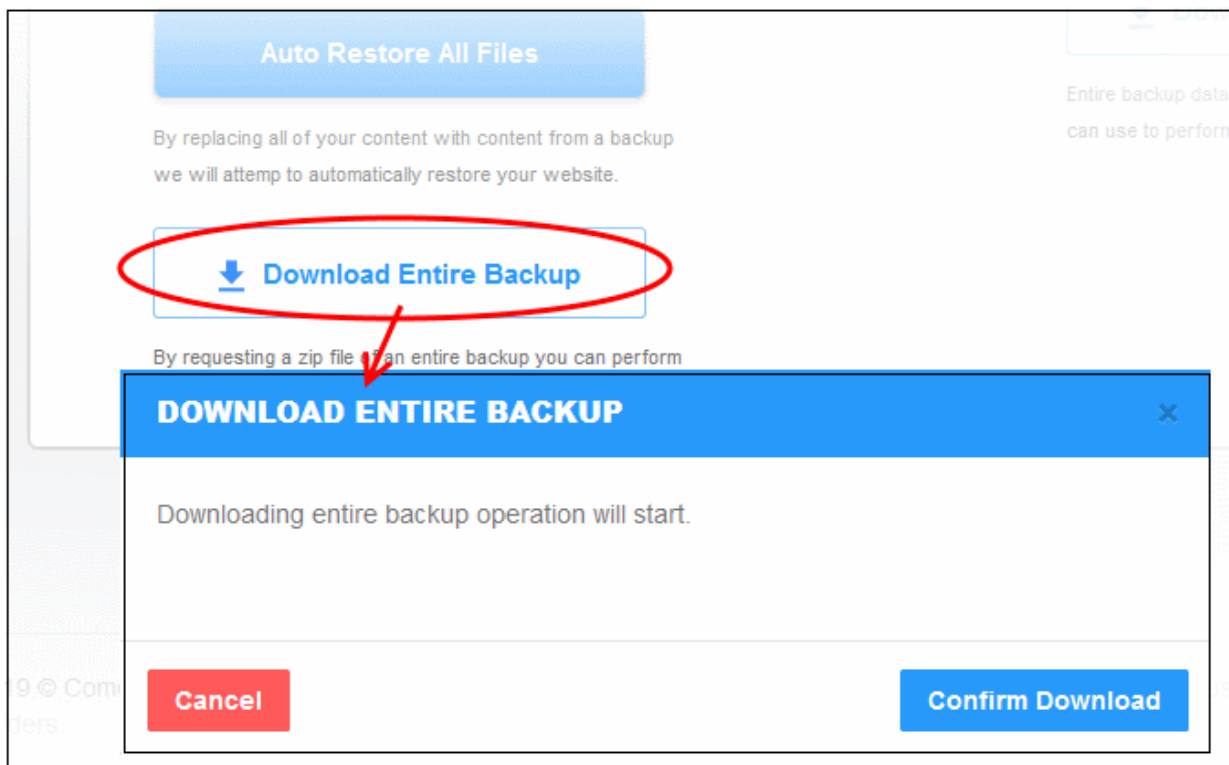
- Results are shown at the end of the operation:

The screenshot shows the 'Restore History' table after the operation is complete. The 'Restore Status' is now 'Completed' and the 'Result' column shows 'Files Restored: 2' and 'Failed to restore: 0'.

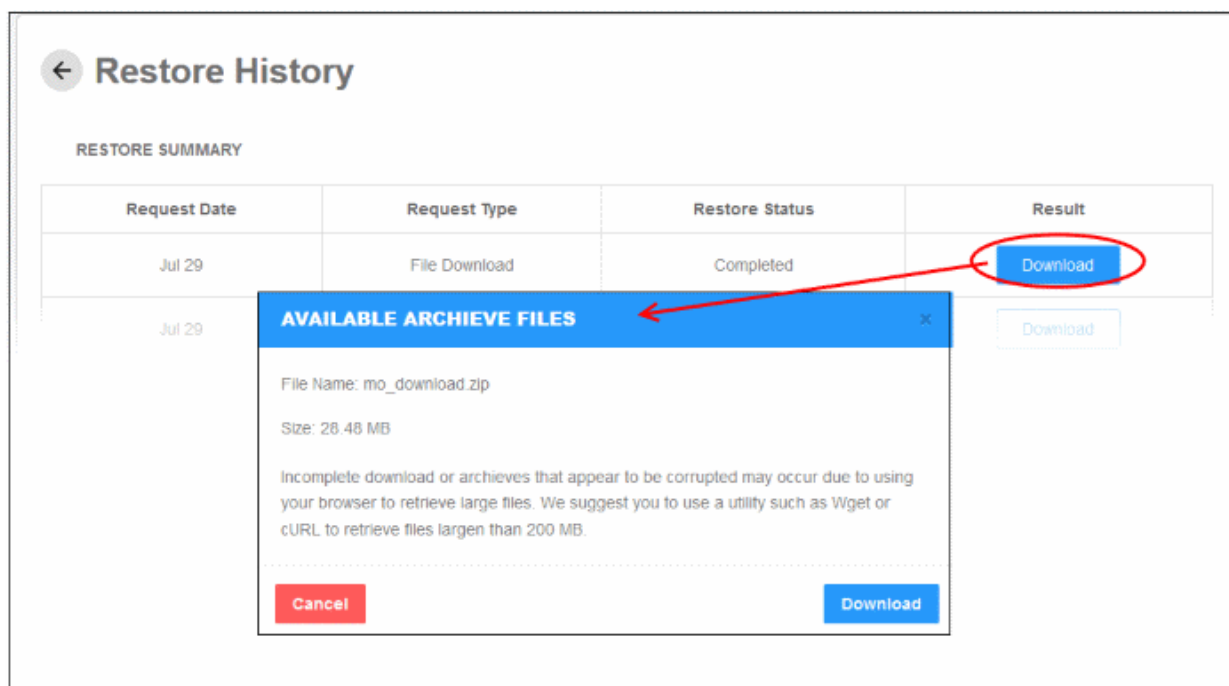
Request Date	Request Type	Restore Status	Result
Jul 29	Auto Restore	Completed	Files Restored: 2 Failed to restore: 0

## Download Entire Backup

- Click the 'Restore' button in the row of the backup you want to use
- Click 'Download Entire Backup' > 'Confirm Download':



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

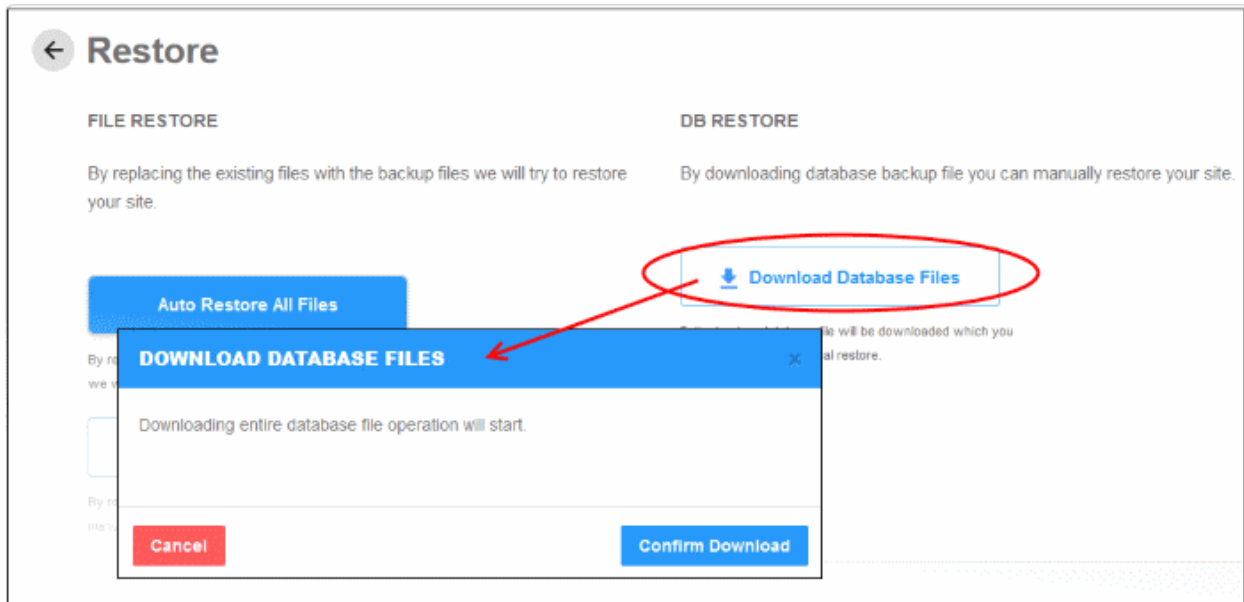


Note – Use Wget or cURL to download files larger than 200 MB.

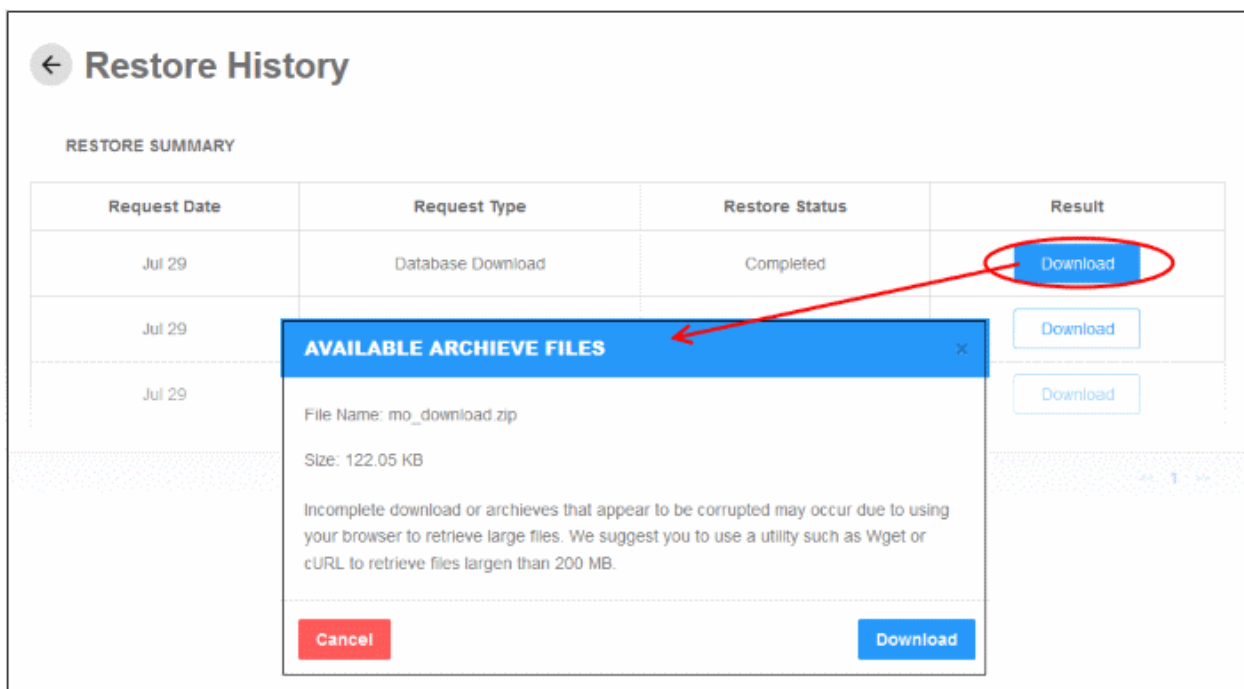
## Database Restore

- Click the 'Restore' button in the row of the backup you want to use
- Click 'Download Database Files' > 'Confirm Download':





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




Note – Use Wget or cURL to download files larger than 200 MB.

## 5 View and Upgrade Licenses for Domains

- Click your profile icon at the top-right and choose 'Plans'
- The plans page shows licenses added to your account, and the domains associated with them
- You can add new sites for unused licenses and upgrade licenses for existing domains

### Manage Licenses

- Click the user icon  at the top-right
- Select 'Plans' from the drop-down

The screenshot shows the cWatch website administrator interface. At the top right, there is a user profile icon circled in red. A dropdown menu is open, showing options: my profile, home, plans (circled in red with an arrow), and logout. Below the dropdown, the 'Plans' section is visible, containing a table with the following data:

PLAN	SITE NAME	EXPIRATION DATE	STATUS	ACTIONS
Premium Trial	cwatchdemo.com	31/07/2019	Expired	<a href="#">Upgrade</a>
Backup Small	cwatchdemo.com	05/08/2019(will expire in 3 days)	Valid	<a href="#">Upgrade</a>
Premium Trial	checkmysite.com	31/07/2019	Expired	<a href="#">Upgrade</a>
Basic	--	Indefinite Usage	Valid	<a href="#">Add Site</a>

Plans - Column Descriptions	
Column Header	Description
Plan	The license type
Site Name	Domain associated with the license
Expiration Date	Validity term of the license
Status	Whether the license is valid or expired
Actions	Controls to: <ul style="list-style-type: none"> <li>• <b>Associate a domain with a unused license</b></li> <li>• <b>Upgrade the license on a domain</b></li> </ul>

From this interface you can:


- Upgrade the license on a domain
- Add a new domain to a unused license

### Upgrade license for a domain


You may want to upgrade your cWatch license if:

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

### Upgrade license

- Click the user icon  at top-right
- Select 'Plans' from the drop-down
- The plans screen shows a list of available, unused licenses
- Click 'Upgrade' in the row of the target website
- Select the license you want to associate with the domain:

## Plans

PLAN	SITE NAME	EXPIRATION DATE	STATUS	ACTIONS
Premium	example.net	20/04/2019	Valid	
Pro	--	20/04/2019	Valid	<a href="#">+ Add Site</a>
Premium	--	30/12/2018	Expired	
Pro	--	--	Valid	<a href="#">+ Add Site</a>
Basic	example.org	Indefinite Usage	Valid	<a href="#">Upgrade</a> 
Pro	wiki.testmypcsecurity.com	03/04/2019	Valid	Pro (1 Site / 23 days left)

< 1 / 1 >

- Click 'Yes' at the confirmation screen:

**DO YOU CONFIRM?**
✕

**License of example.org will be upgraded.**

No

Yes

The license will be applied to the domain.

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

X

1  
Select a plan

2  
Process Payment

3  
Finish

1  
Month

12  
Months

24  
Months

36  
Months

**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	✓	✓

Premium

Pro

**\$24.90**

-month-

**\$9.90**

-month-

Continue

- Select the license period and type. See **License Types** for more details on the features of each license.
- Click 'Continue' and complete the payment form:

X

1  
Select a plan

2  
Process Payment

3  
Finish

### Payment Profile

Card Number

MM

YYYY

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 / example.org</b>	Subtotal
	\$24.90
	Savings
	\$0.00
	Total
	\$24.90

### Billing Address

<u>Company Name</u>	<u>Phone Number</u>
<input type="text"/>	<input type="text"/>
<u>Address</u>	<u>Address 2</u>
<input type="text"/>	<input type="text"/>
<u>City</u>	<u>State</u>
<input type="text"/>	<input type="text"/>
<u>Country</u>	<u>Postal Code</u>
<input type="text"/>	<input type="text"/>

I'm not a robot

Process Payment


- Click 'Finish' at the payment confirmation screen:

1  
Select a plan

2  
Process Payment


3  
Finish

X

Need help? [Contact Support](#)

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

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

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


---

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

- You can now go back to the license upgrade process as described earlier.

### Add a new domain to a unused license

You can add a new website for cWatch protection and associate it with an existing license.

- Click the user icon  at top-left
- Select 'Plans' from the drop-down
- Click the 'Add Site' button in the row of an unused license.
- This starts the 'Add Websites' wizard:

## Plans

PLAN	SITE NAME	EXPIRATION DATE	STATUS	ACTIONS
Premium	example.net	20/04/2019	Valid	
Pro	example.org	20/04/2019	Valid	<a href="#">Upgrade</a> ▾
Premium	--	30/12/2018	Expired	
Pro	--	--	Valid	<a href="#">+ Add Site</a>
Basic	--	Indefinite License	Valid	<a href="#">+ Add Site</a>

**ADD WEBSITES** X

1

Add  
Website

2

Select  
License

3

Site Provisioning  
In Progress

**Step 1 - Enter Site Name**

Please Enter your Site Name ❗

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

→ Continue Setup

- Enter the domain name of the website you want to register. Do not include 'www' at the start.
- Click 'Continue Setup' to move to the next step.
- The license is pre-selected
- The wizard moves to 'Step 3 - Site Provisioning'

**ADD WEBSITES** X

**Step 3 - Site Provisioning In Progress**

Congratulations your site provisioning is in progress now!

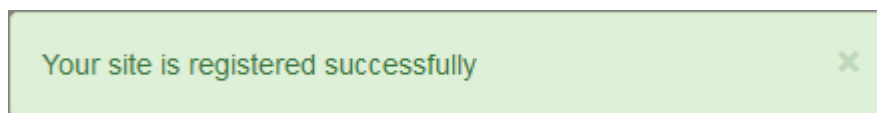
This process may take several minutes

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

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

★ Get Started

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




- Next up is to enable cWatch protection on the site.
  - Click 'Get Started' to open the 'Overview' page for the site
  - The overview page lets you configure malware and vulnerability scans, firewall rules, CDN settings, and more.
  - This is covered in more detail in the [Website Overview](#) section.

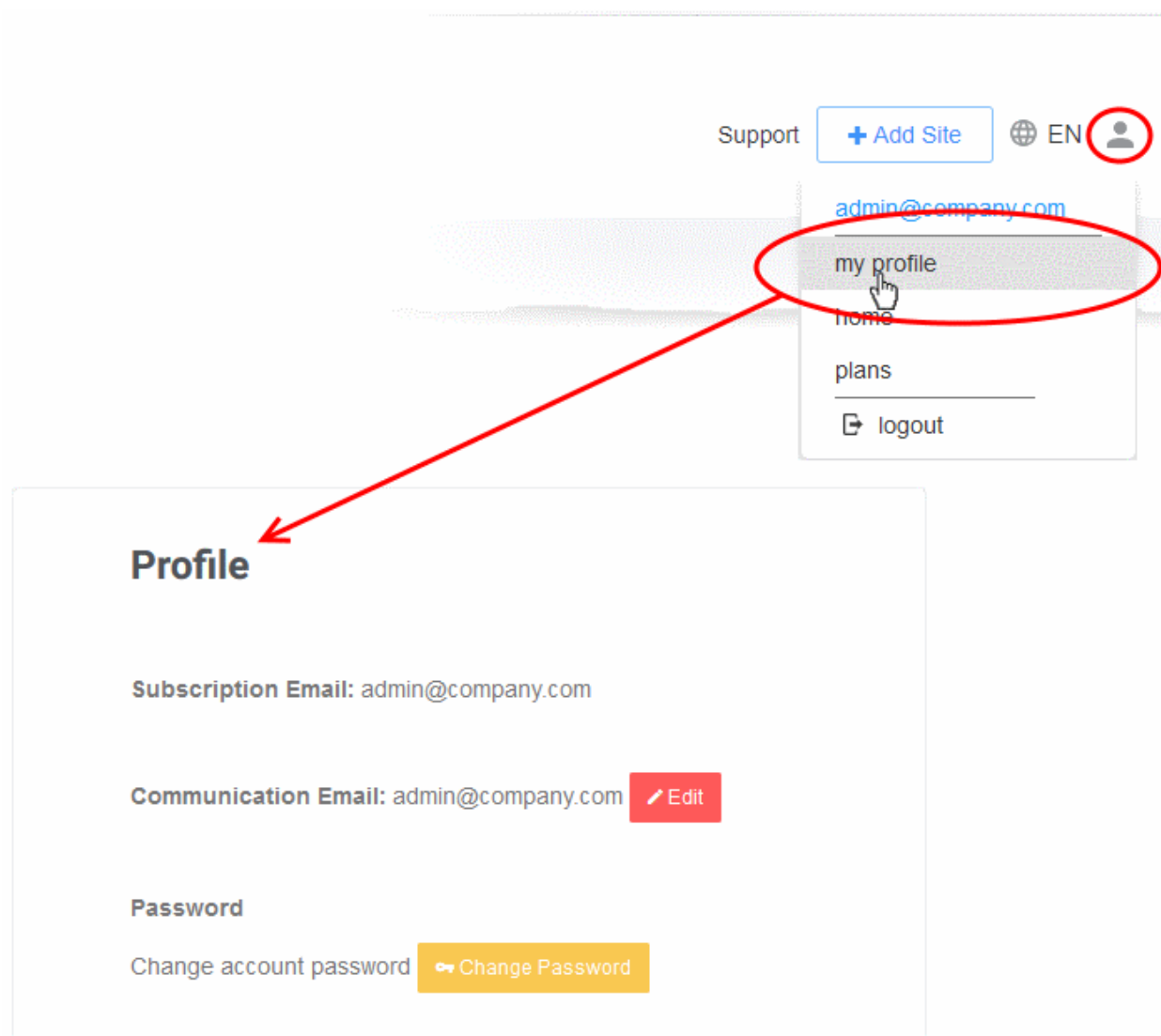
## 6 Manage Your Profile

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

### Manage your profile


- Click the user icon  at top-right
- Select 'My Profile' from the drop-down

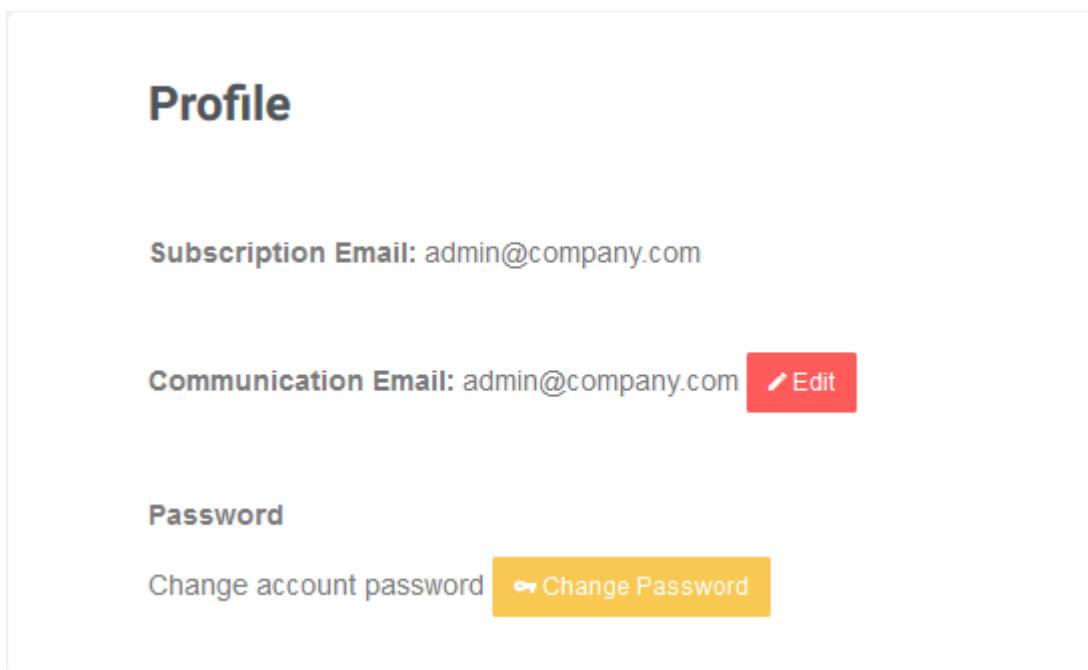




- **Edit your profile**
- **Change your password**

### Edit your profile

- Click the user icon  at the top-right
- Select 'My Profile' from the drop-down



**Profile**

**Subscription Email:** admin@company.com

**Communication Email:** admin@company.com [Edit](#)

**Password**

Change account password [Change Password](#)

- **Subscription Email** - The address you entered during sign-up. This cannot be edited.
- **Communication Email** -The address to which cWatch notifications are sent. By default, this is same as the subscription email.
  - All alerts, account and license emails are sent to this address.  
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
  - You can change this address if you want to receive the notifications at a different address.
    - Click 'Edit' beside 'Communication Email'


The image shows a 'Profile' page with two email addresses: 'Subscription Email: admin@company.com' and 'Communication Email: admin@company.com'. A red circle highlights an 'Edit' button next to the communication email. A red arrow points from this button to a modal form titled 'EDIT COMMUNICATION EMAIL'. The modal form contains the following fields:

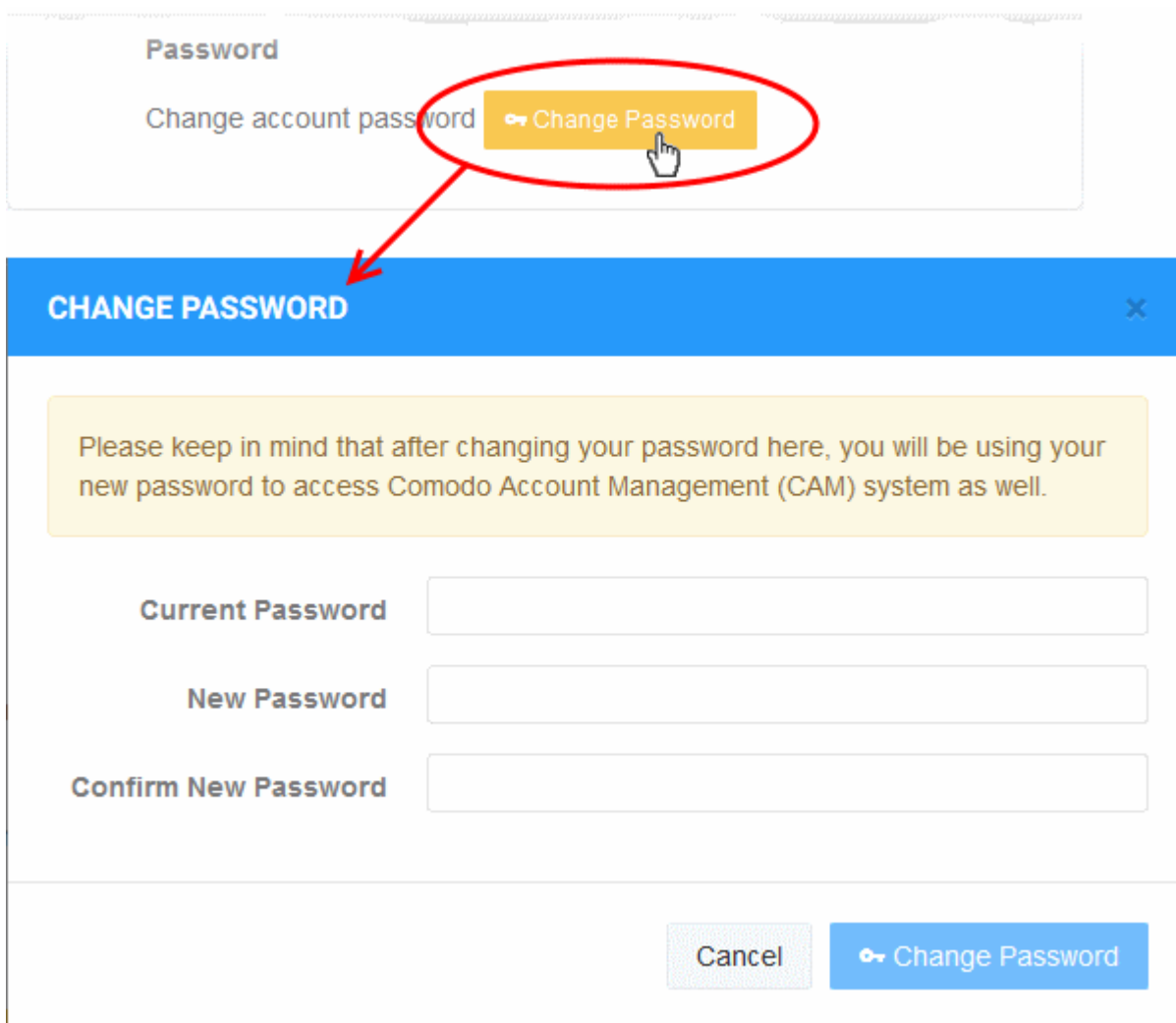
- Communication Email: admin@company.com
- New Communication Email:
- Re-Enter Communication Email:

Below the 'Re-Enter Communication Email' field, there is a red error message: 'Confirm email does not match!'. A blue 'Submit' button is located at the bottom right of the modal form.

- Enter the new email address and re-enter the same for confirmation.
- Click 'Submit' to save your changes.

### Change your password

- Click the user icon  on the top-left
- Select 'My Profile' from the drop-down
- Click 'Change Password' in the 'Profile' page



**Password**

Change account password [Change Password](#)

**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**

[Cancel](#) [Change Password](#)

- Confirm your existing password and create a new password
- Click 'Change Password'

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

## 7 Get Support

- The support page shows all malware clean-up requests you have submitted
- You can also create a new request from this interface
- Click 'Support' at top-right:

The screenshot shows the cWatch Support interface. At the top, there is a 'Choose Domain' dropdown and a 'Support' section with a '+ Add Site' button and a user profile icon. Below this, the 'Support' section is active, with tabs for 'ALL', 'OPEN TICKETS', and 'CLOSED TICKETS'. A blue '+ Add Ticket' button is visible. The main content is a table of tickets with the following data:

ID	TYPE	DOMAIN	DESCRIPTION	STATUS
6057726	MRR	checkmysite.com	Please check	OPEN
6055348	MRR	checkmysite.com	Please scan and check my site.	CLOSED
6055276	MRR	cwatchdemo.com	Please scan	CLOSED
6014215	MRR	cwatchdemo.com	Automatic Clean Up Request	CLOSED
6013528	MRR	cwatchdemo.com	Automatic Clean Up Request	CLOSED
5551463	MRR	cwatchdemo.com	I think my site is blacklisted...	CLOSED
5360506	MRR	cwatchdemo.com	--	CLOSED
5360415	MRR	cwatchdemo.com	--	CLOSED

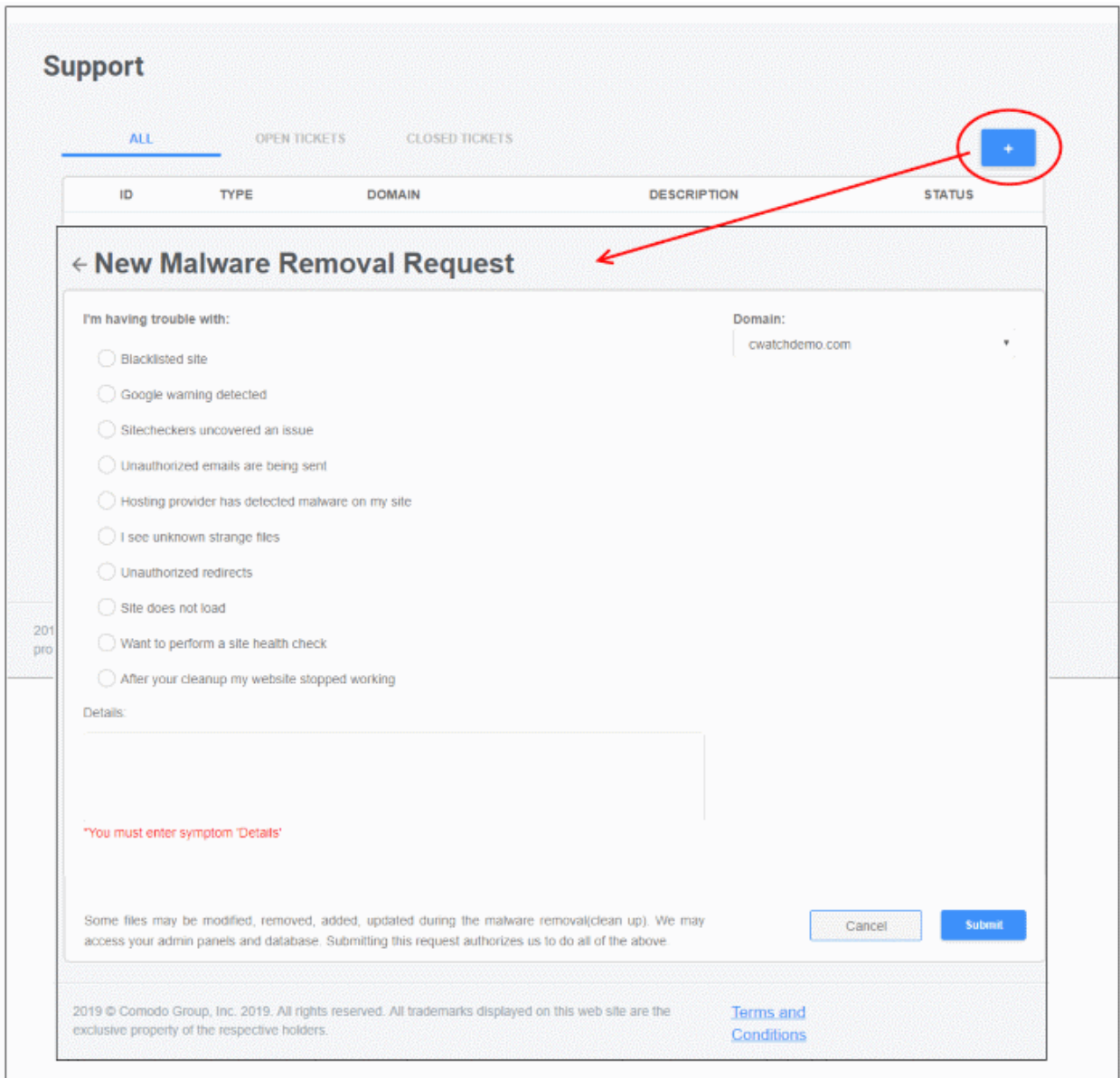
At the bottom of the table, there are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

- **All** – Shows both open and closed requests
- **Open Tickets** – Shows requests that are in-progress
- **Closed Tickets** – Shows completed requests

Support - Table of Parameters

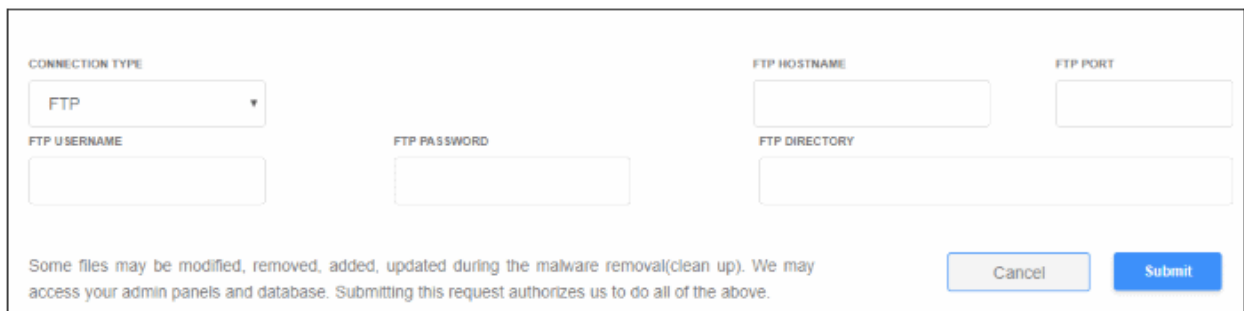
Column Header	Description
ID	Auto-generated ticket number. Click this to view the progress and download ticket report.
Type	Ticket category – 'MRR' (malware removal request) is the only category you will see here.
Domain	The website for which the ticket was raised.
Description	Notes on the issue which were provided when the ticket was created. Automatic Clean Up Request – Ticket raised automatically if option 'Switch On for automatic malware' is enabled in 'Malware' > 'Settings' > 'Automatic Malware Removal' pane.
Status	Indicates whether the issue is pending or completed.

- Click the '+' button to create a ticket manually



- **Domain** – Your websites will be listed in the drop-down. Select the website for which you want to create a ticket.
- Select the issue(s), provide short notes about the problem in the details box and click 'Submit'
- A ticket will be created and listed in the table. Our technician will attend to the problem.

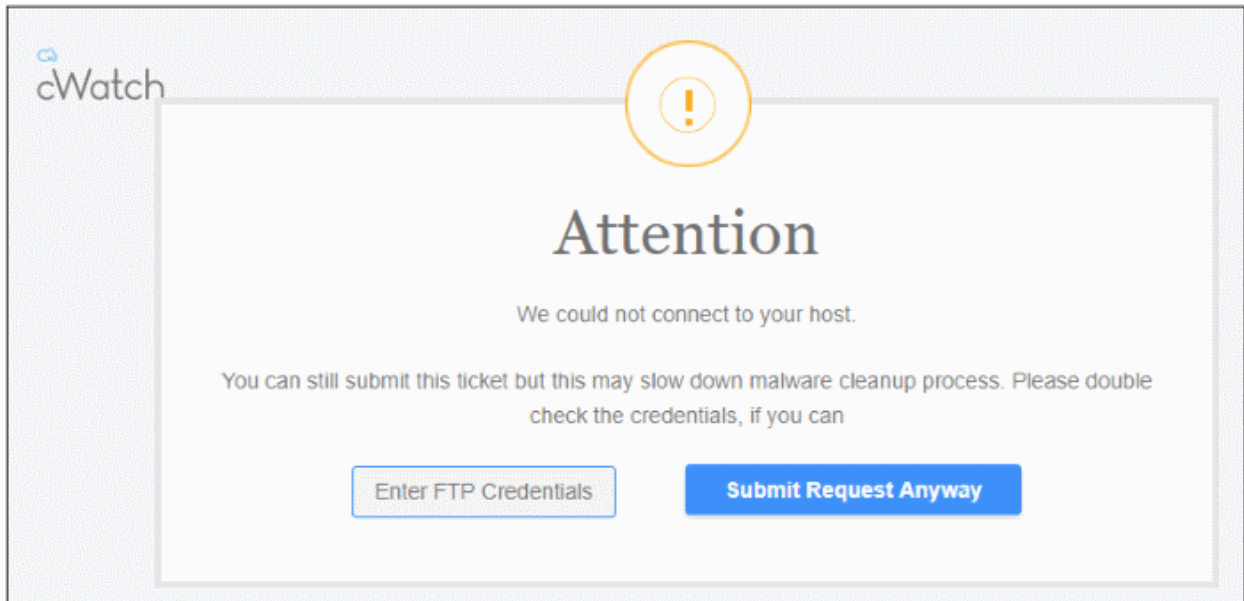
The following option appears if the site does not have scanning enabled, or the the FTP credentials have changed.



- Enter your site's FTP details and click 'Submit'
- You can configure the FTP settings in the malware page, or upload the agent manually. See '**Automatic**

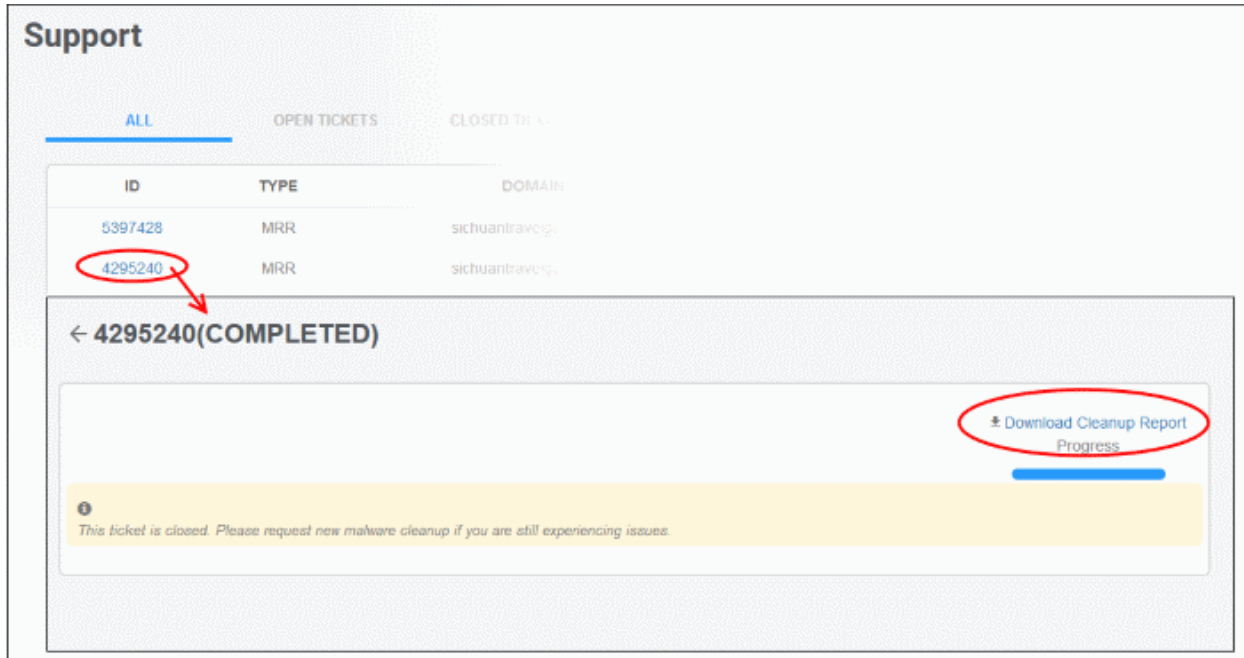
**Configuration** and **Manual Configuration** for help with malware scanner configuration.

If you submit the request without providing the FTP details, the following alert is shown:



Comodo recommends you provide FTP details for quicker resolution of the request.

- Click 'Submit Request Anyway'. Note – This will slow down the malware cleanup process.
- Click the request ID to download the cleanup report:



- Click 'Download Cleanup Report' and save the file.



### Malware Cleanup report for [sichuantravelguide.com](http://sichuantravelguide.com)

MRR created: 2019-04-28 04:02:07 UTC  
 MRR closed: 2019-05-27 05:47:07 UTC  
 Report generated: 2019-08-01 06:45:36 UTC

#### Summary

The malware scan for your domain [sichuantravelguide.com](http://sichuantravelguide.com) was completed successfully and we found a total of 3 files to be suspicious in nature. The breakdown is as follows:

Infection Type	Count	Action performed
Malicious	2	Fully malicious files
Safe	0	Files marked as safe for execution
Suspicious	0	Files that look suspicious but don't have verdict yet
Infected	1	Files that were infected
Quarantine Success	0	Malicious files that were moved to quarantine
Quarantine Failed	0	Files for which attempts to quarantine were unsuccessful
Total	3	

#### Details

Cured:

File Path	Action Taken
./well-known/index.php	Cured successfully
./manager/includes/controls/phpmailer/vwzfgbbo.php	Cured successfully

Deleted:

File Path	Action Taken
./b601f3e7.ico	File deleted

Comment:

End of report

Thank you for your patience and choosing cWatch. Please do feel free to reach out to us should you have any queries.  
<https://cwatch.comodo.com>

The report provides details such as number of infected files, path of the file, action taken and so on.



# 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)