COMODO
Creating Trust Online®

Comodo

cWatch Web Security

Software Version 4.10

Website Administrator Guide

Guide Version 4.10.040119

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

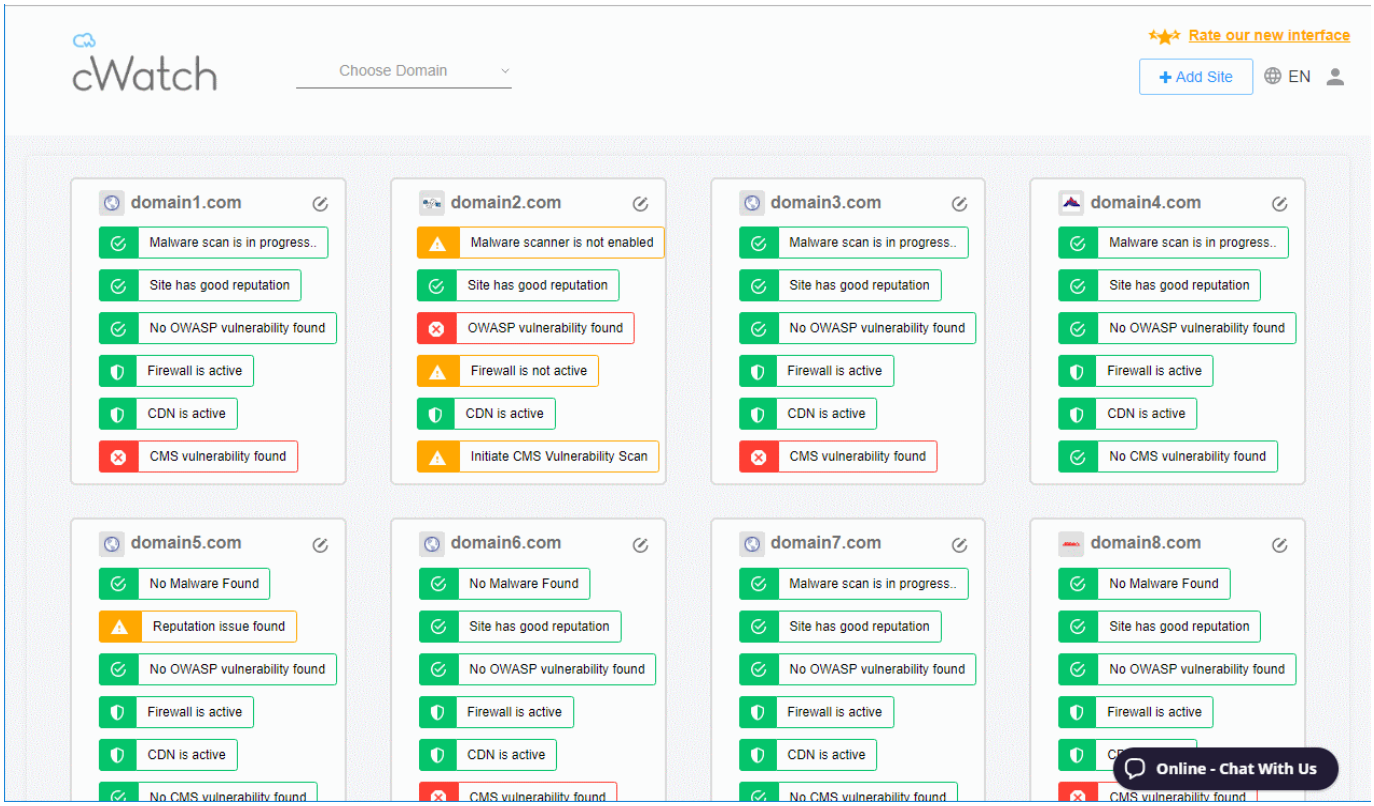
Table of Contents

1 Introduction to Comodo cWatch Web Security

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

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

cWatch Web Security is available in three different service levels. More details are available in **License Types**.



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**

1.1 Purchase a License

Three types of cWatch license are available:

- Basic
- WAF Starter
- Pro
- Premium

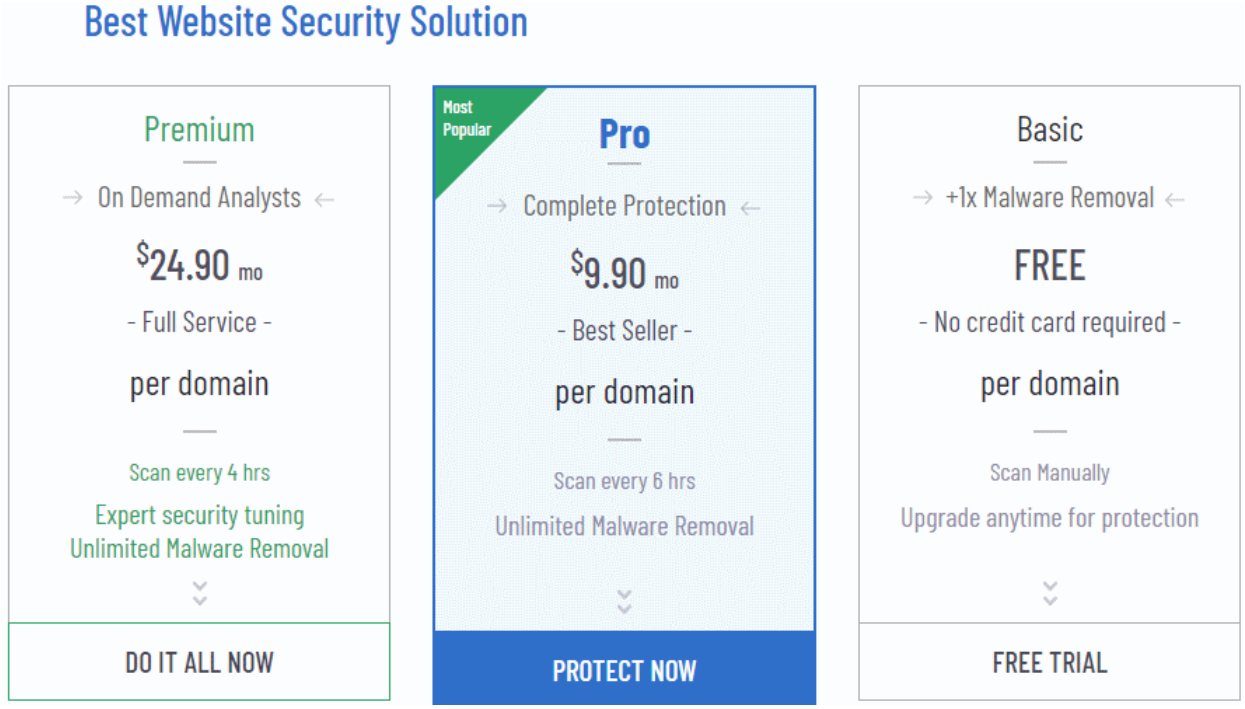
For more details on the services offered with each, see **License Types**.

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

- You can associate websites with licenses in the cWatch interface. See **Add Websites** for more details.

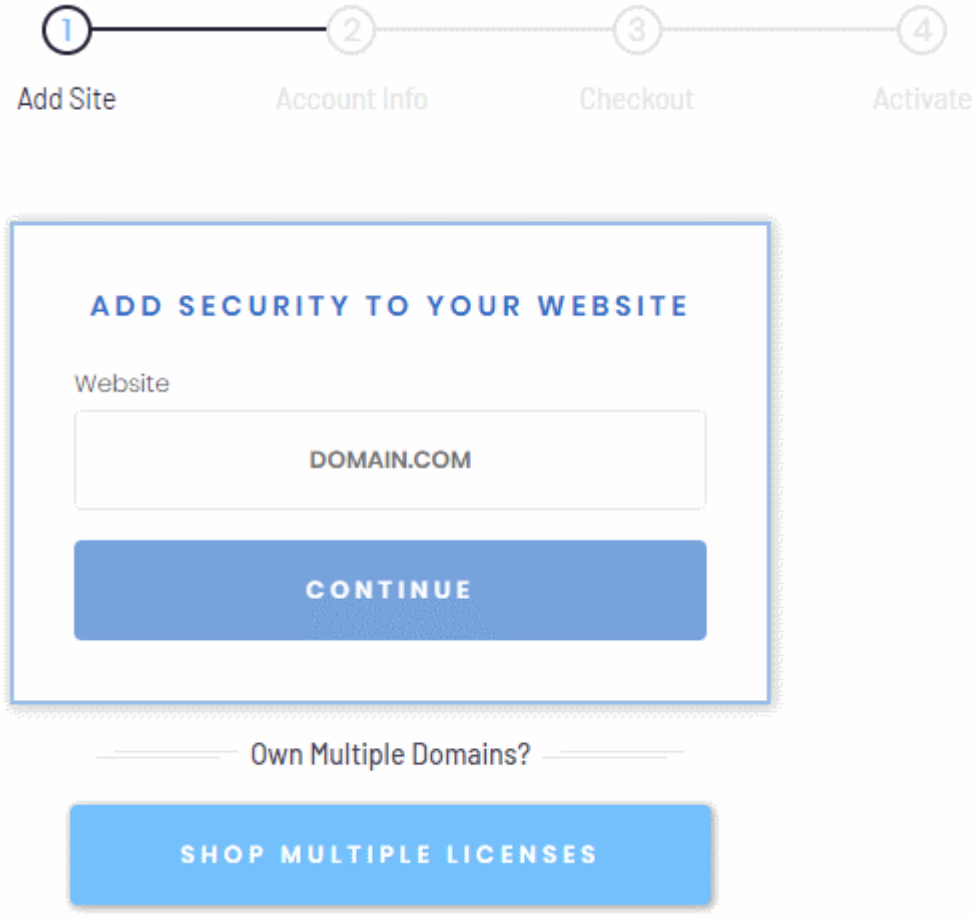
Purchase a license

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



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

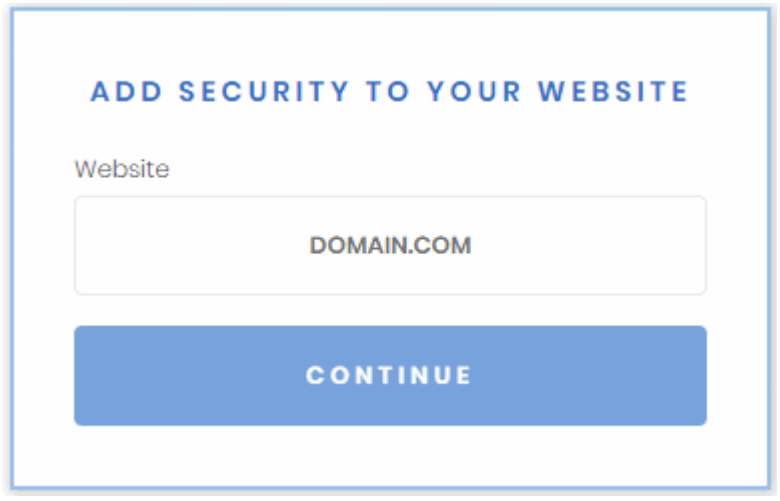
You will be taken to license configuration page:



- 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.

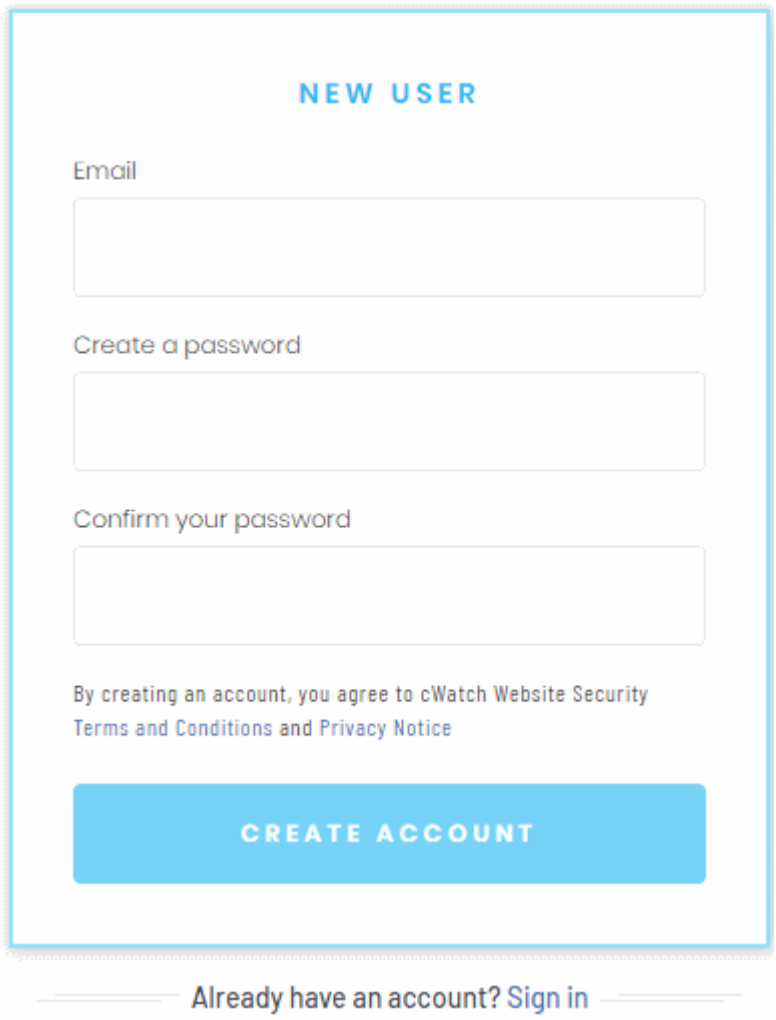
Purchase single domain license

Step 1 - Enter your domain name

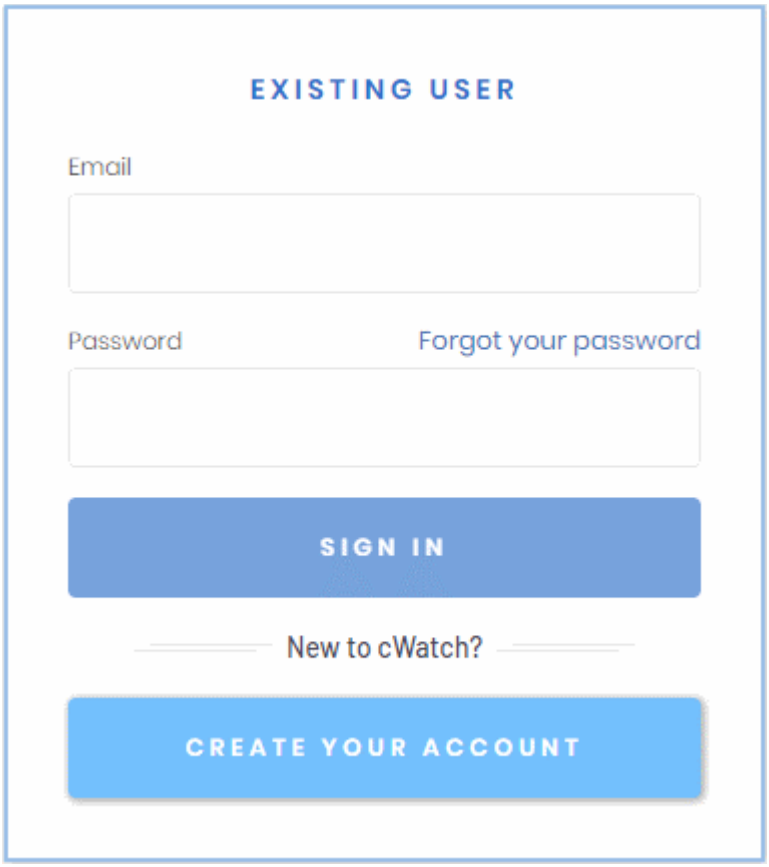


- Type your website (without 'www.') in the Website field and click continue

Step 2 - Enter your Comodo account Information

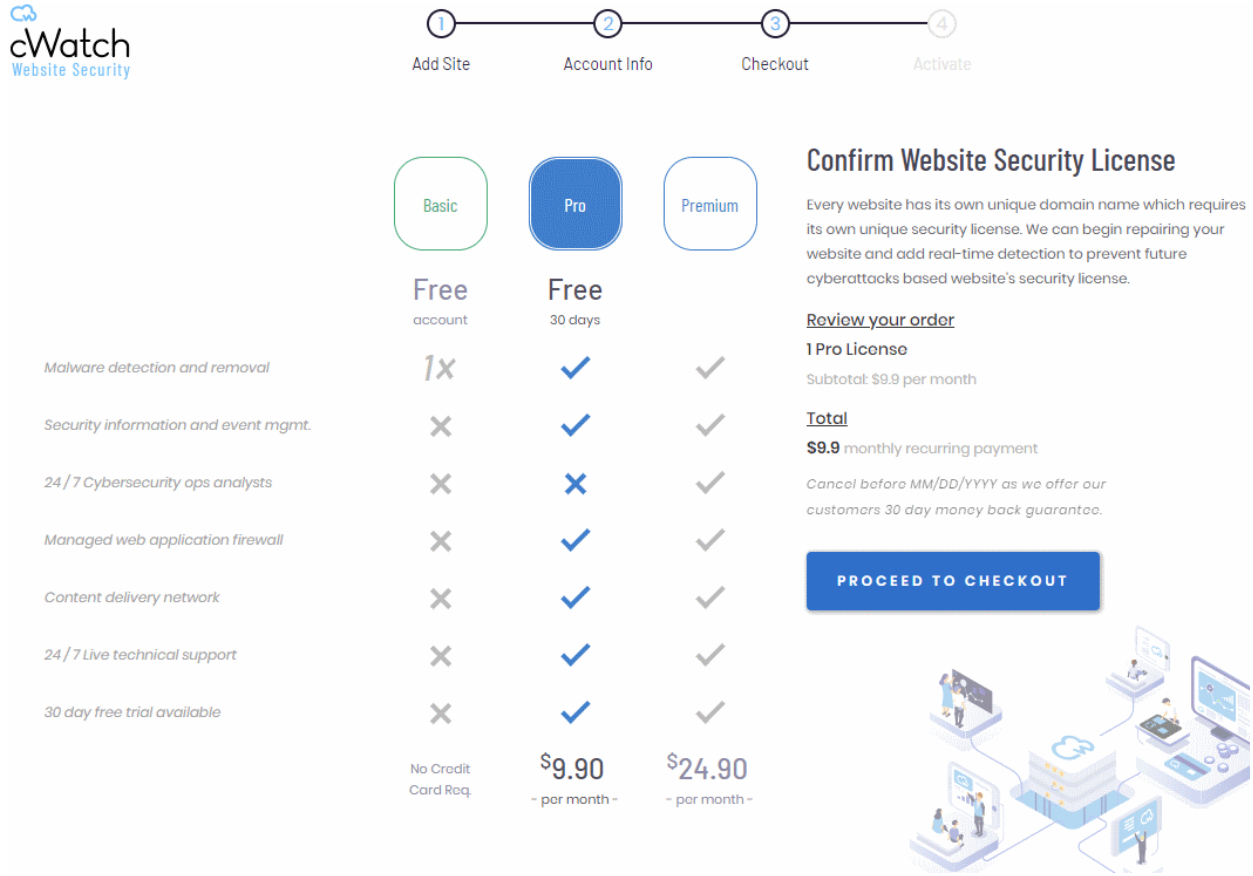


- If you don't have a Comodo account, enter your email address and a password to create a new account
- If you already have a Comodo account, click 'Sign in'



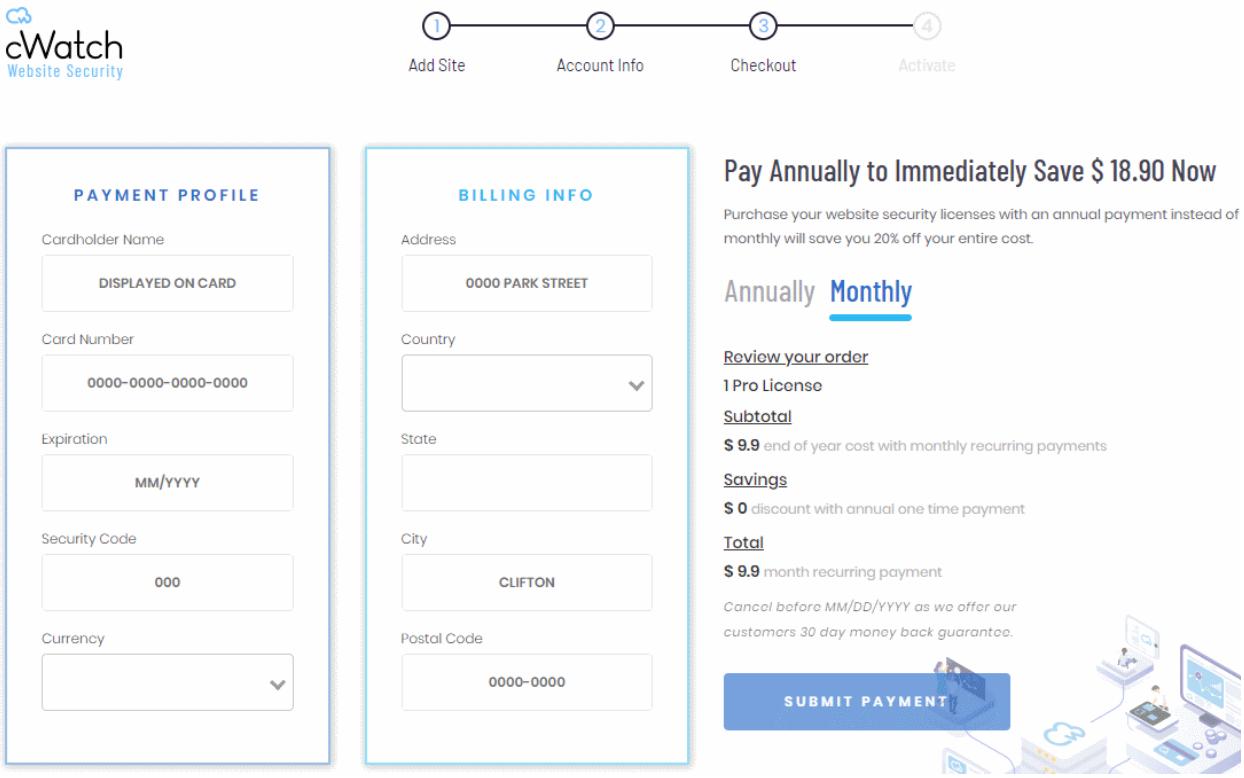
- Enter your username and password and click 'Sign-in'

Step 3 - Select License Type



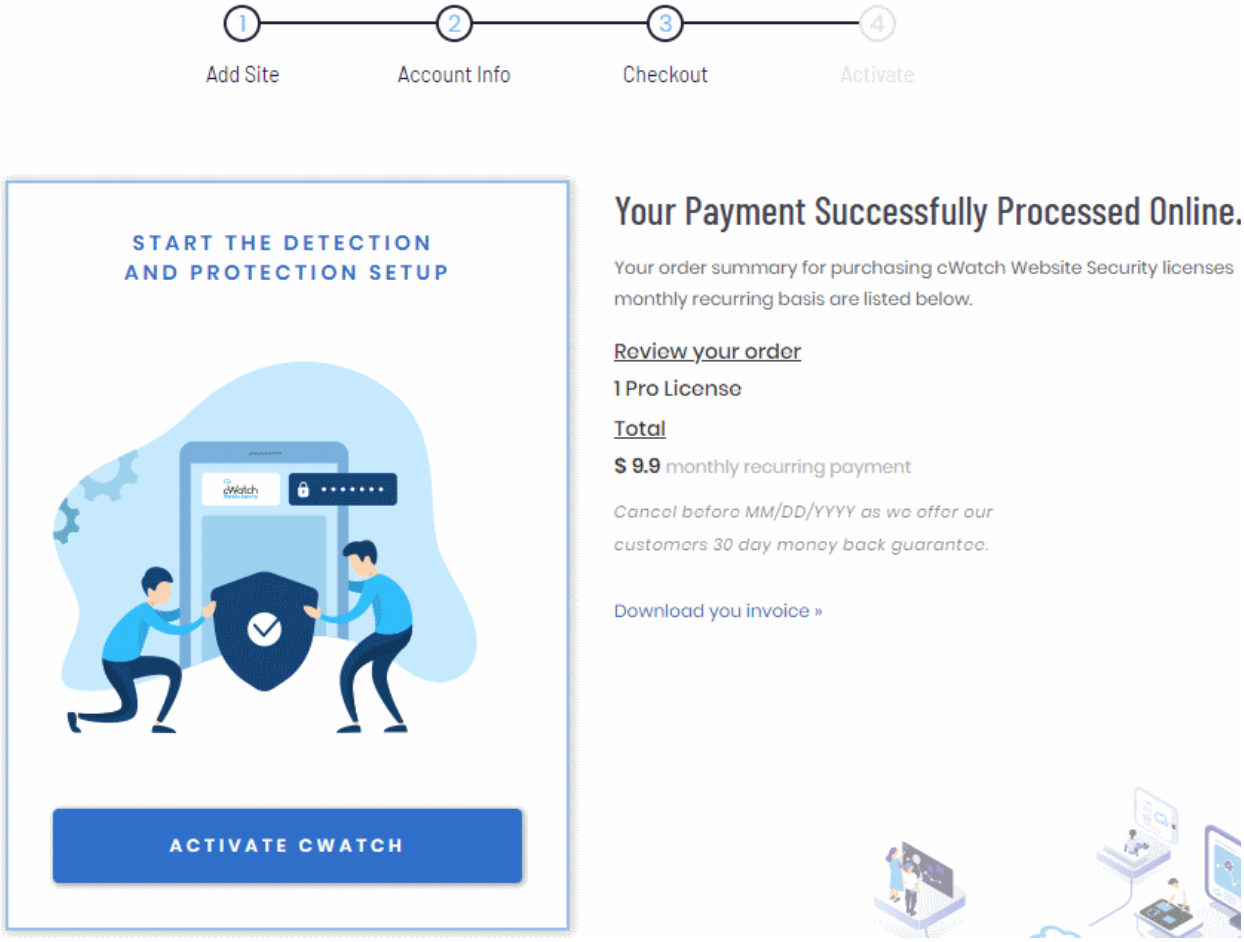
- Select the license type for the domain. See **License Types** for more details about the features of each license.
- Click 'Proceed to Checkout'

Step 4 - Enter Payment Details

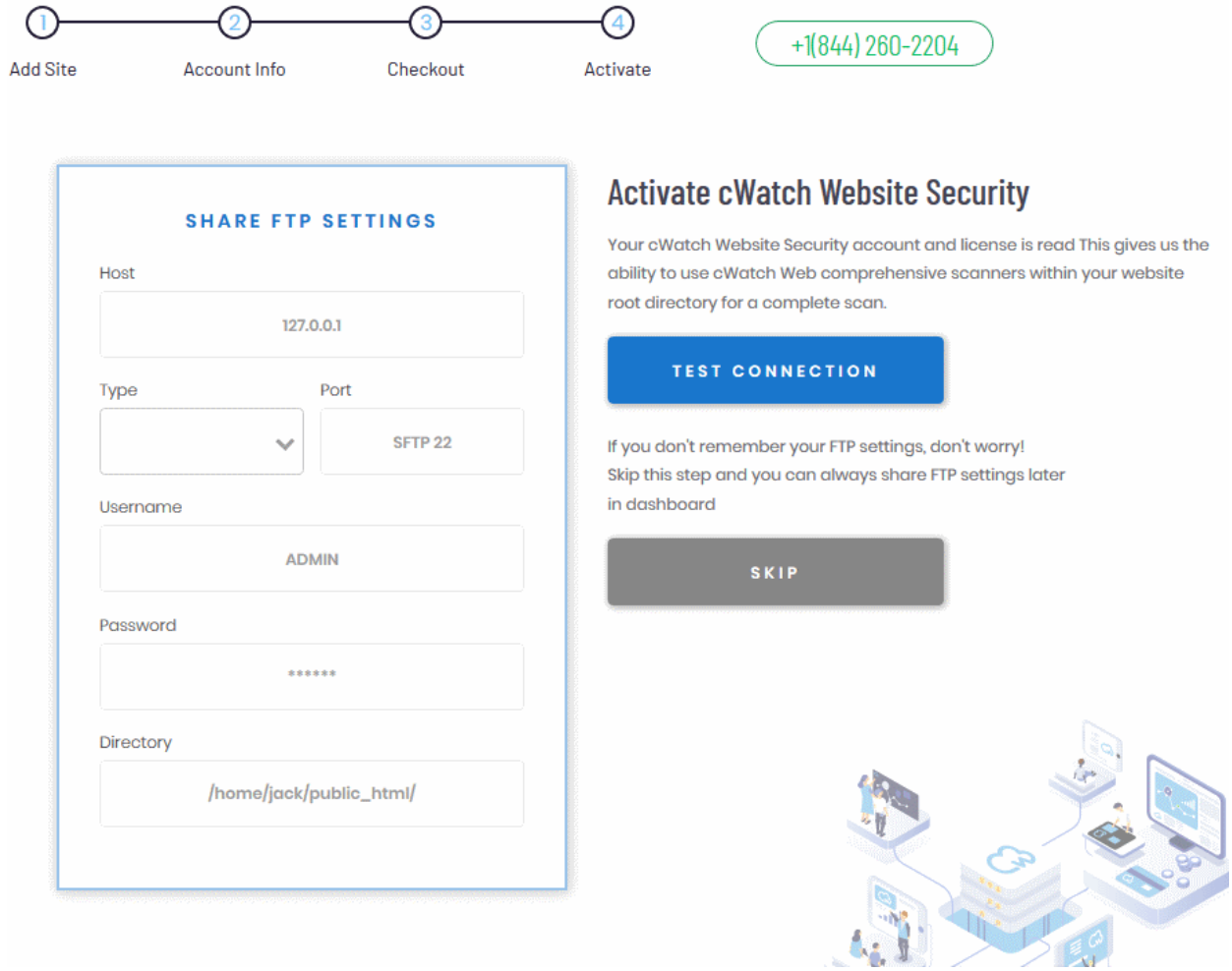


- Payment Profile - Enter your card details for recurring payments for auto-renewal of license.
- Billing Info - Enter your billing address
- Choose the period of license. The available options are 'Annually' or 'Monthly'.
- Click 'Submit Payment'

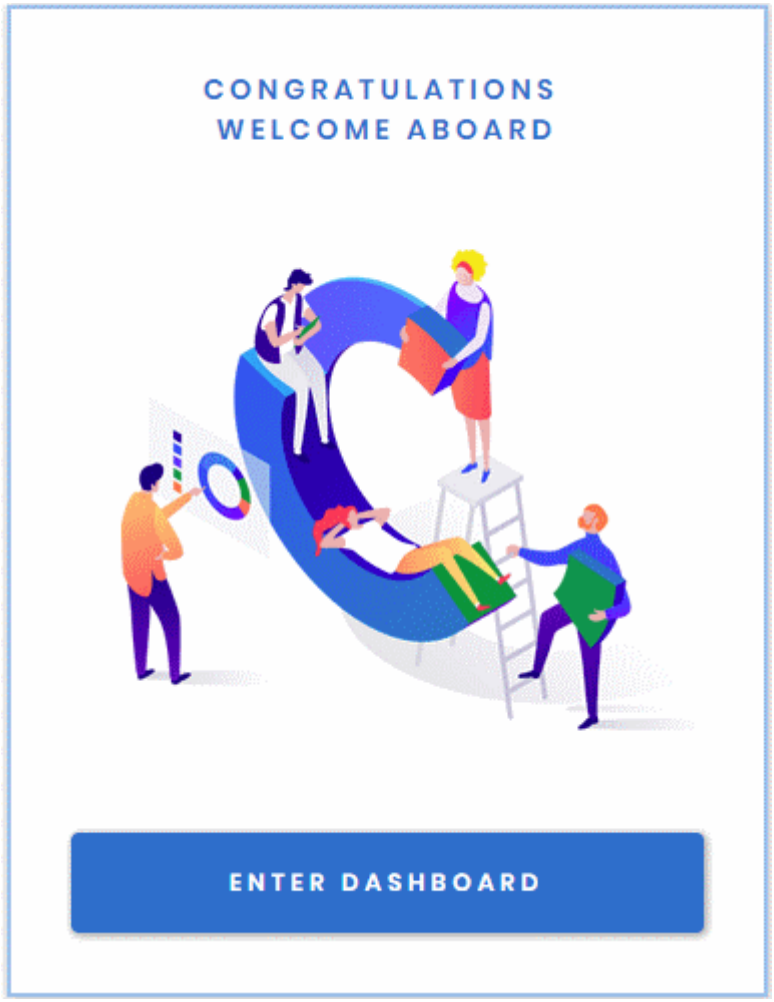
Step 5 - Activate License



- Click 'Activate cWatch' to start protecting your website
  - 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.

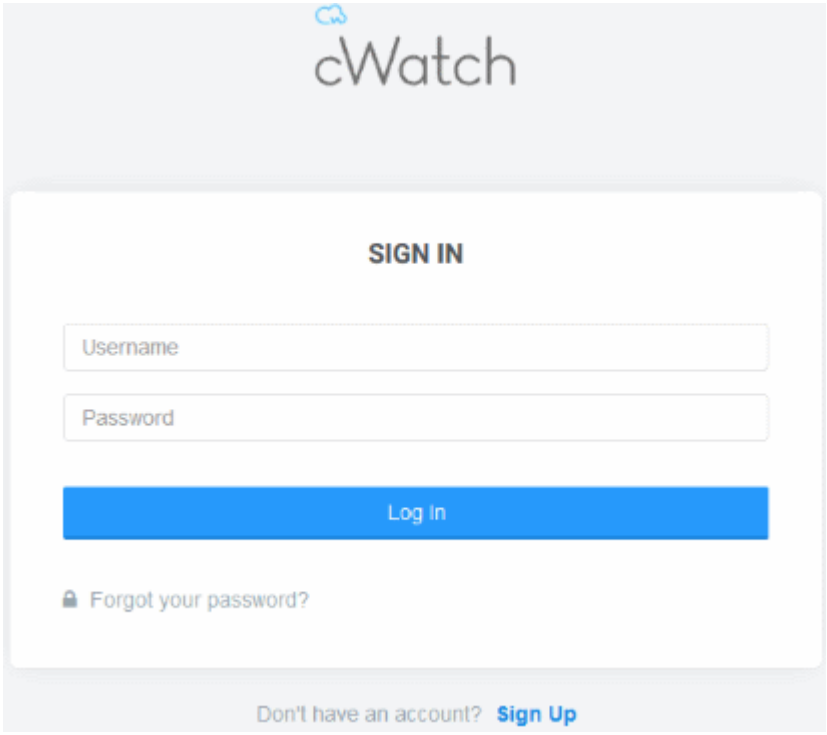


- Enter the hostname, login details and upload directory. The location must be publicly accessible.
- Click 'Test Connection' for cWatch to check whether it can reach the location.
  - Note. Our technicians will also use these settings to access your site IF you request them to remove malware.
- Click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

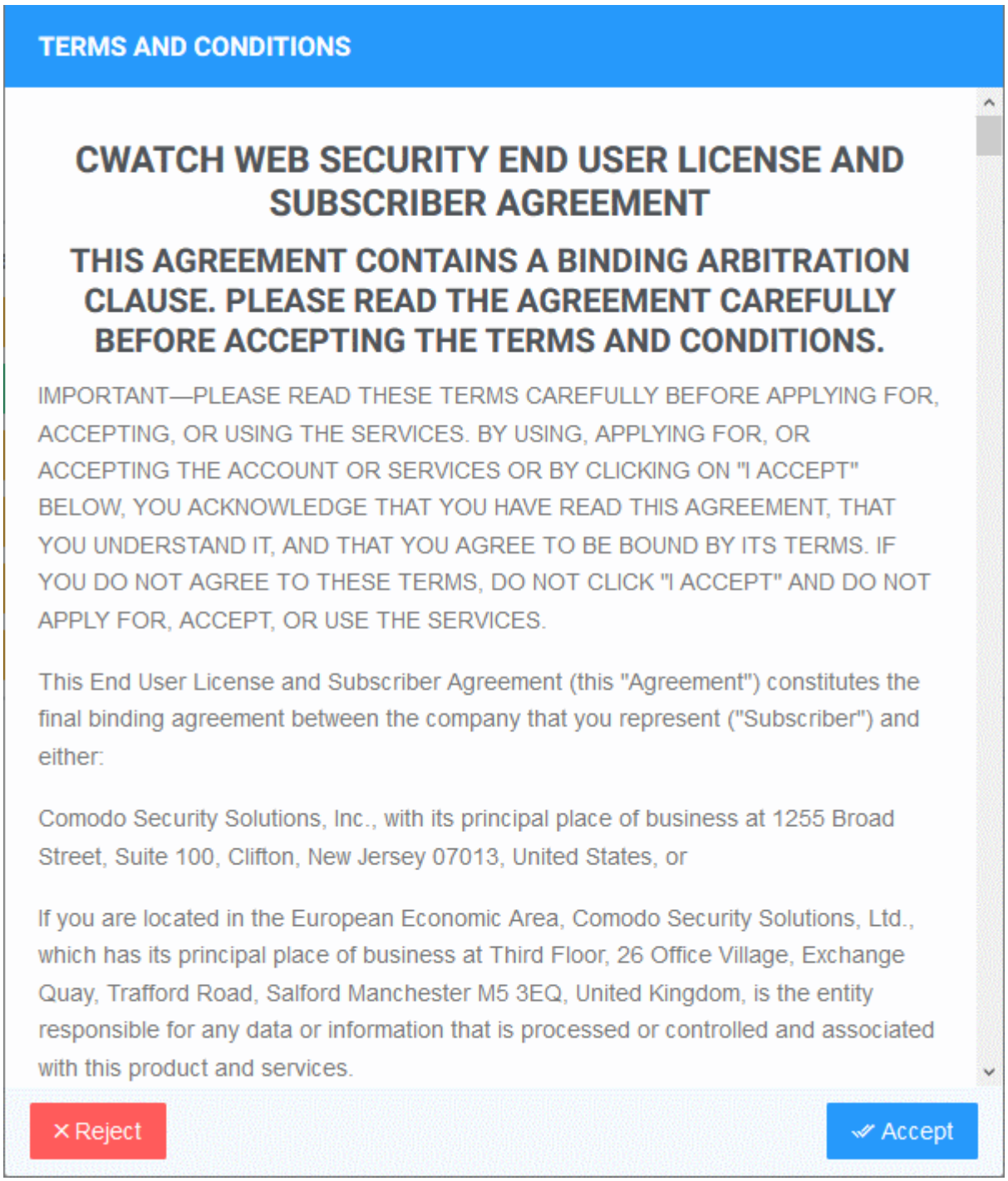


Your license is now activated.

- Click 'Enter Dashboard' to login to cWatch



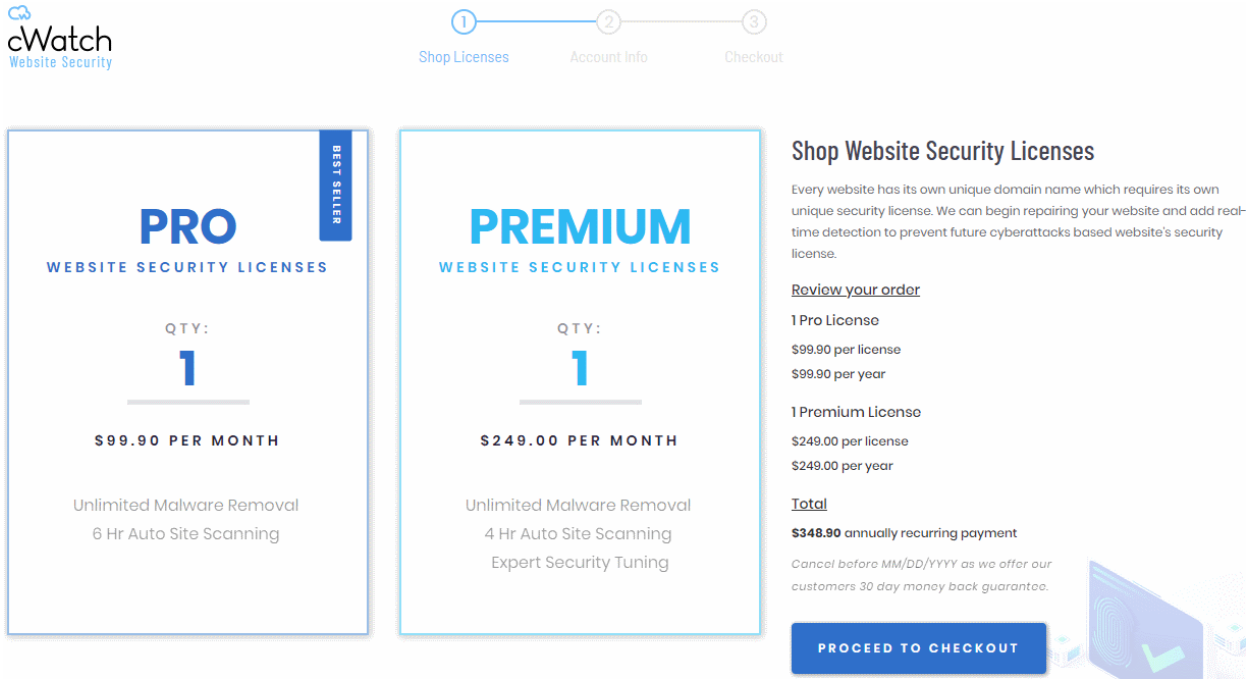
- Use your Comodo username and password to login to cWatch.
- You have to read and accept to the 'Terms and Conditions' on your first login.



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

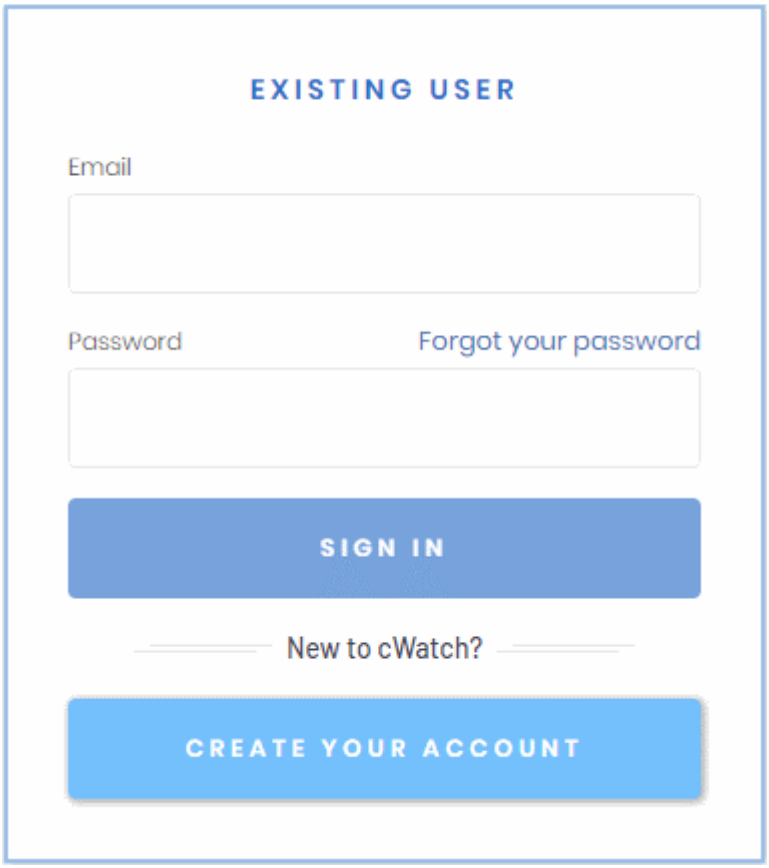
Purchase multi-domain license

Step 1 - Select Licenses

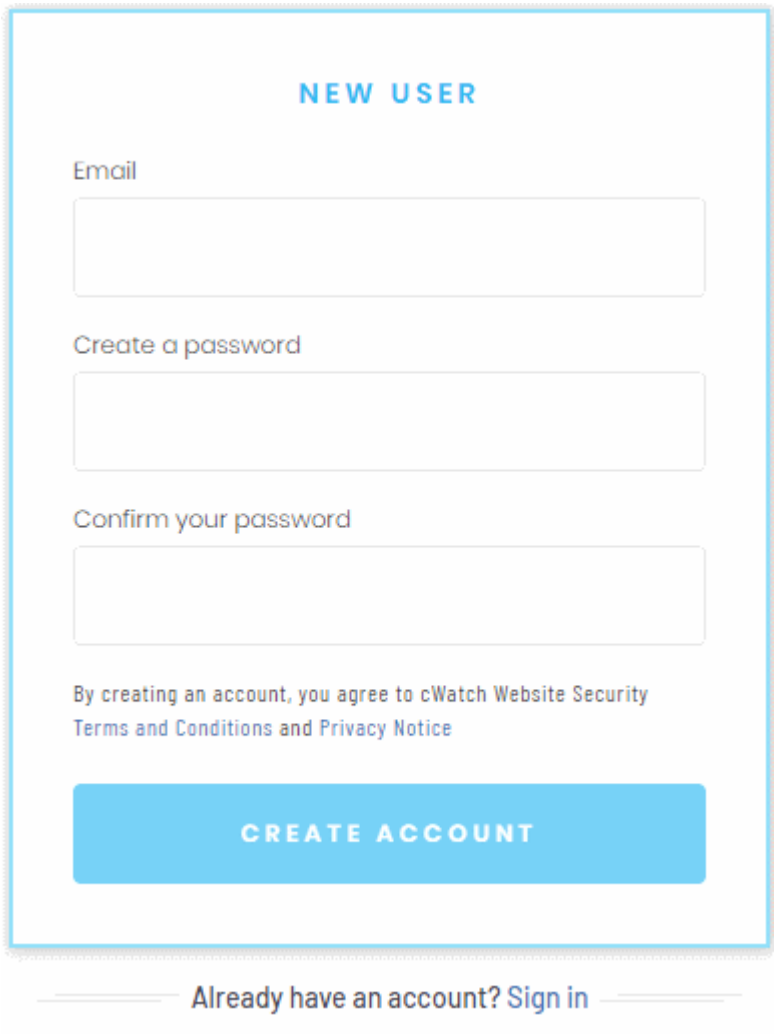


- Enter the number of licenses you want in the 'Pro' and/or 'Premium' boxes.
- Each license covers one domain or sub-domain
- Click 'Proceed to Checkout'

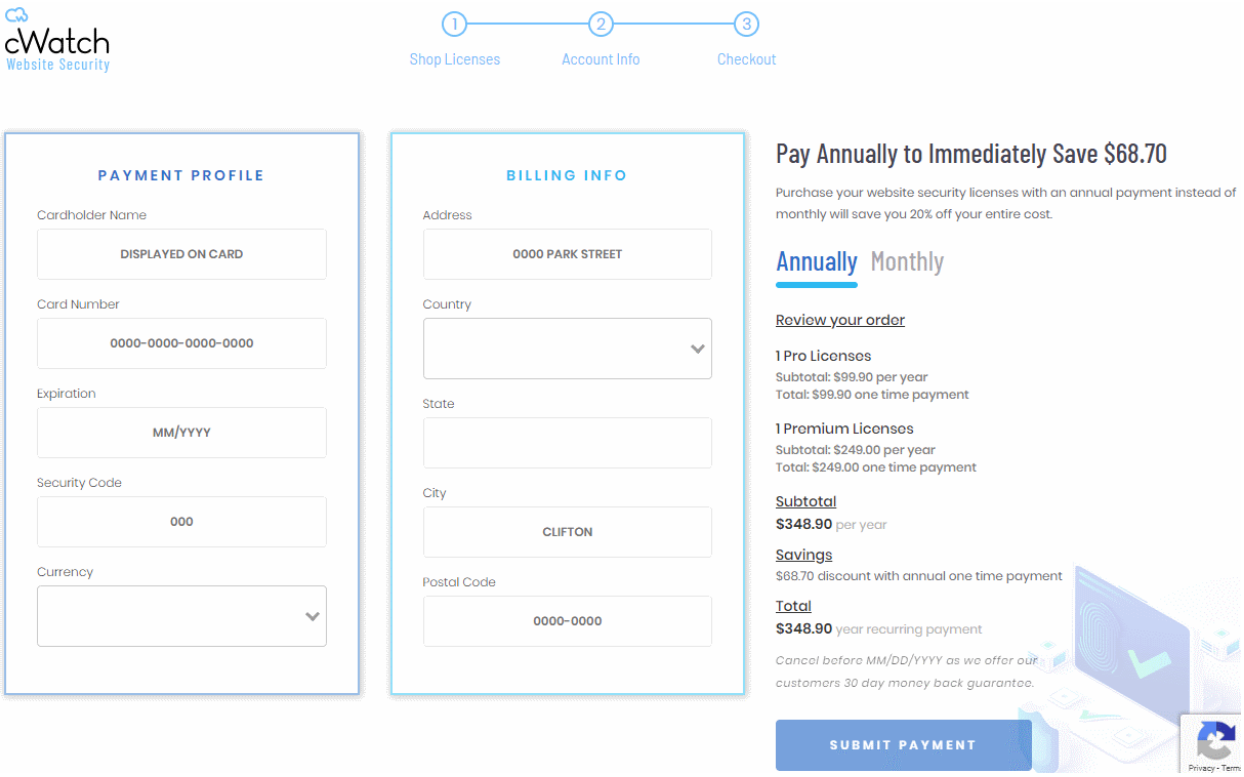
Step 2 - Enter your Comodo account Information



- 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

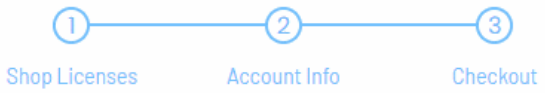


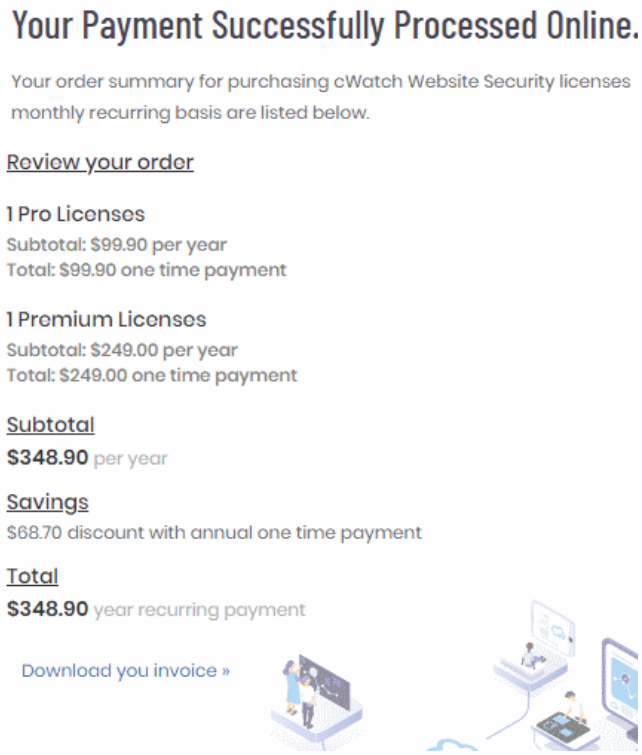
Step 3 - Enter Payment Details



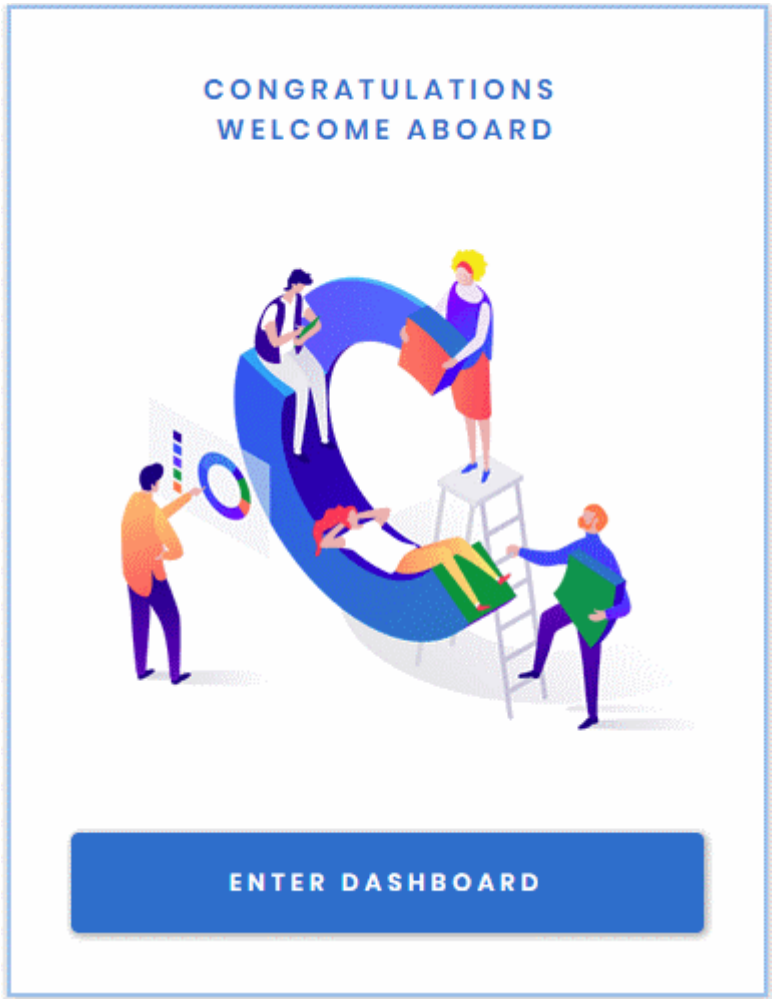
- Payment Profile - Enter your card details for recurring payments for auto-renewal of licenses.
- Billing Info - Enter your billing address
- Choose the period of license. The available options are 'Annually' or 'Monthly'.
- Click 'Submit Payment'

Step 4 - Activate License



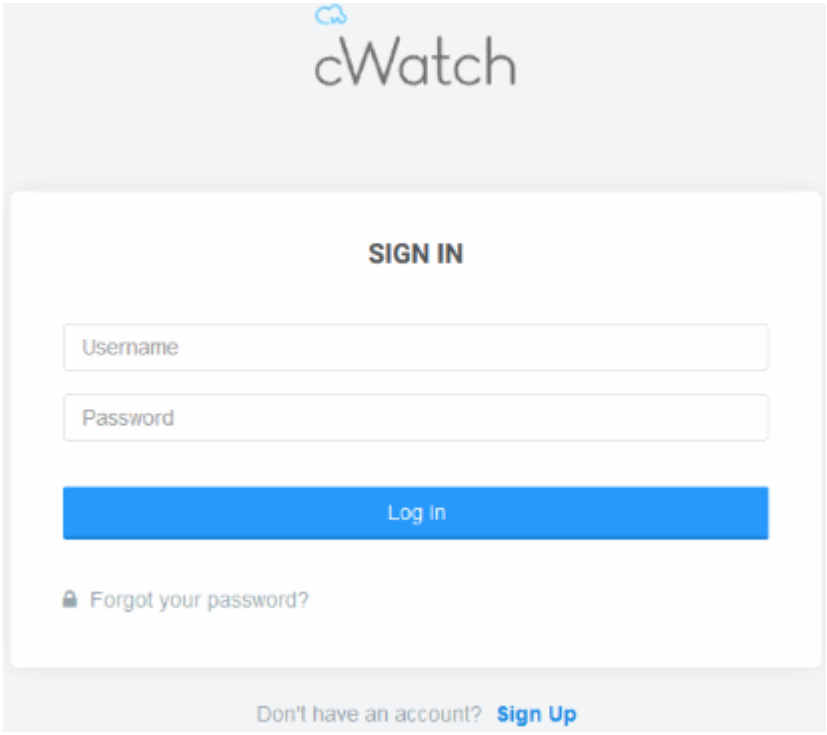


- Click 'Activate cWatch' to start protecting your website

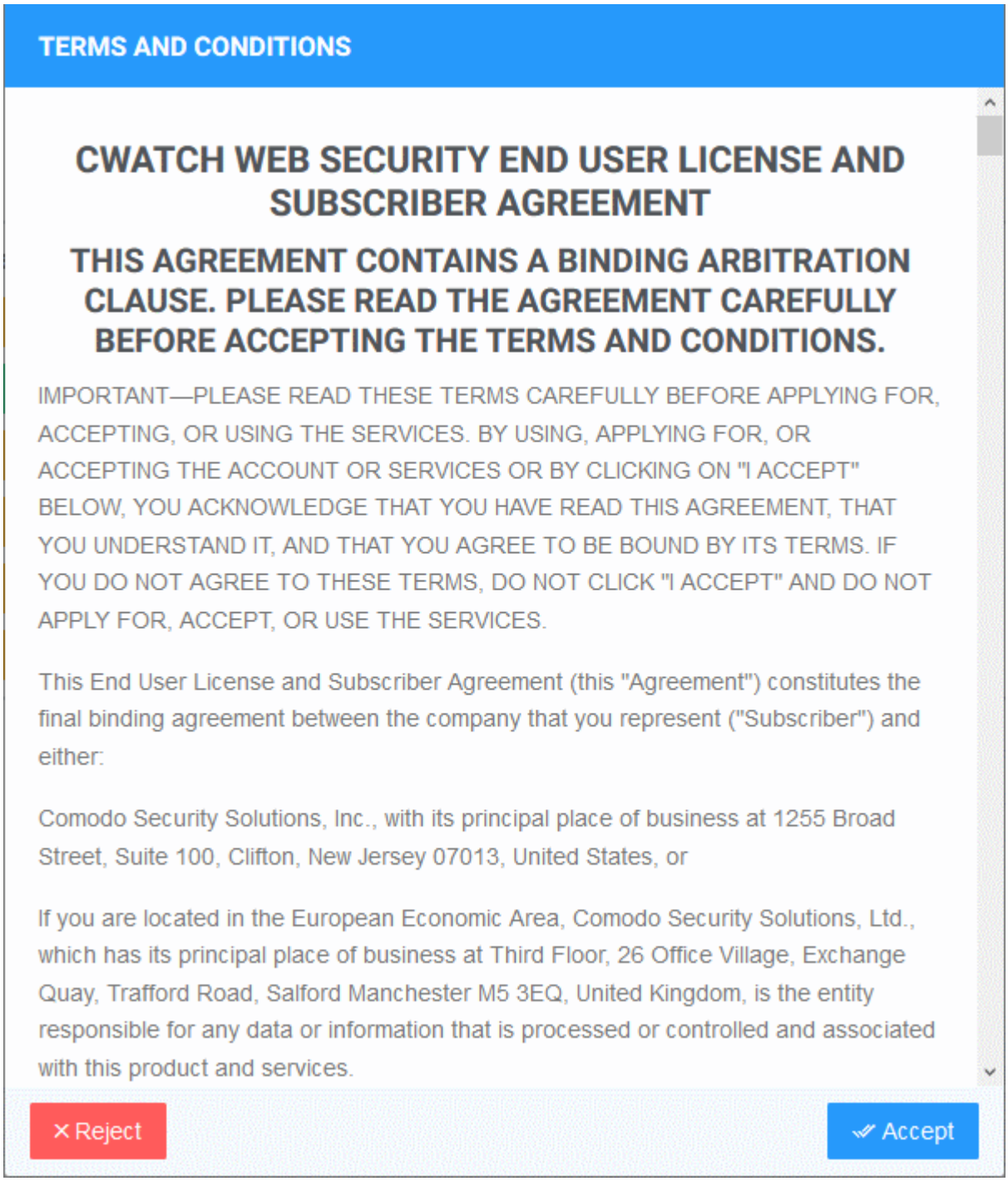


Your license is now active.

- Click 'Enter Dashboard' to login to cWatch



- 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.



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

The three license types are:

- Basic

- WAF Starter
- Pro
- Premium

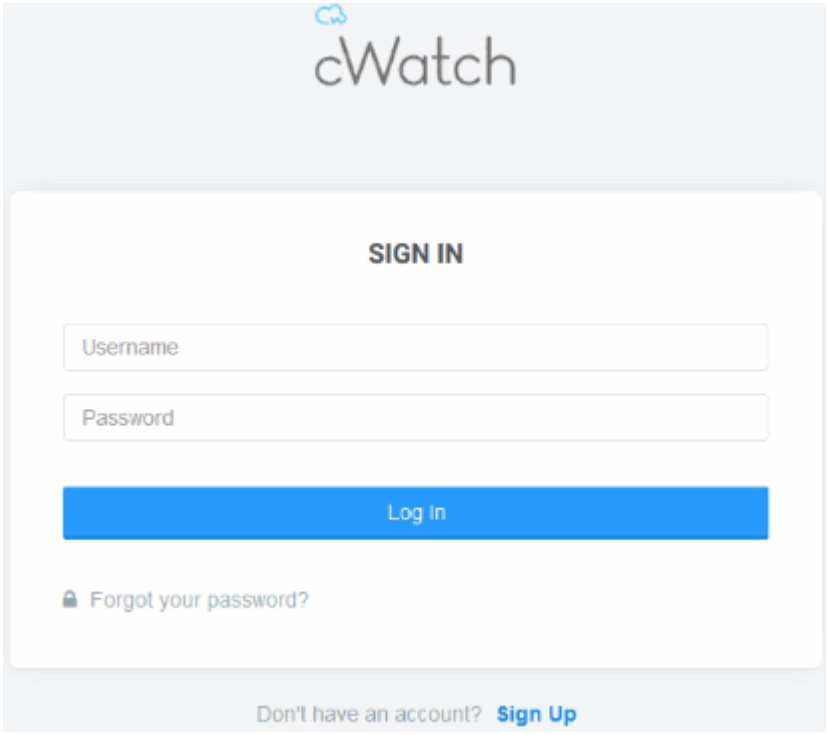
The following table shows the features available with each license type:

Feature/Service	Premium	Pro	WAF Starter	Basic
Malware Detection and Removal				
Malware removal by experts Hack repair and restore Vulnerability repair and restore Traffic hijack recovery SEO/Search poisoning recovery	Unlimited	Unlimited	One time	One time
Automatic Malware Removal	✓	✓	✗	✗
Spam & Website Filtering	✓	✓	✗	✗
Malware Scan	Every 6 hours	Every 12 hours	Every 24 hours	Every 24 hours
Vulnerability (OWASP) Detection	Every 6 hours	Every 12 hours	Every 24 hours	Every 24 hours
Security Information and Event Management (SIEM)	✓	✓	✗	✗
24/7 Cyber-Security Operations Center (CSOC)	✓	✓	✓	✗
Dedicated analyst	✓	✓	✓	✗
Web Application Firewall (WAF)				
Custom WAF rules	✓	✗	✗	✗
Bot Protection	✓	✓	✓	✗
Scraping Protection	✓	✓	✓	✗
Content Delivery Network (CDN)				
Layer 7 DDoS Protection	✓	✓	✓	✓
Layer 3, 4, 5 & 6 DDoS Protection	✓	✓	✓	✓
Trust Seal	✓	✓	✓	✓

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:

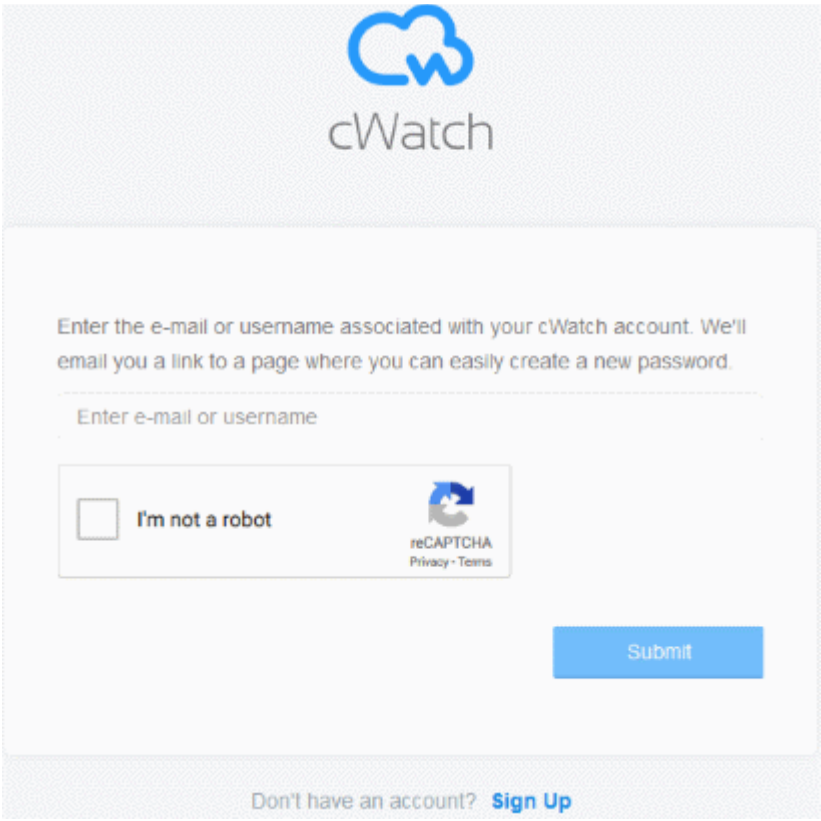


First time login

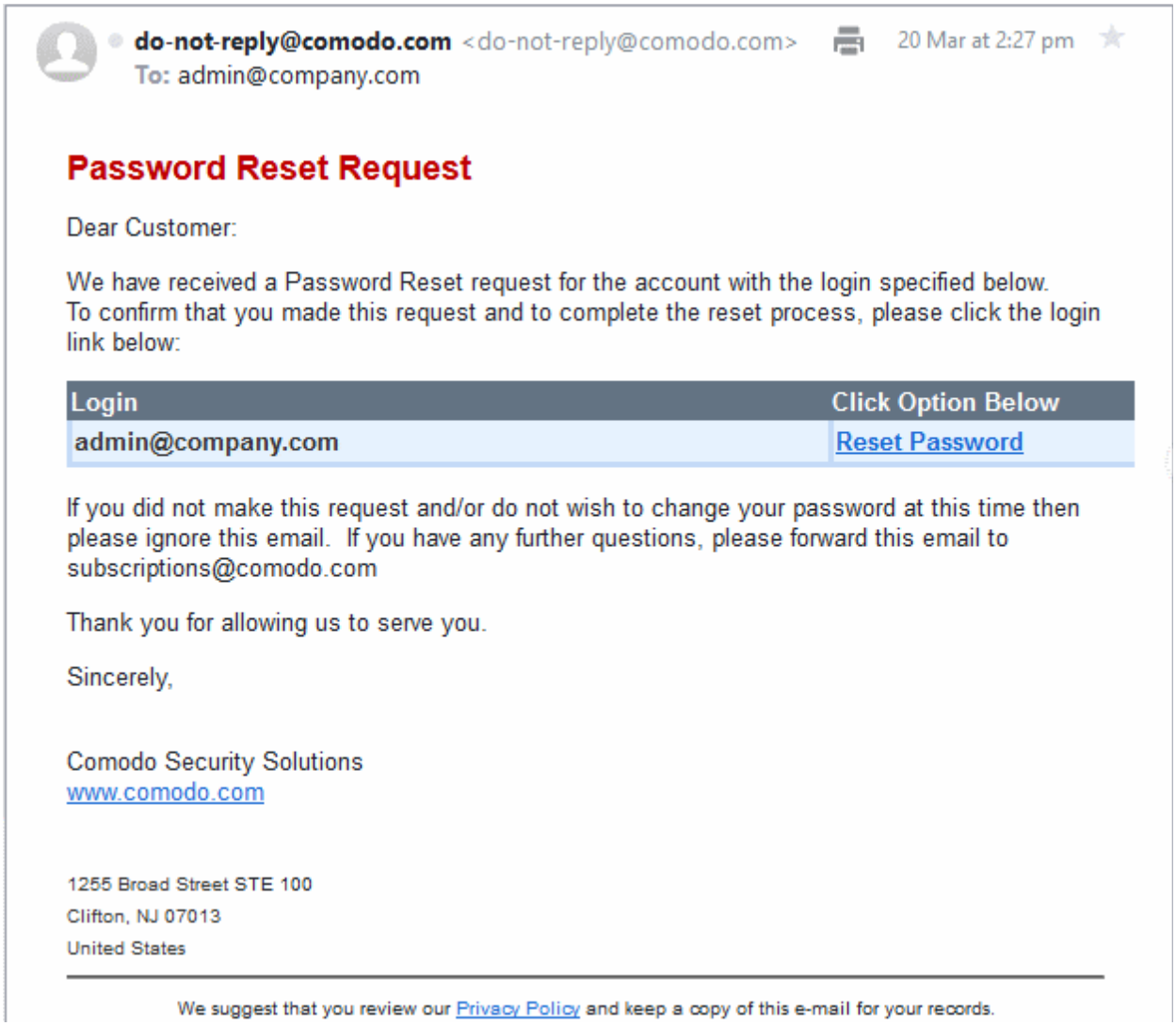
- Get your username and password from the cWatch confirmation email.
- After logging in, we strongly recommend you change your password for security reasons.

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:



- 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	Reset Password

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

Thank you for allowing us to serve you.

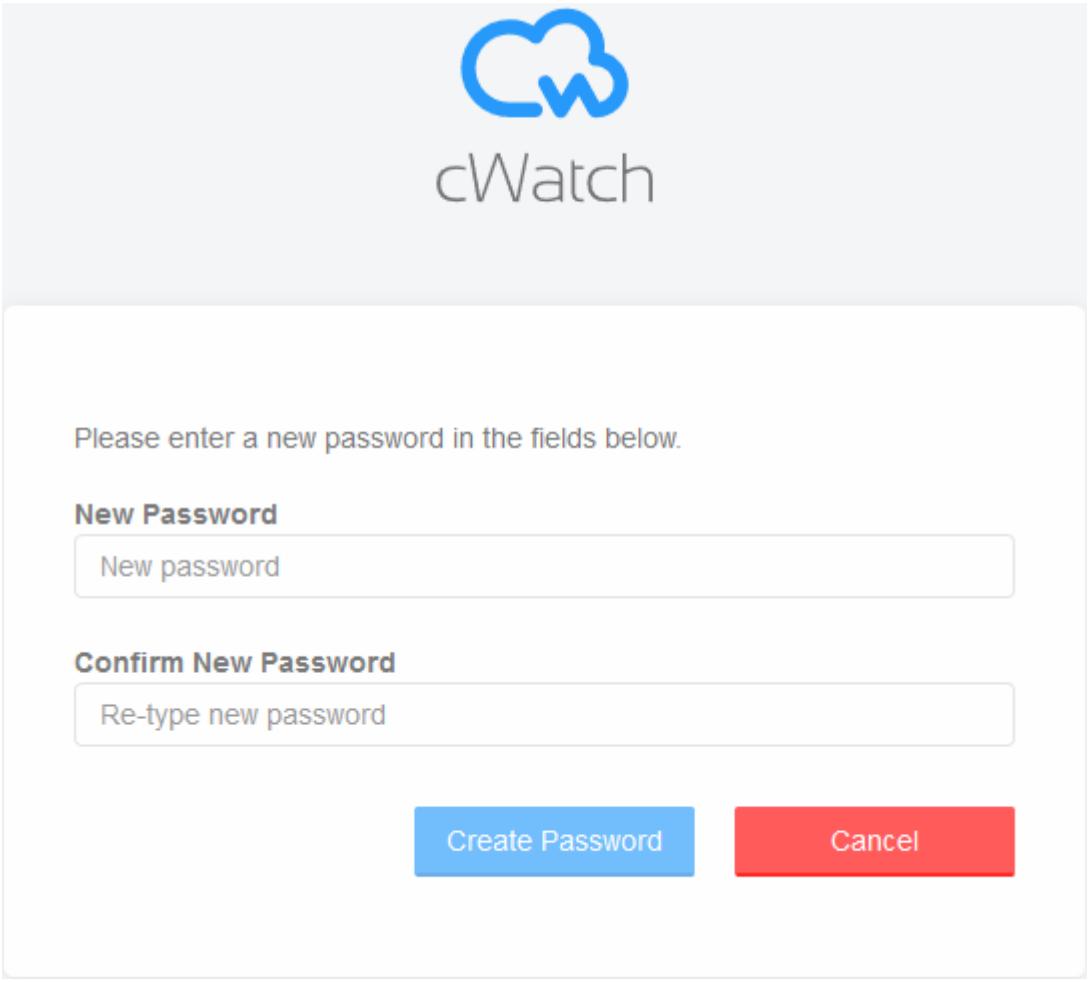
Sincerely,

Comodo Security Solutions
www.comodo.com

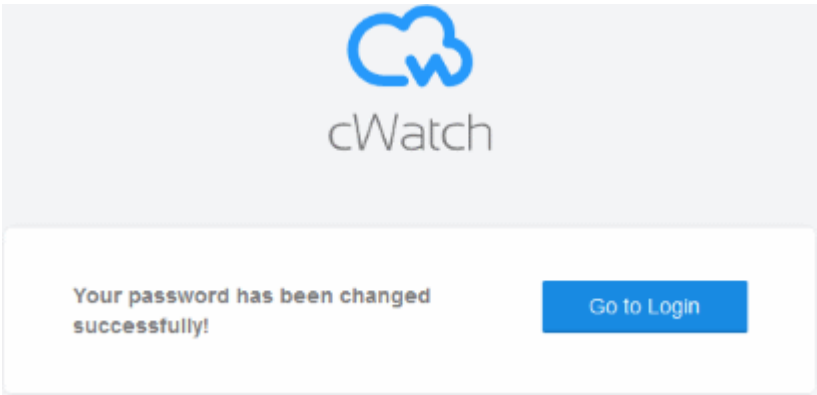
1255 Broad Street STE 100
Clifton, NJ 07013
United States

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:



- Click 'Create Password'



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

1.4 Add Websites

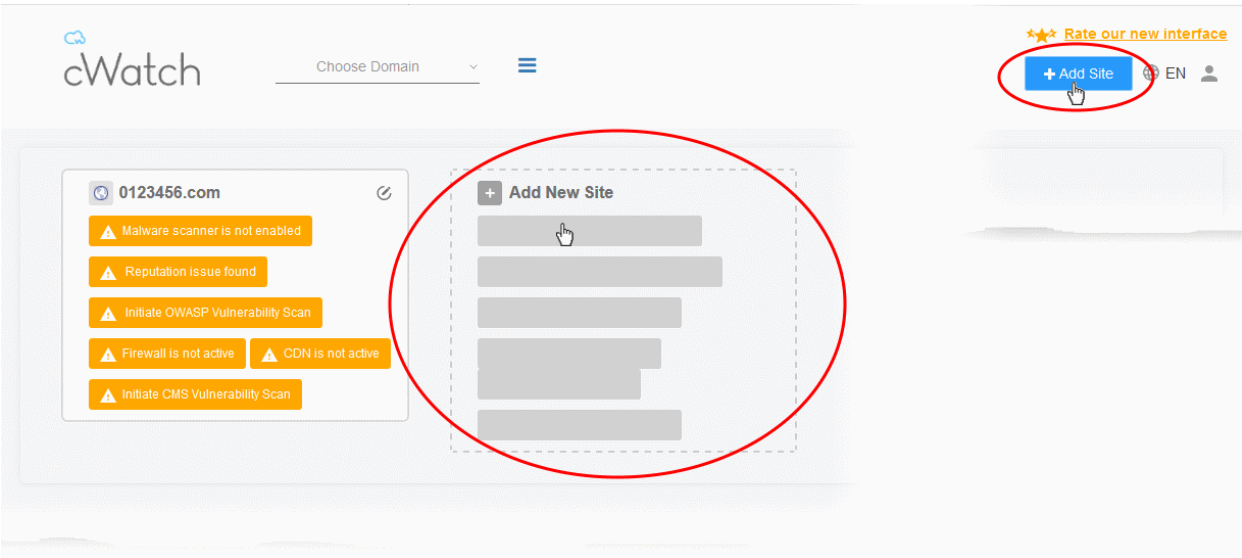
- You need to add websites to cWatch to enable protection and to take advantage of the content delivery network (CDN).
- The number of sites you can add depends on your license. See **Purchase a License** for details about license types.
- Once added, you can configure threat monitoring and CDN settings for each site.

Add a new domain

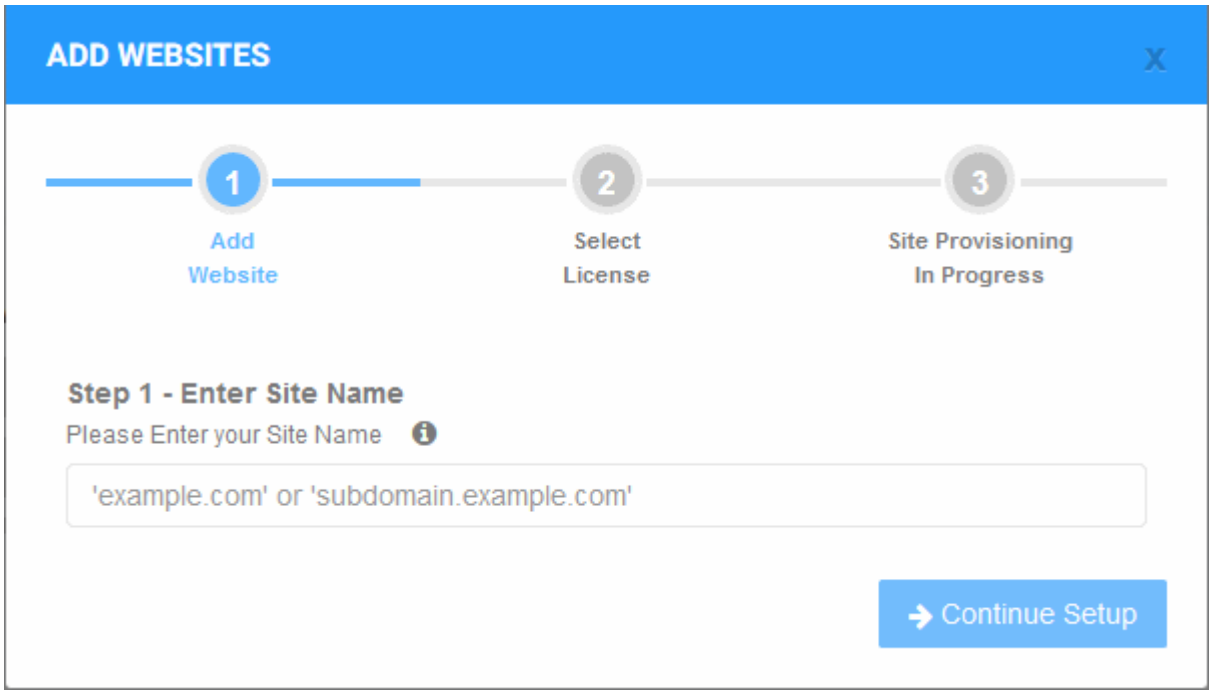
- Login to cWatch at **https://login.cwatch.comodo.com/login** with your username and password.

The dashboard appears and shows enrolled websites as tiles.

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



The 'Add Websites' wizard starts:

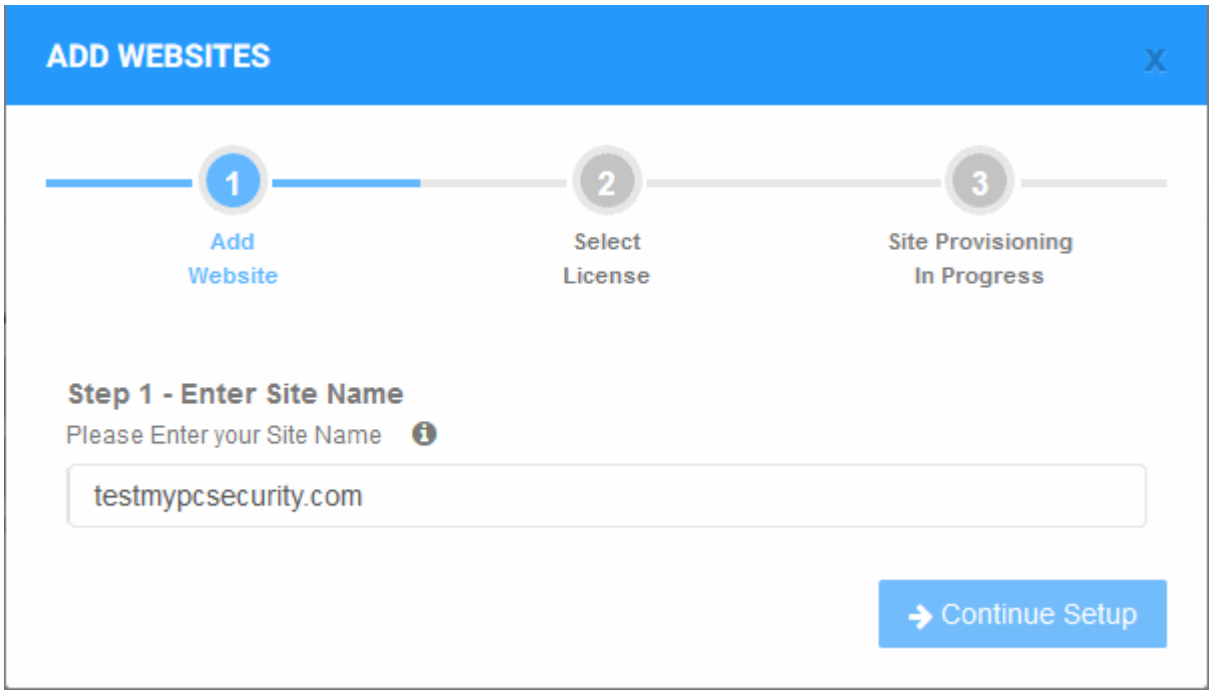


The wizard has three steps:

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

Step 1 - Register your website

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

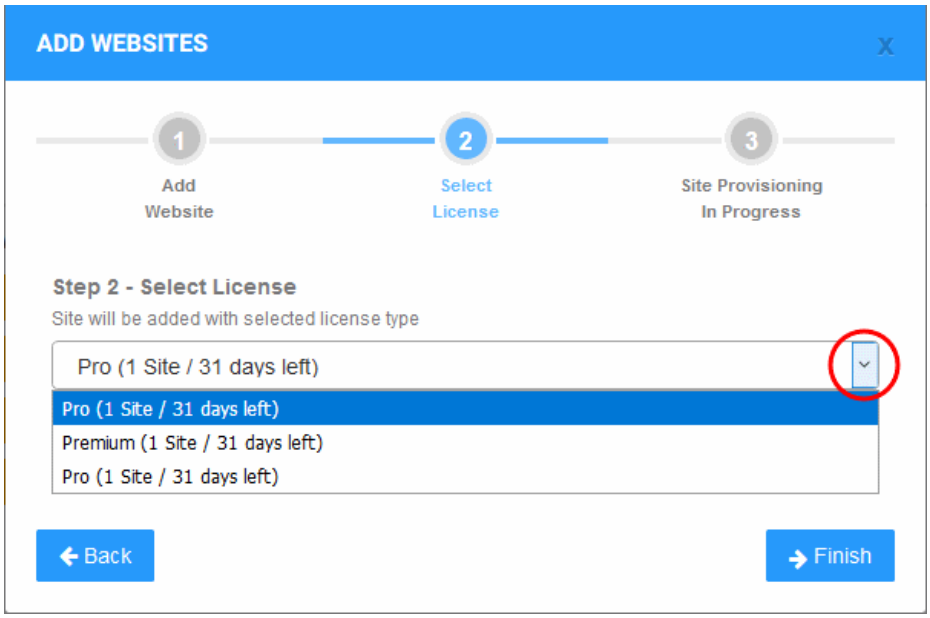


- Click 'Continue Setup' to move to the next step.

Step 2 - Select License

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

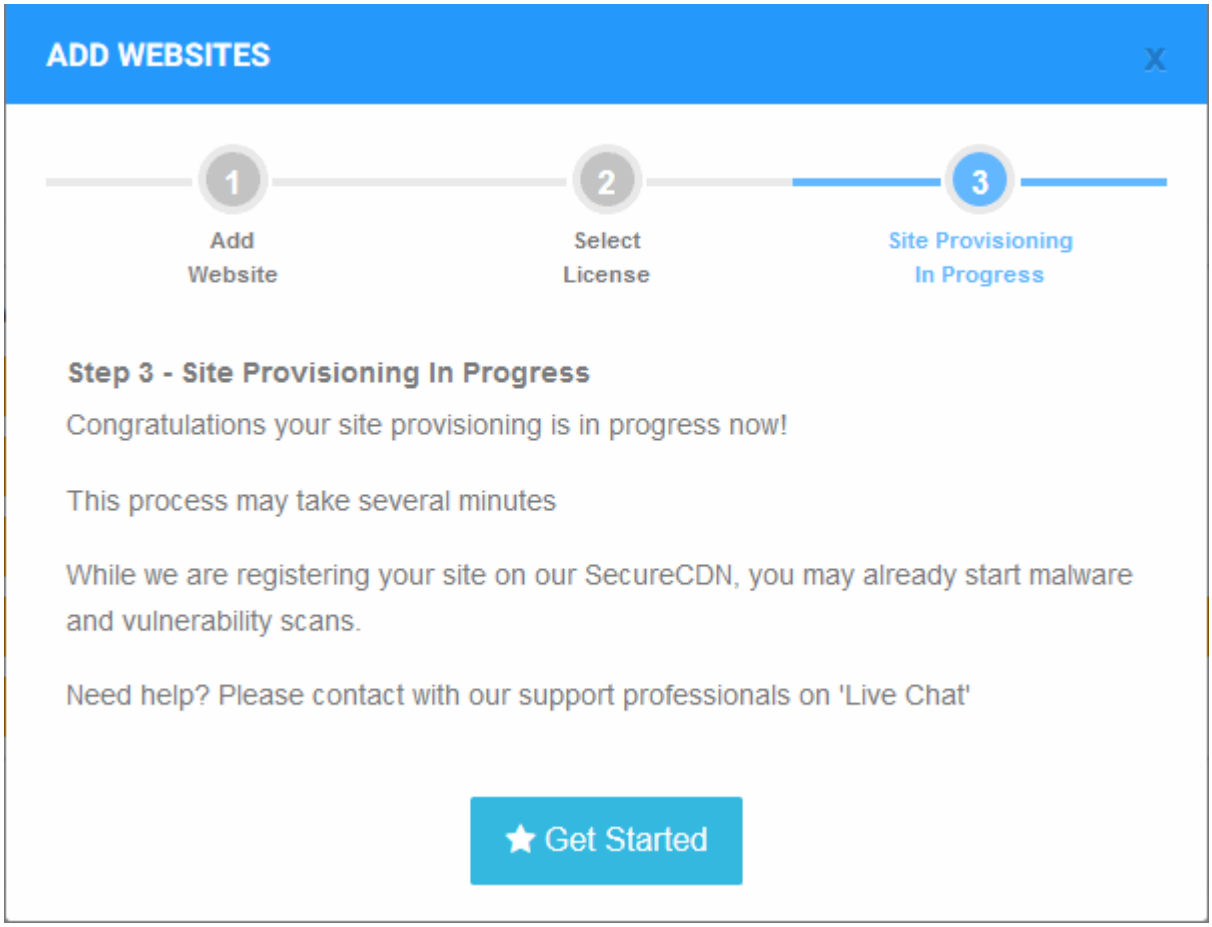
- cWatch features vary according to license type. See **License Types** for more details.
- The drop-down menu lets you select from all licenses you have purchased.
- Choose the type of license you wish to associate with the domain:



- 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:

- 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**.

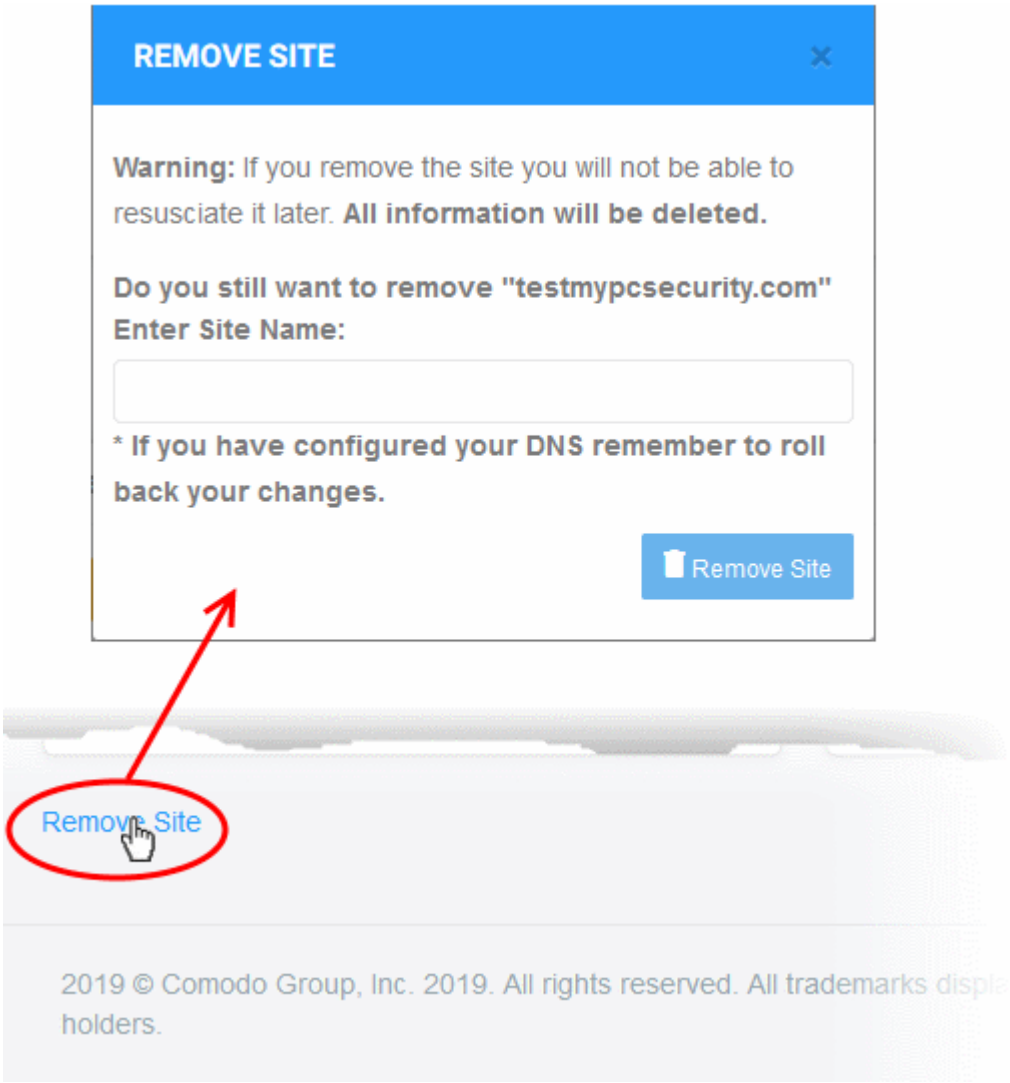
Tip: You can skip this step for now and add the CNAME to DNS later. See **DNS Configuration** for help with this.

- 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:

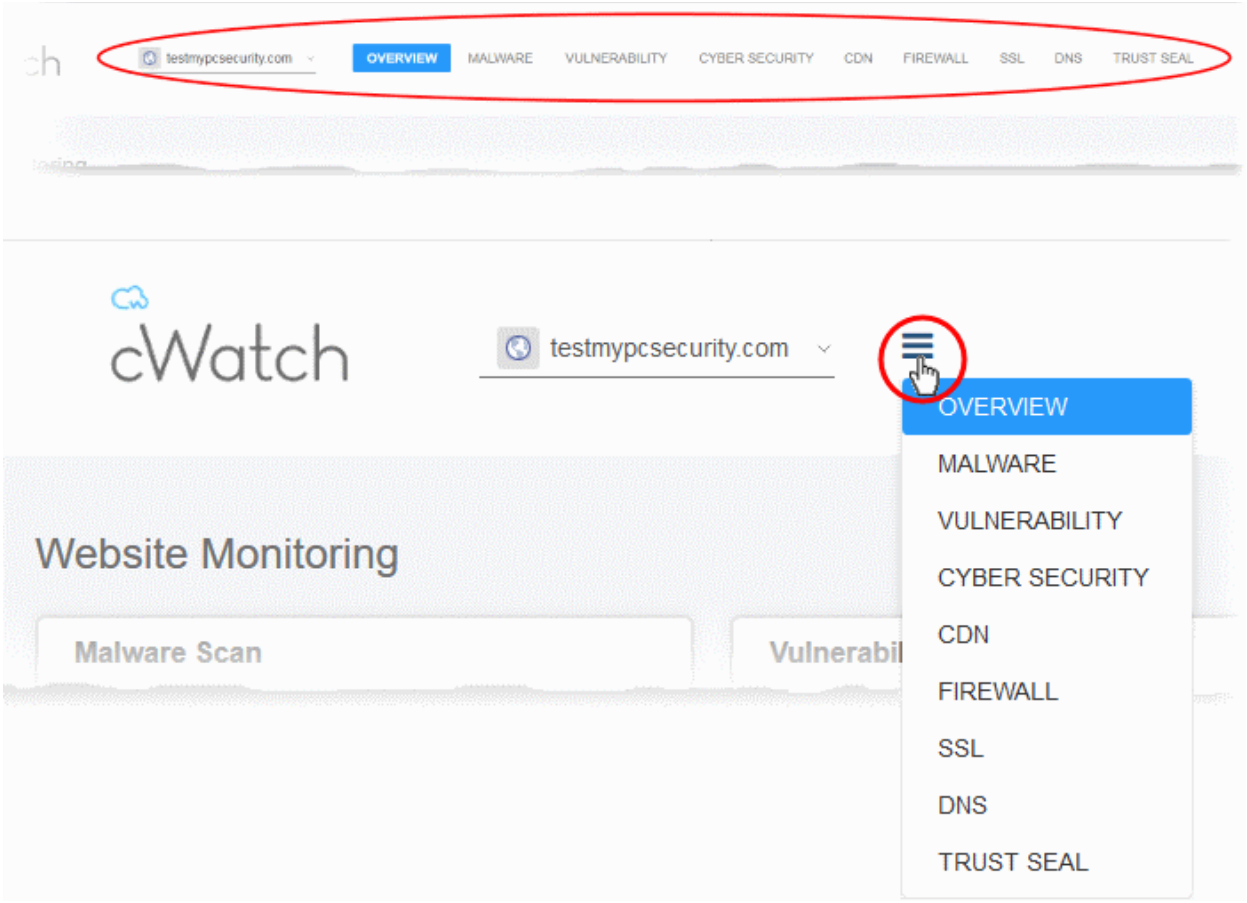
- Removing a website will delete all its data from cWatch. The site's traffic will no longer be routed through

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



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

    The scanner supports the following types of CMS:
    - WordPress
    - Joomla

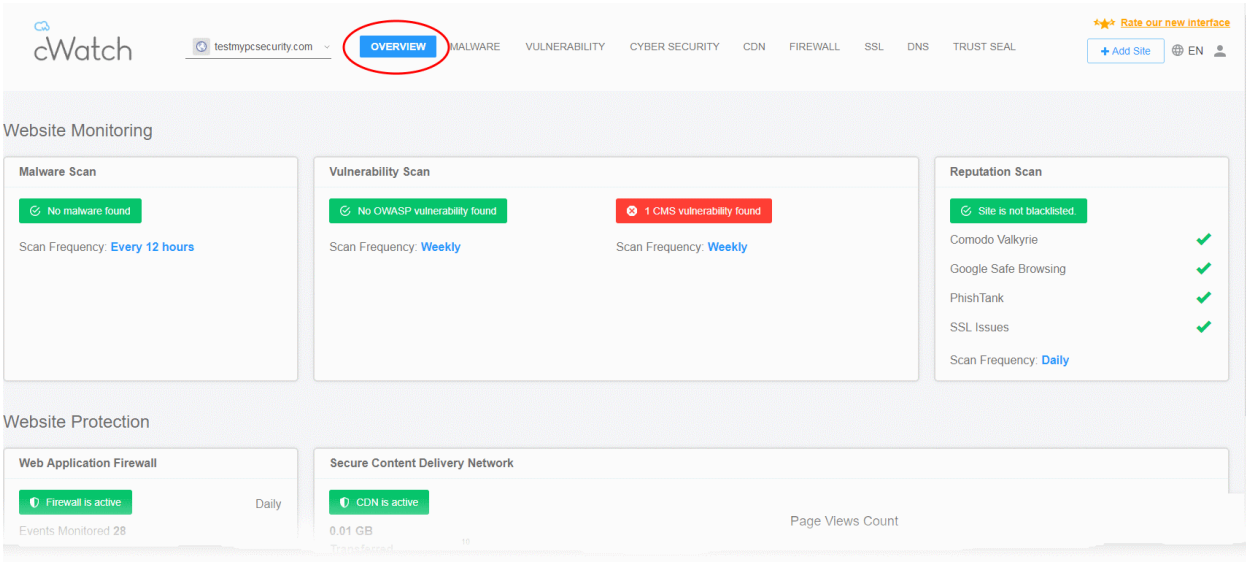
- Drupal
- ModX
- Typo3

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

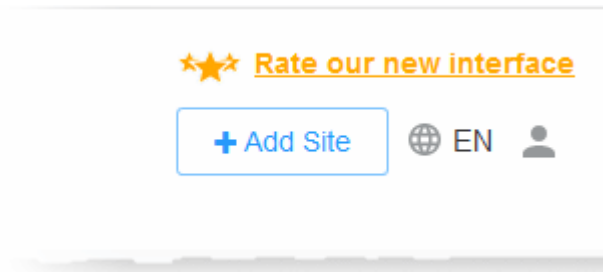
- **OWASP top-ten threats** - Scan your site for OWASP vulnerabilities and view results. You can also enable or disable automatic weekly scans.

See **Comodo Vulnerability Scans** for more details.

- **Cyber Security** - Real-time analysis of attack patterns on your website from the Comodo Security Operations Center. See **Cyber Security Operation Center Results** for more details.
- **CDN** - Activate and configure CDN services and view details about your content delivery network traffic. This includes total usage, data throughput and the locations from which your traffic originated. See **Content Delivery Network Metrics** to find out more.
- **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 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.
    - The main display shows data for the selected item.



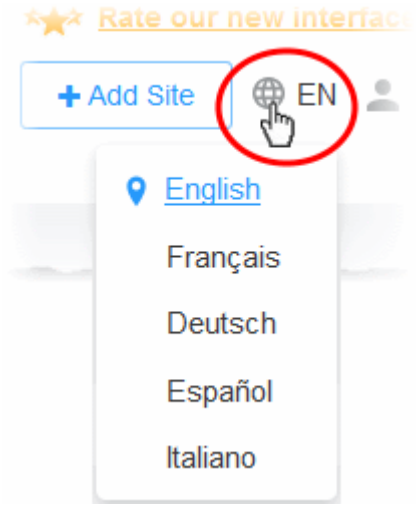
- The options on the top right let you to add a new website, select your language, manage your profile, view your subscriptions and logout:



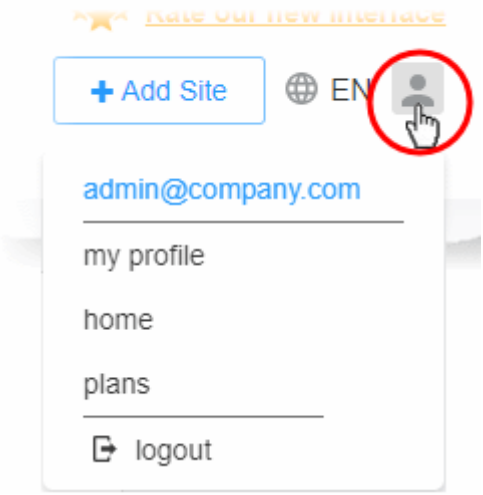
+ Add Site - Starts the site enrollment wizard. See **Add Websites** for more details.

EN - The current interface language.

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



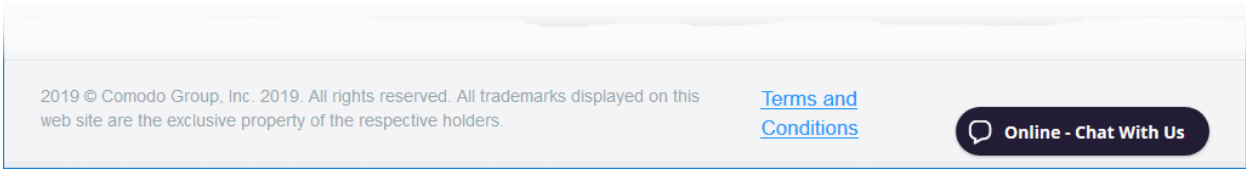
- Click to manage your profile and view your subscriptions.



- **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:

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



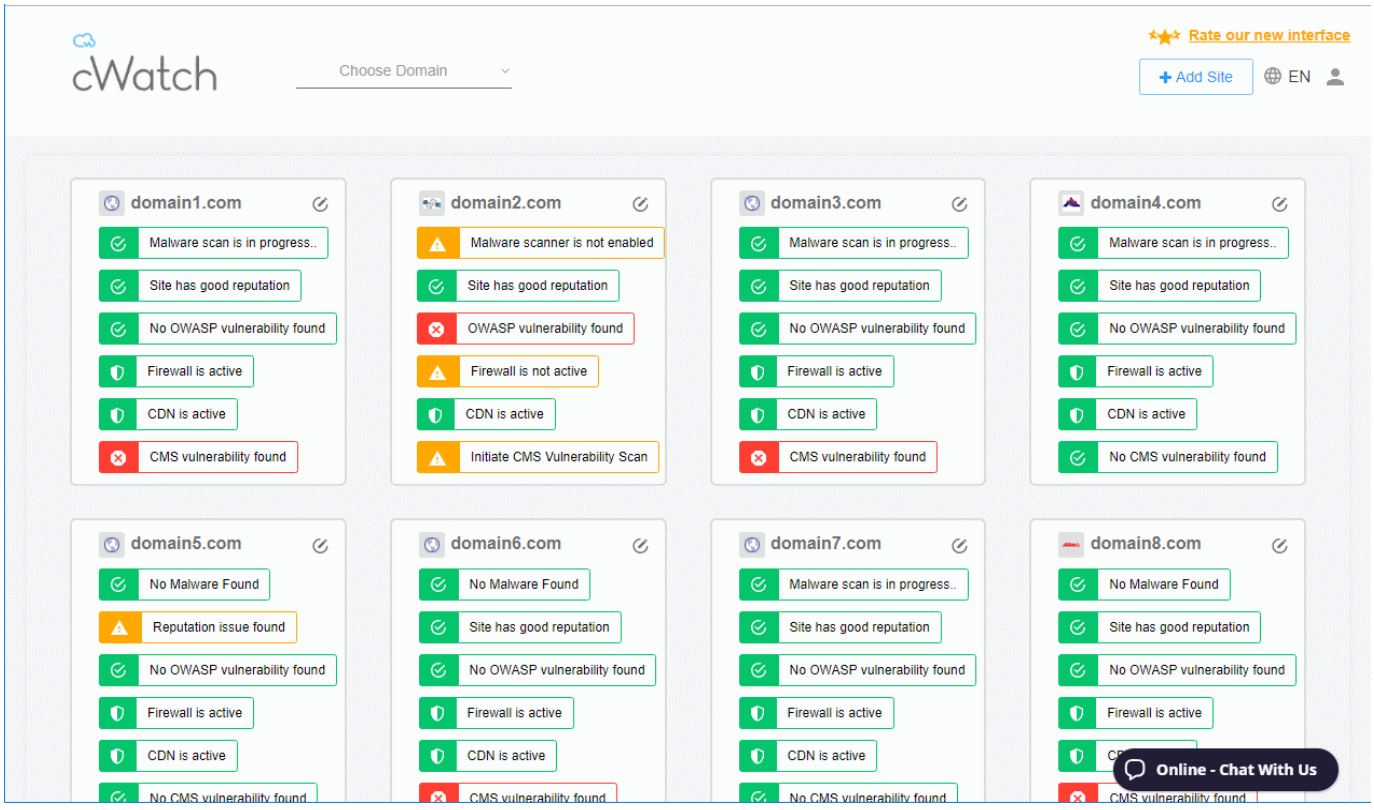
- Click the 'Terms and Conditions' link to view the cWatch EULA.
- Click the 'Chat with us' button for instant support from technicians at Comodo. See **Get Support** for more details.

3 The Dashboard

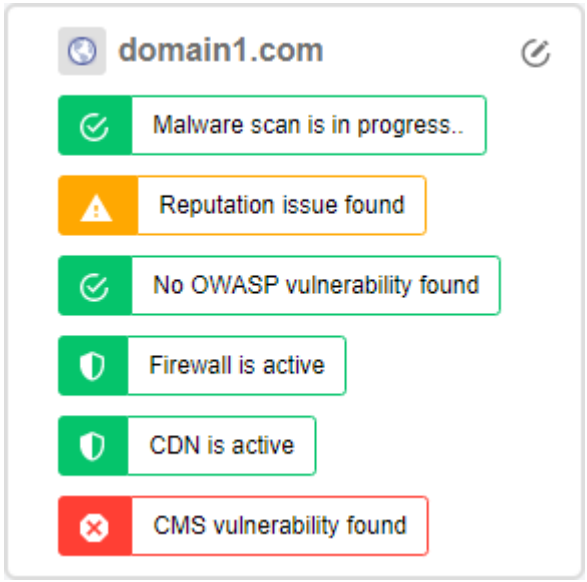
- Click the cWatch logo at the top left

The dashboard shows a top-level security summary of all sites on your account. This allows you to quickly identify issues and effectively track the risks associated with your sites.

- Click the cWatch logo at the top left to open the dashboard



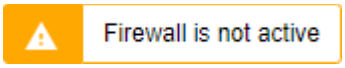
- Each site on your account is shown as a separate tile.
- The rows on each tile tell you the security status of cWatch component:

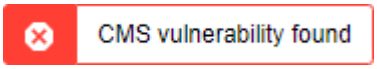


- Green - No threats found in the category
- Yellow - Requires action. For example, activate the firewall or run a malware scan.
- Red - Threats found in this category

- Click the 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:

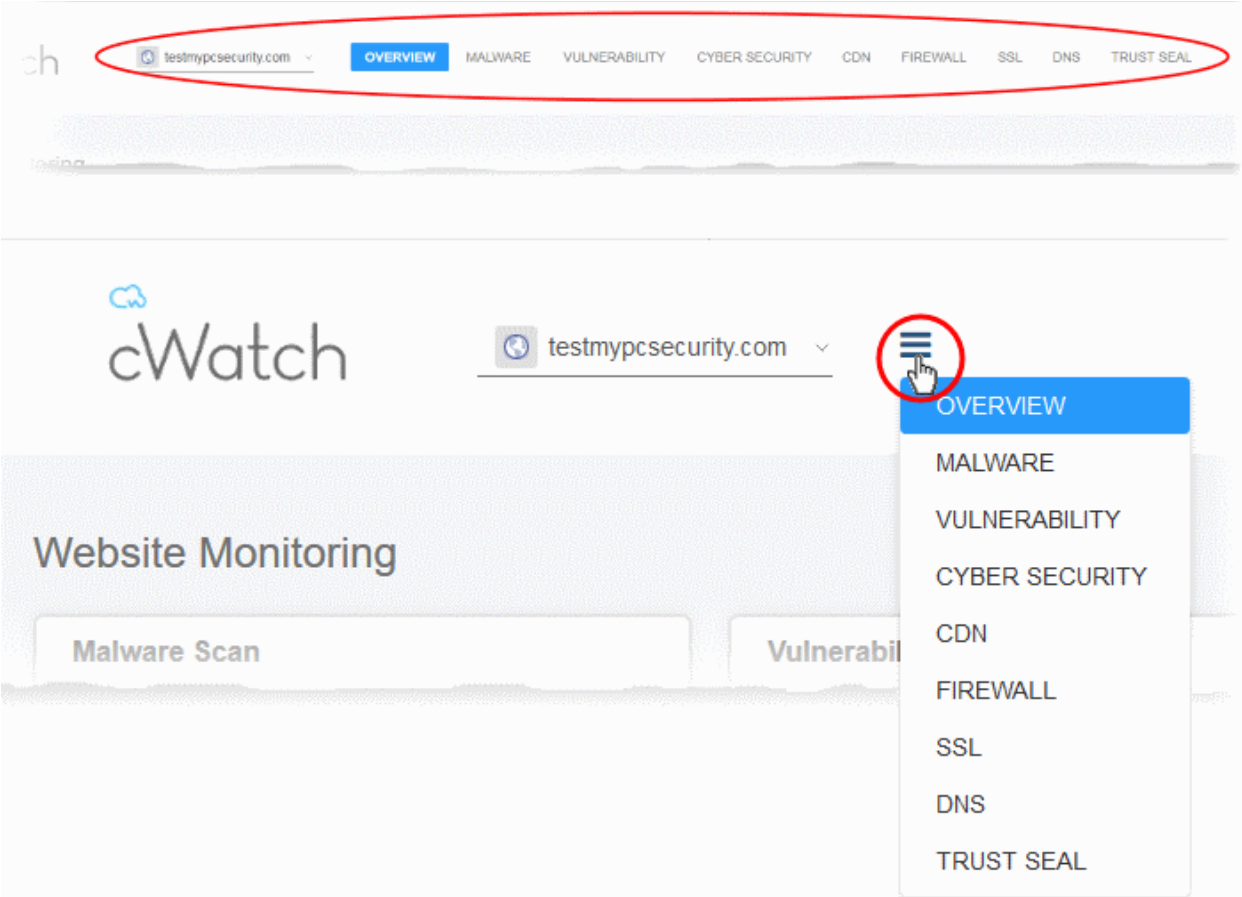
- 

- Opens the web application firewall settings page. See **Configure WAF Policies**.
- 

- 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.
- **Malware** - Activate the malware scanner, run virus scans, view scan results and monitor malware cleanup progress. You need to upload our .php file to the server in order to enable malware scans. See the **Malware Scans** section for more details.
- **Vulnerabilities**:
    - **CMS vulnerability scans** - Identify weaknesses in your content management system (CMS). You can also enable or disable automatic weekly scans.

      The scanner supports the following types of CMS:
        - WordPress
        - Joomla
        - Drupal
        - ModX
        - Typo3

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

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

See **Comodo Vulnerability Scans** for more details.

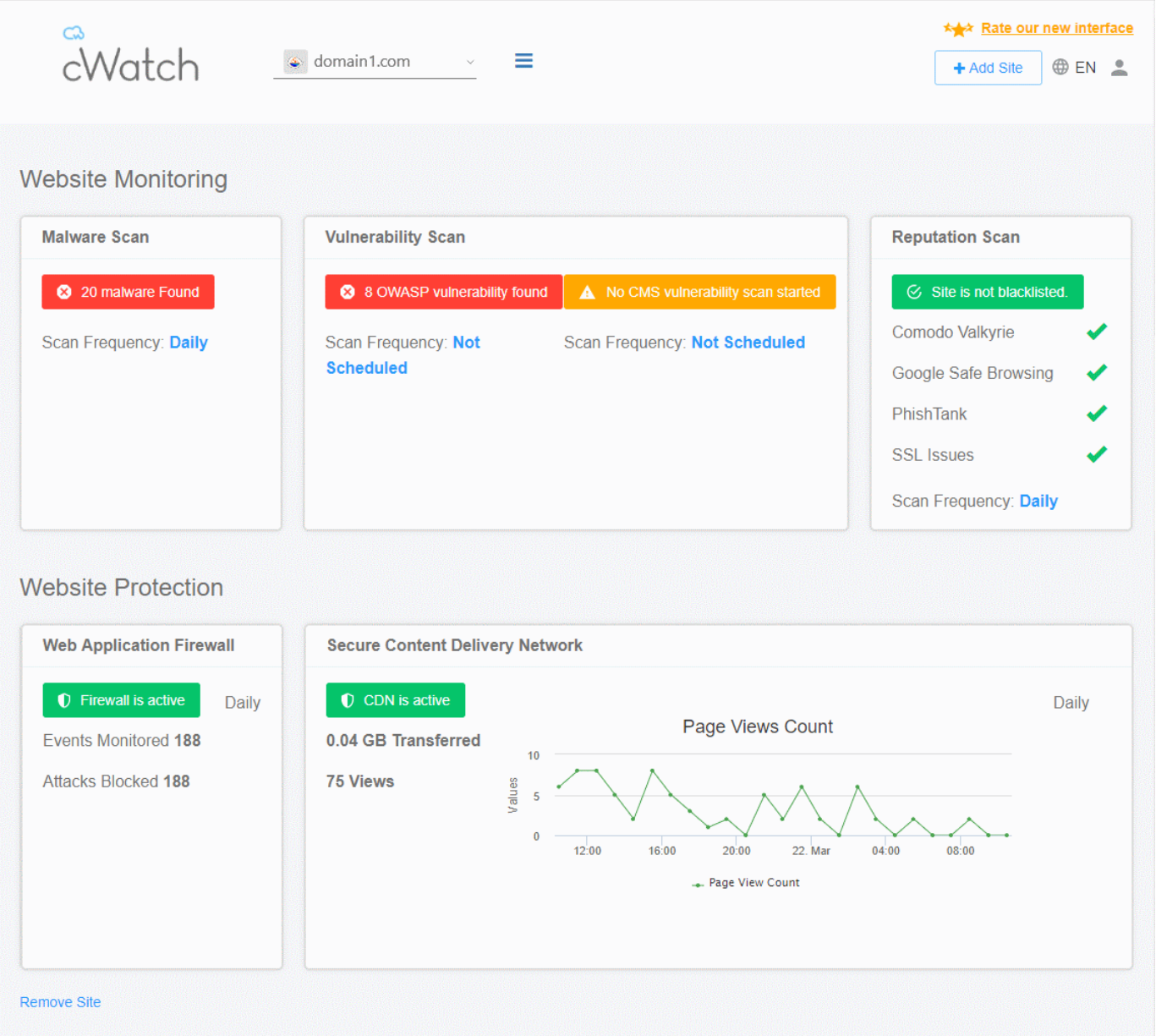
- **Cyber Security** - Real-time analysis of attack patterns on your website from the Comodo Security Operations Center. See **Cyber Security Operation Center Results** for more details.
- **CDN** - Activate and configure the Content Delivery Network (CDN), and view details about your CDN traffic. This includes total usage, data throughput, and the locations from which your traffic originated. See **Content Delivery Network Metrics** to find out more.
- **Firewall** - 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, or 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.

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 a range of important security information from various cWatch modules.
- The tiles also contain shortcuts to more detailed results and threat remediation advice.
- You can also remove a site from cWatch from its overview page.

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

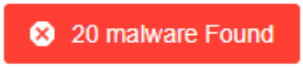
- Shows key information from cWatch scans. This includes malware scan results, vulnerability scan results, and site reputation checks.

Malware Scan:

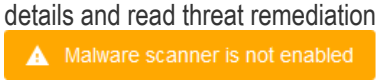
The result of the most recent manual or scheduled virus scan.

Scan Frequency - Scan timings.

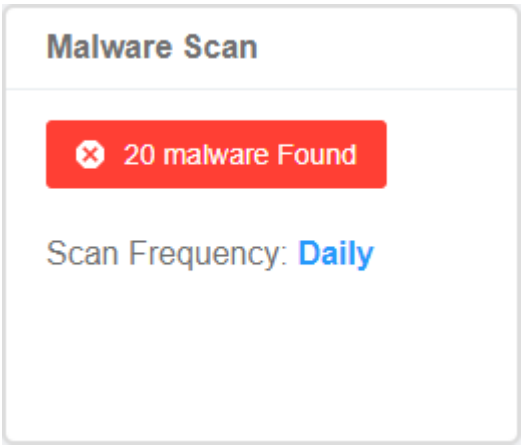
Note: You need to upload the cWatch agent to your site to enable malware scans.

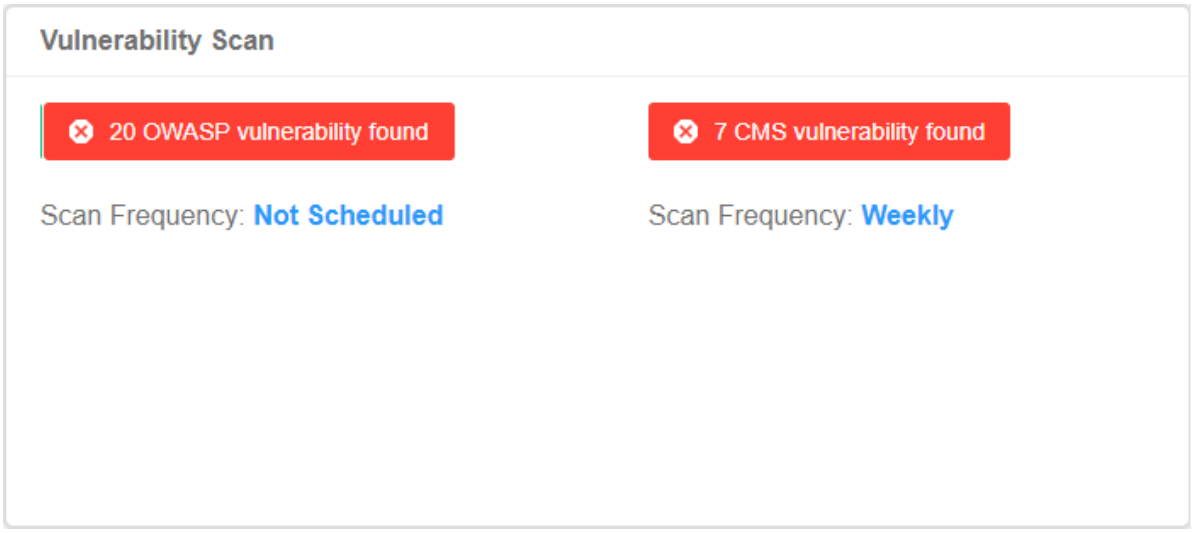


- Click the 'malware found' stripe to see full malware details and read threat remediation advice.



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





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).

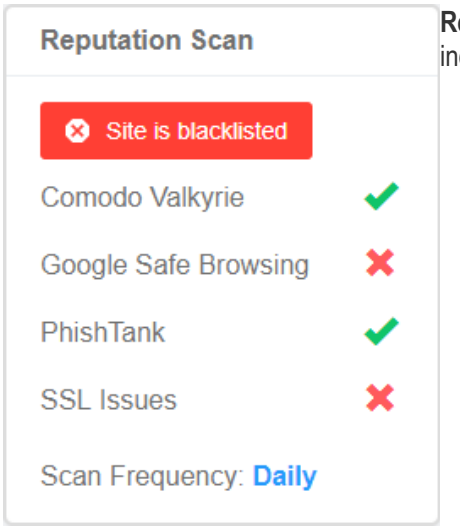
- The scanner supports the following types of CMS:
  - WordPress
  - Joomla

- 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.

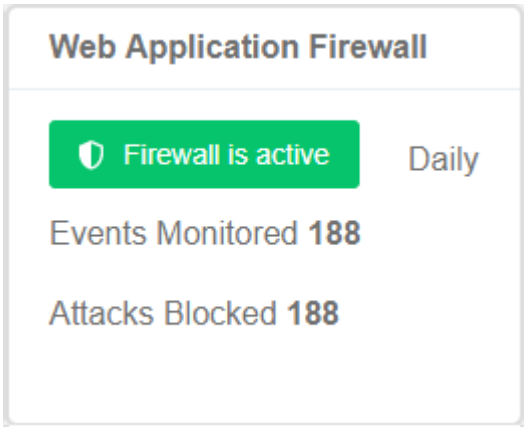


Reputation - The trustworthiness of the site according to key security indicators.

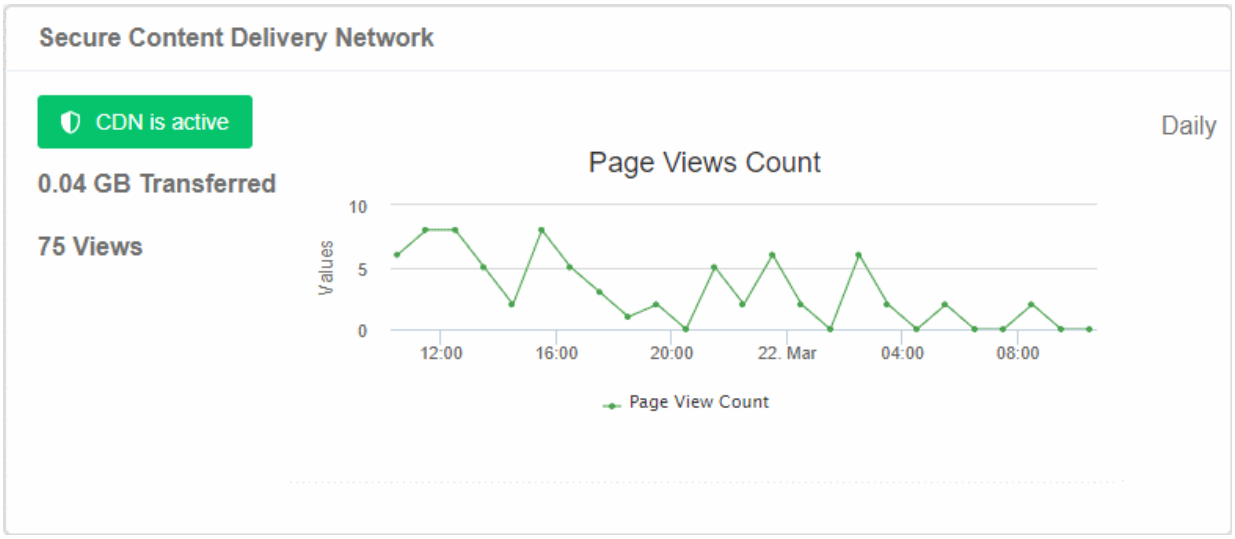
- **Comodo Valkyrie** - Comodo Valkyrie is a threat analysis platform that provides verdicts on the trust level of websites. A check-mark indicates that your site is not blacklisted by Valkyrie.
- **Google Safe Browsing** and **Phishtank** - These are long-established blacklists of dangerous websites. A check-mark indicates that your site is not on their blacklist.
- **SSL issues** - The site's TLS certificate is misconfigured, invalid, or uses out-dated protocols.

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 CDN is not active to start the configuration process.
- See **Content Delivery Network Metrics** for more details about CDN statistics.

4.2 Malware Scans

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

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

There are two ways to do this:

1. **Automatically** - Use the cWatch interface to upload the file to your site.
   - Click 'Malware' > 'Enable Scanner' to get started.
   - Choose 'Automatic' in the 'Enable Scanner' dialog and provide your web-server details.
   - See **Automatic configuration** for guidance on this.
2. **Manually** - Download the agent and copy it to your site. The agent is a .php file.
   - Click 'Malware' > 'Enable Scanner' to get started.
   - Choose 'Manual' in the 'Enable Scanner' dialog and download the .php file
   - Upload the file to a publicly accessible location on your site and enter the URL of the file
   - See **Manual Configuration** for guidance on this .

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

the 'Malware' page.

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

Open the 'Malware' interface

- Select the website from the menu at top-left of the dashboard
- Click the 'Malware' tab (or click the hamburger button and select "Malware')
- The 'Malware' page shows the last ten scheduled and manual scans on the site.
- Each row shows the number of malicious files found, and the time of the scan. See '**View malware scan results**' for more details.
- You will receive a notification email if malware is found by a scan.
- You can request Comodo technicians manually remove all threats from your site.

From this interface you can:

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

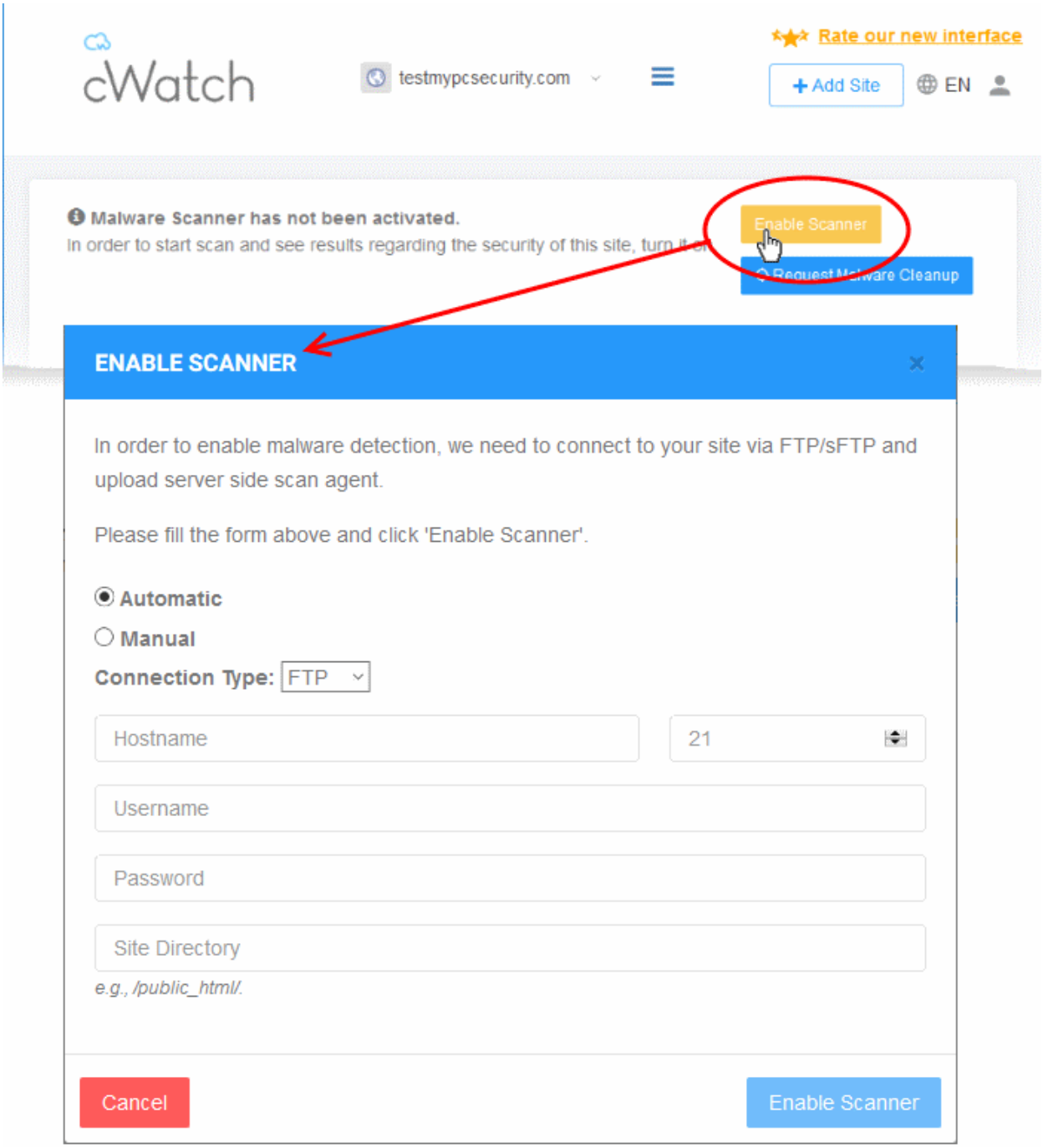
4.2.1 Configure Malware Scan Settings

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

Upload the scanner file

- Select the website from the menu at top-left of the dashboard

- Click the 'Malware' tab (or click the hamburger button and select "Malware")
- Click 'Enable Scanner'

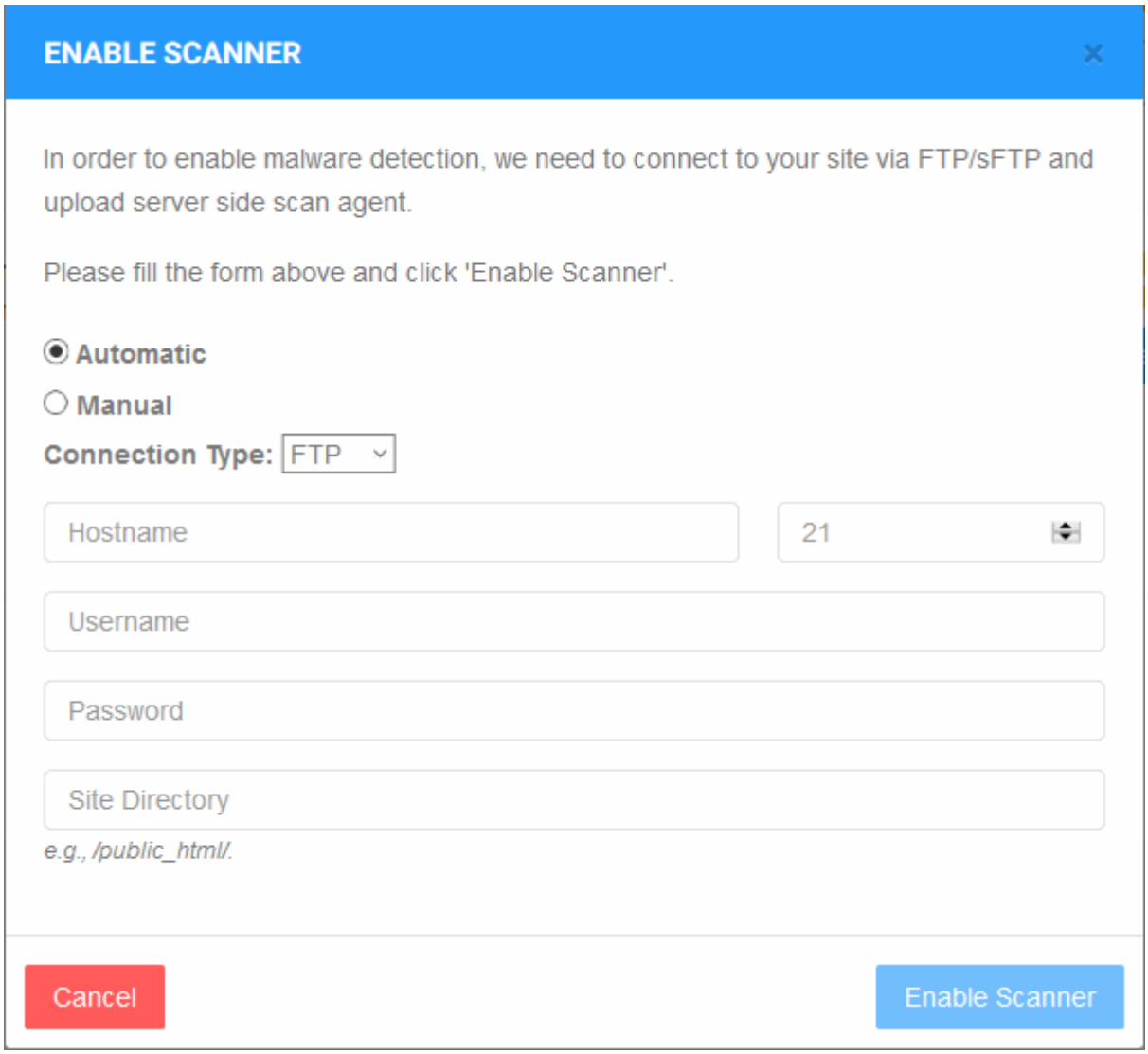


See the following sections for help with:

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

4.2.1.1 Automatic configuration

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



- Choose 'Automatic' and enter your website information

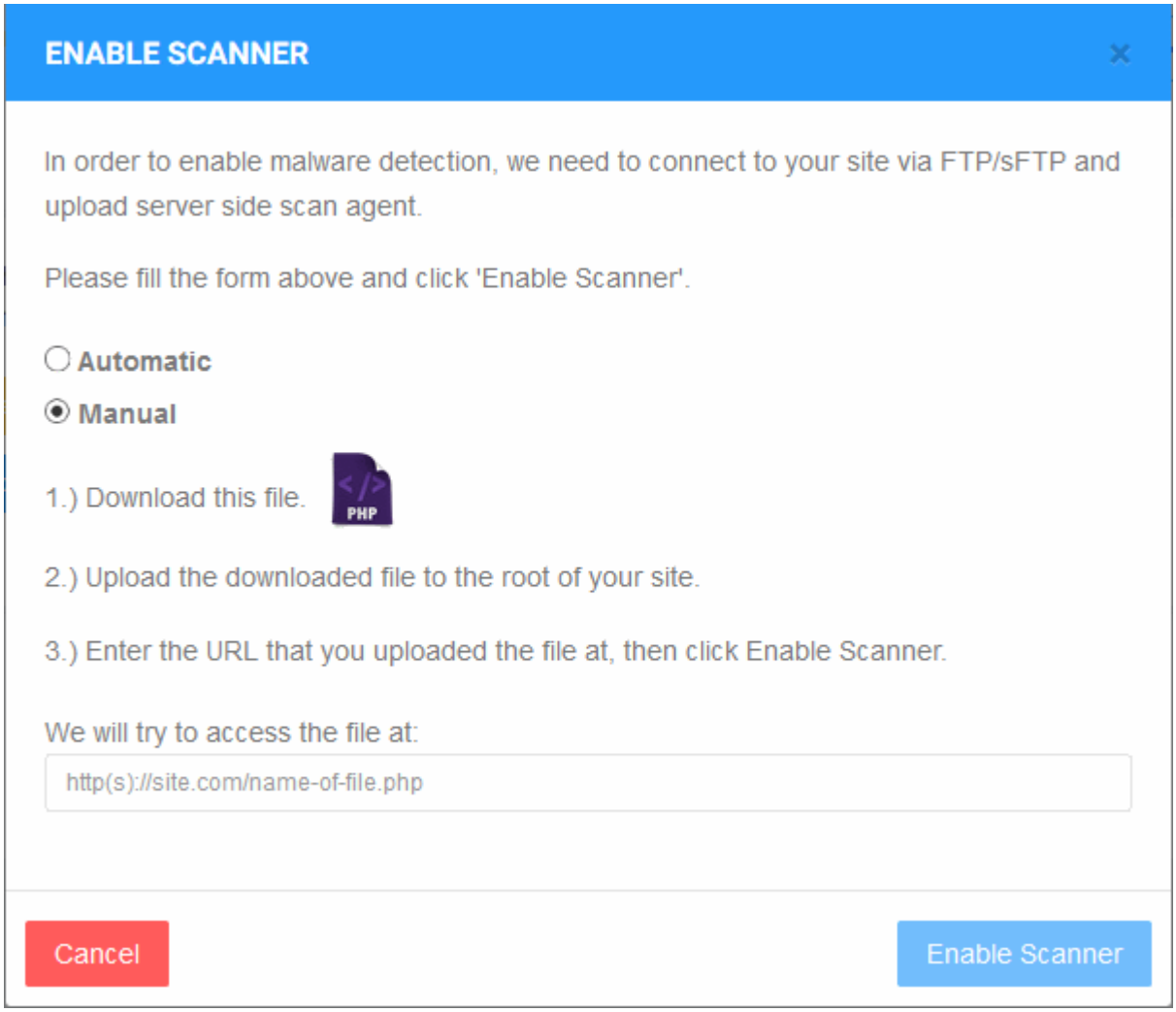
FTP / s/FTP Settings - Table of Parameters	
Parameter	**Description**
Hostname	IP or hostname of your web-server
Port	By default, FTP/sFTP connections use port 21. Change this setting if your web-server uses a different port for FTP/sFTP connections.
Username/ Password	Login credentials to your web-server.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

- Click 'Enable Scanner' to upload the file
- Note. Our technicians will also use these settings to access your site IF you request them to remove malware

4.2.1.2 Manual Configuration

- Open the cWatch dashboard
- Select the target website from the menu at top-left

- Click the 'Malware' tab (or click the hamburger button and select "Malware")
- Click 'Enable Scanner'
- Select 'Manual' in the 'Enable Scanner' dialog

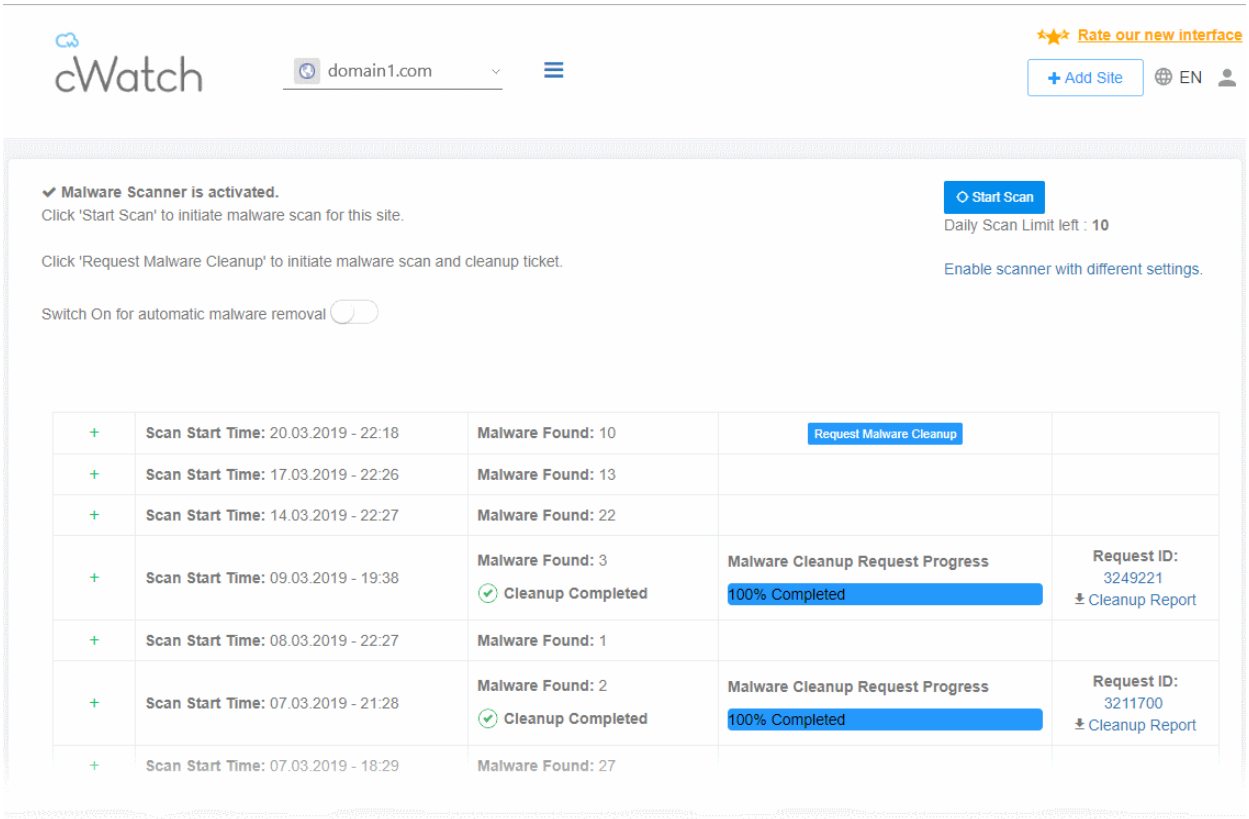


- Download the PHP file in step 1
- Upload the file to the root folder of your website. The file should be publicly accessible.
- Enter the URL of the uploaded file in the text field.
- Click 'Enable Scanner' to run the check.
- Automatic scans on your site will be enabled if the file-check is successful.

4.2.2 Run Malware Scans and View Results

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

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 malware page shows the last ten scheduled and manual scans on the site.

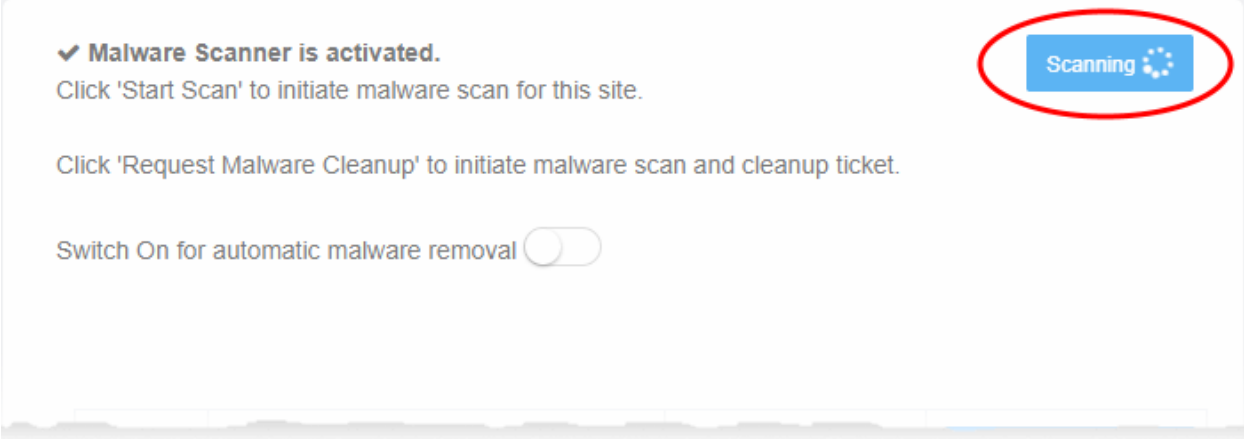
From this interface you can:

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

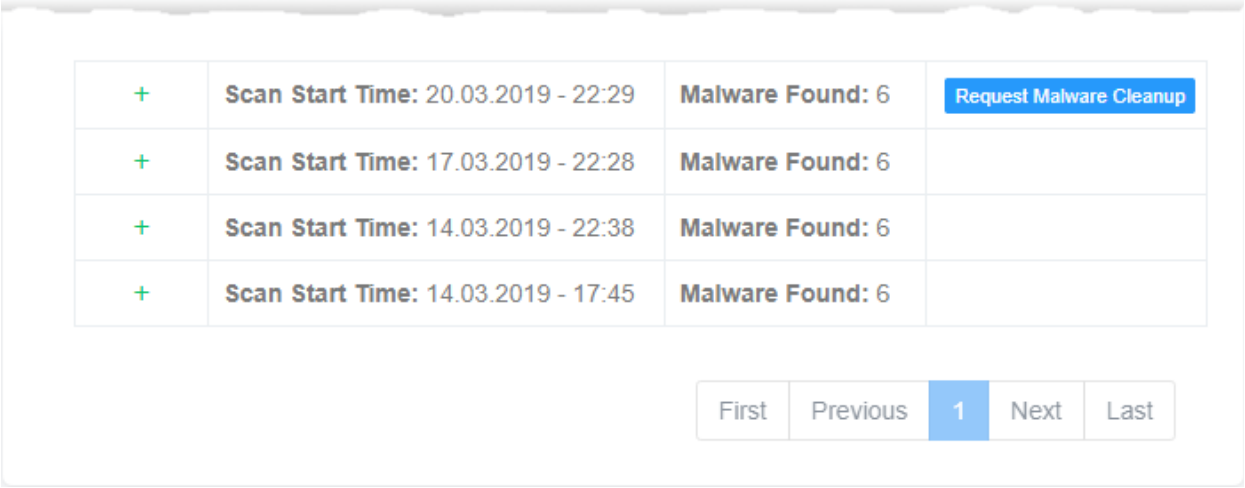
Start a manual scan

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

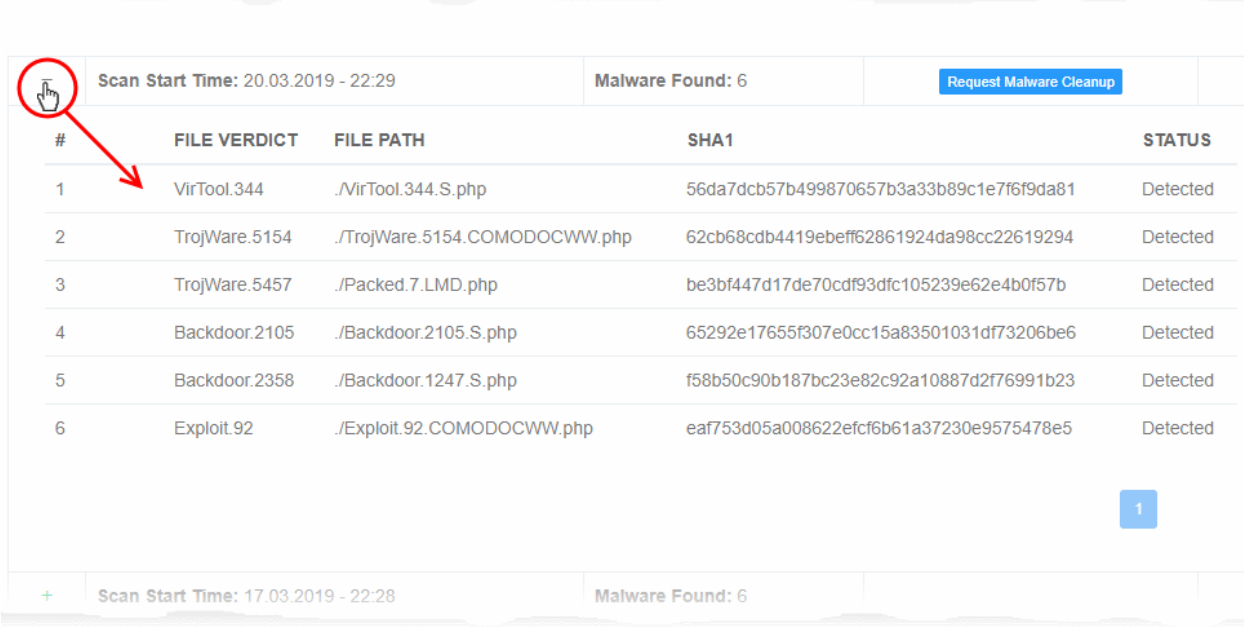
The scanning process starts:



The results are shown at the end of the scan:



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



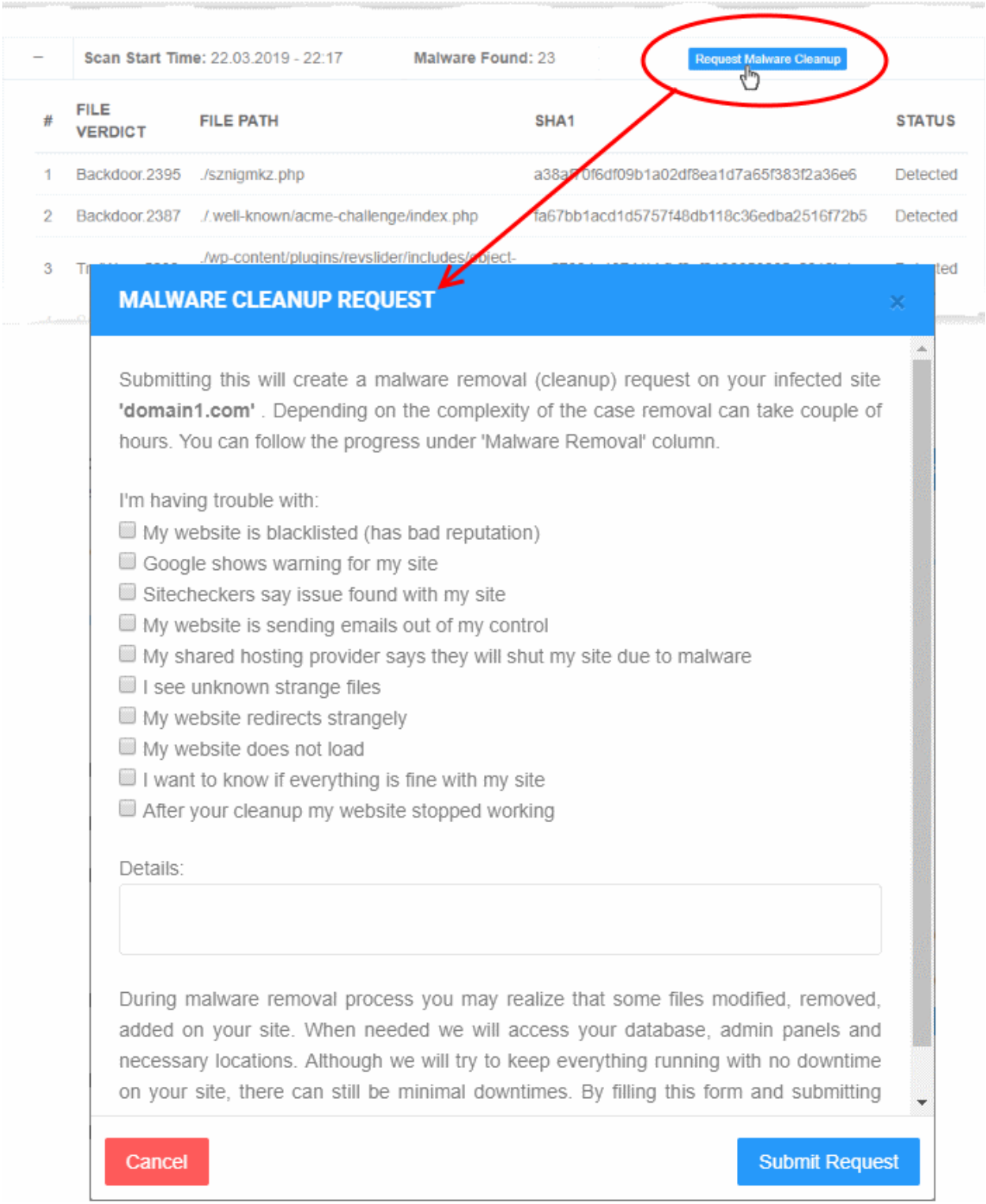
- Click 'Request Malware Cleanup' to instruct Comodo technicians to remove the malware. See the following section, **Submit a malware cleanup request**, for more on this.

Submit a malware cleanup request

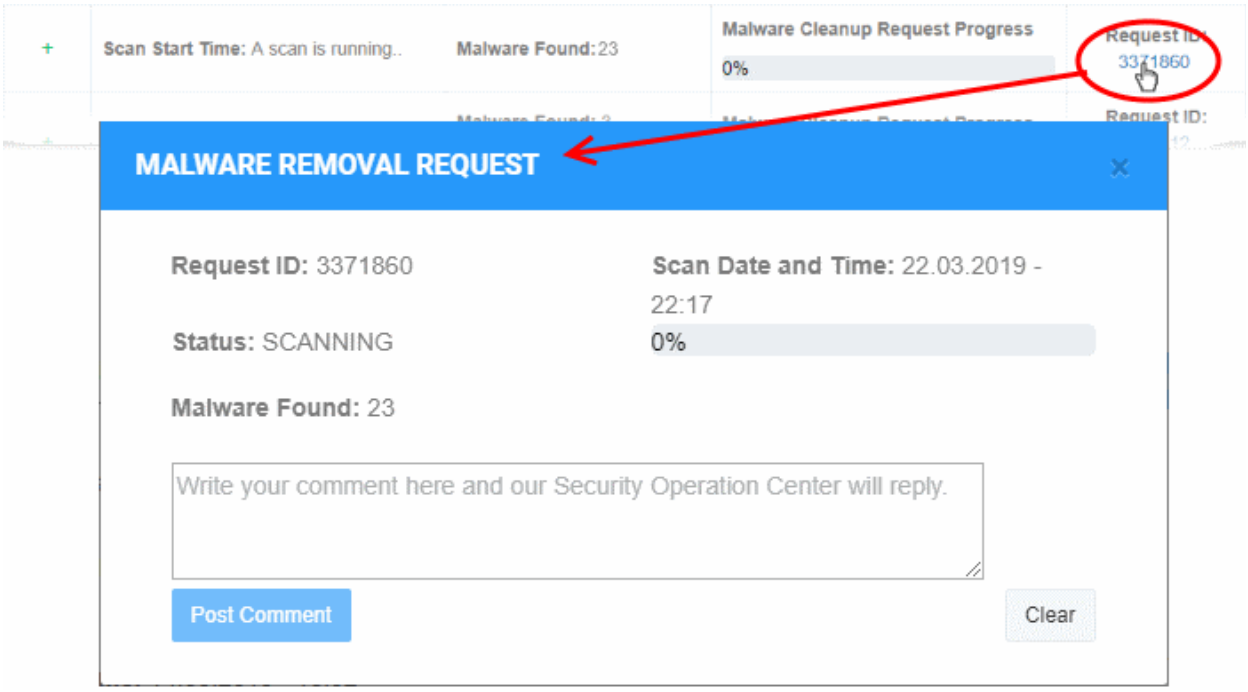
- You can request Comodo technicians professionally remove any malware found by a cWatch scan.
- The request form allows you to pick the exact issue, or issues, you would like us to deal with

Request malware removal

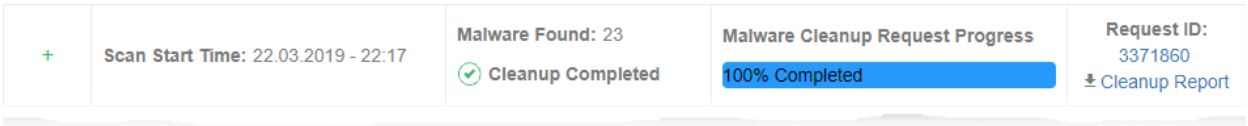
- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Malware' tab (or click the hamburger button and select "Malware')
- Click the 'Request Malware Cleanup' button in the row of a scan where malware was found:



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



You will see the following when the cleanup is complete:



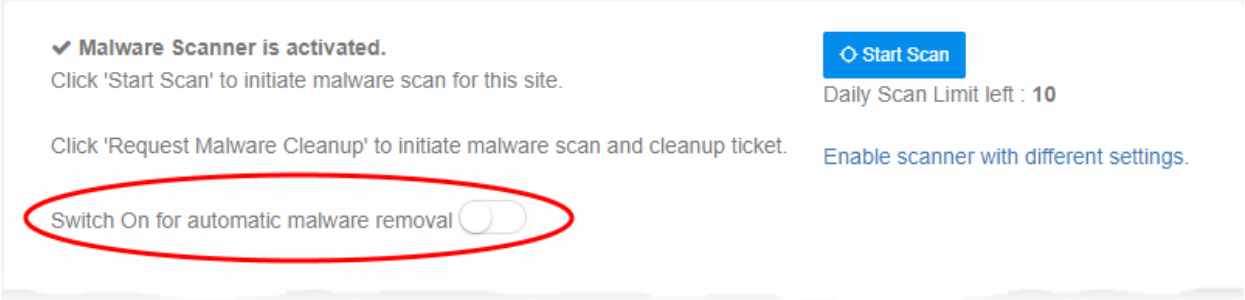
- Click 'Cleanup Report' to download a summary of the operation. The report itemizes each piece of malware removed.

Enable automatic malware removal

- You can configure a website for automatically generating malware removal request at the end of each scan in which malware is found.
- Automatic malware removal is enabled by default for 'Pro' and 'Premium' licenses. The scan and cleanup will automatically take place according to your schedule.
- Automatic malware removal is not covered by 'Basic' and 'Starter' license types. If you enable automatic malware removal, you will be prompted to upgrade your license for the website

Setup automatic malware removal

- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Malware' tab (or click the hamburger button and select "Malware')
- Select the switch beside 'Switch On for automatic malware removal'

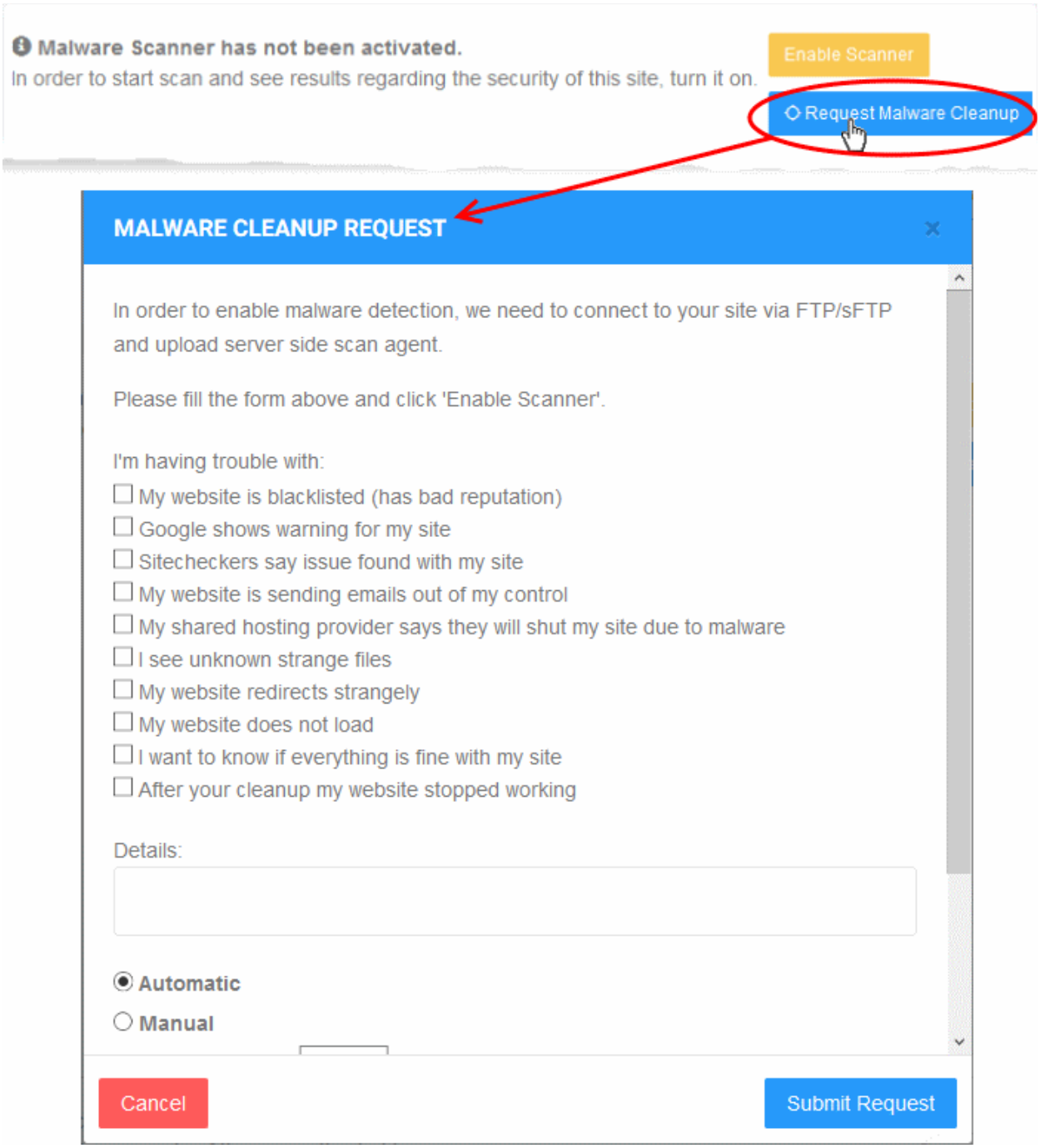


Start a manual scan and request a cleanup in a single step

- 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.

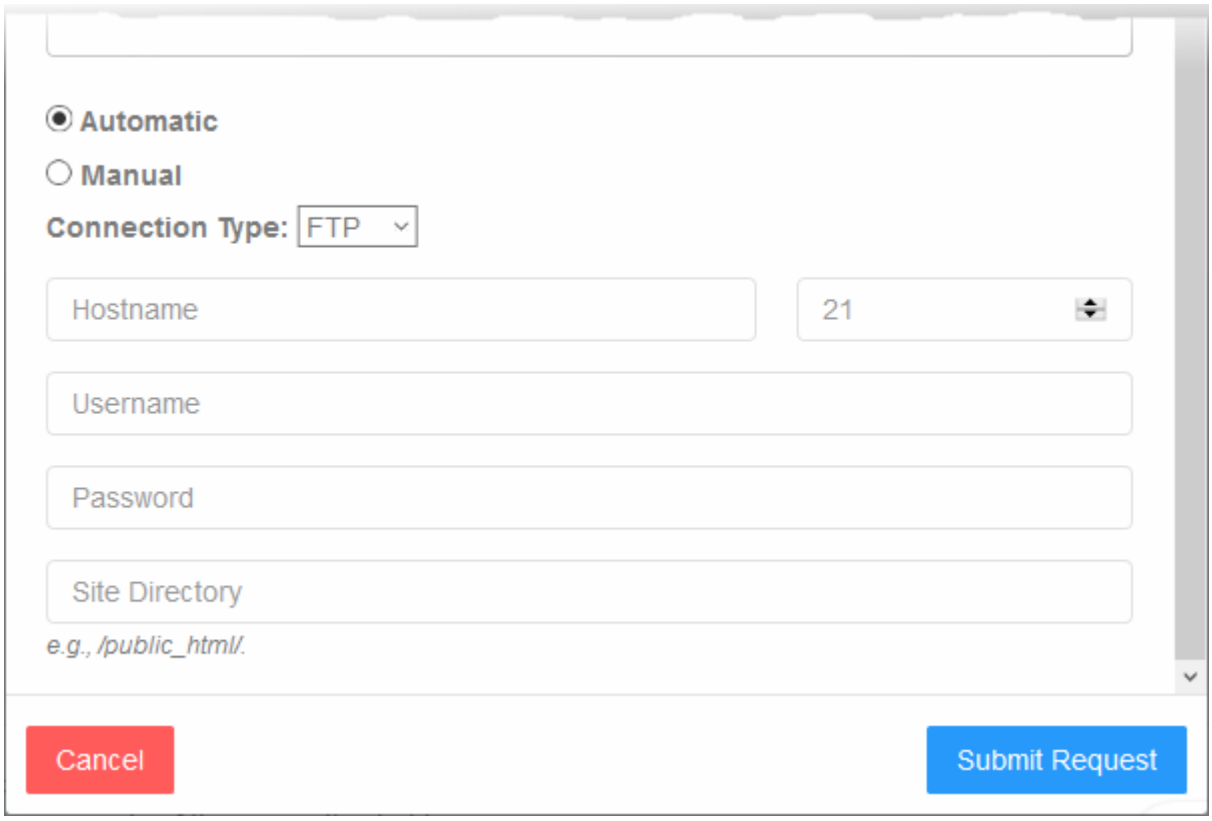
Start a scan and submit malware cleanup request

- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Malware' tab (or click the hamburger button and select "Malware')
- Click the 'Request Malware Cleanup' button on the top right



- 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 the website has not been already enabled for malware scanning you can configure the site by uploading scanner agent to the website. Note - The following options appear only for websites not pre-configured for

malware scans.



There are two ways you can configure malware scans on a site:

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

Automatic configuration

- Choose 'Automatic' in the request dialog.
  - cWatch will upload the file required to run the scan to your site
- Enter your website information

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

- Note. Our technicians will also use these settings to access your site IF you request them to remove malware
- Complete all details and click 'Submit Request'.

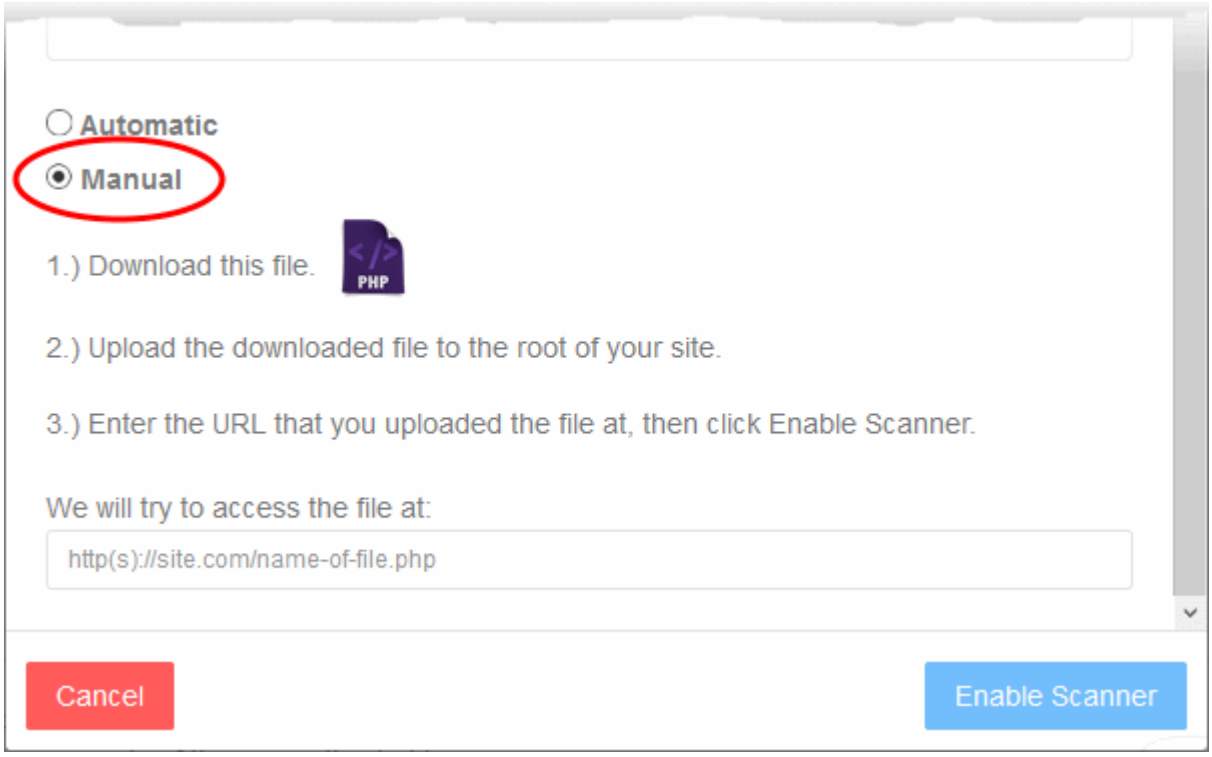
cWatch will upload the agent to your site and commence scanning.

- A cleanup request is created if the scan finds malware.

- Our technicians will access your site to remove malware and remediate any other issues you reported.
- Click 'Request ID' if you want to send a message to the technician while the cleaning is in progress.
- View the cleanup report after the completion of cleaning as described **above**.

Manual configuration

- Choose 'Manual' to download the agent and manually upload it to your site. The agent is a .php file.



- Download the PHP file in step 1
- Upload the file to the root folder of your website. The file should be publicly accessible.
- Enter the URL of the uploaded file in the text field.
- Click 'Enable Scanner' to run the check.

cWatch will try to access the file at the entered URL and commence scanning.

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

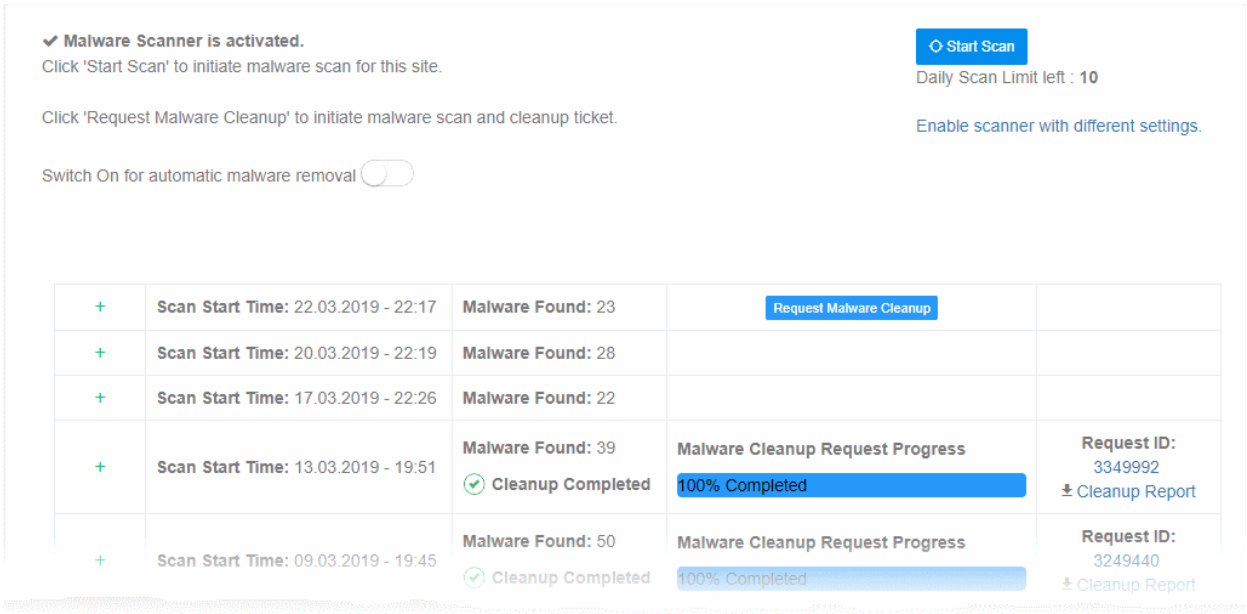
View malware scan results

- 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

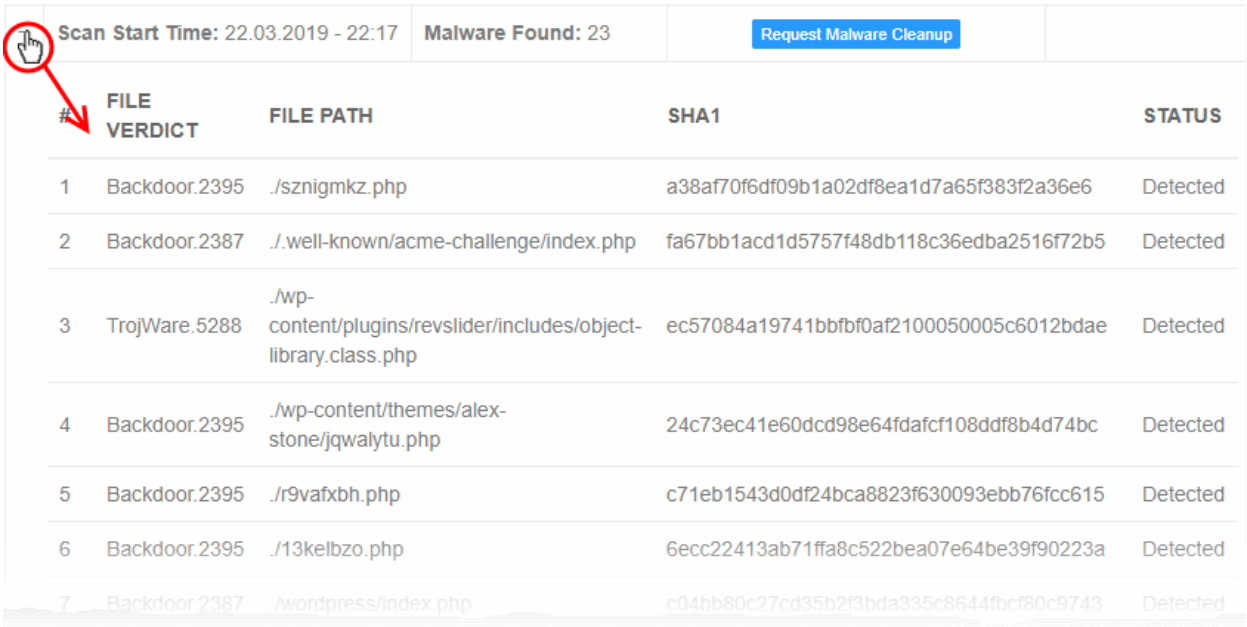
- Click the 'Malware' tab (or click the hamburger button and select "Malware")



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

View the list of malware identified by a scan

- Click the '+' symbol beside a scan row



Malware Scans - Column Descriptions	
Column Header	**Description**

File Verdict	The label of the malware
File Path	Location where the malware was detected on the website
SHA1	The Secure Hash Algorithm 1 (SHA1) hash value of the malware file
Status	Action taken on the malware file

4.3 Comodo Vulnerability Scans

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

CWatch can perform two types of vulnerability scans:

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

CMS Vulnerabilities

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

OWASP Top Ten Threats

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

- The 'OWASP Top 10 Scan' pane shows results from the last scan. 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**

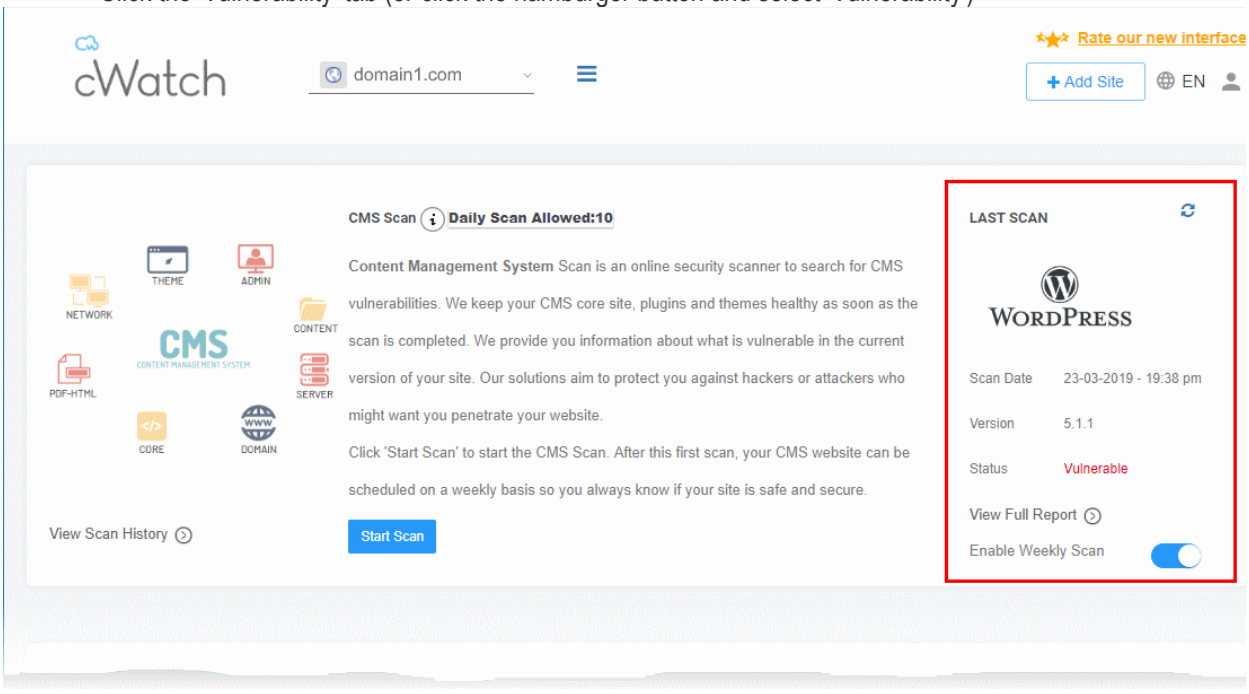
4.3.1 CMS Vulnerability Scans

- Select a website from the drop-down at top-left and choose '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 CMS scans on-demand and/or schedule weekly scans on your website. You can also view the results from the last ten scans.

Run CMS scans and view results

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Vulnerability' tab (or click the hamburger button and select '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 not found' - Shown if the site doesn't use a supported CMS, or because cWatch couldn't detect the CMS type for other reasons.

- Click the 'Refresh' icon on the top-right to reload the results of the latest scan.

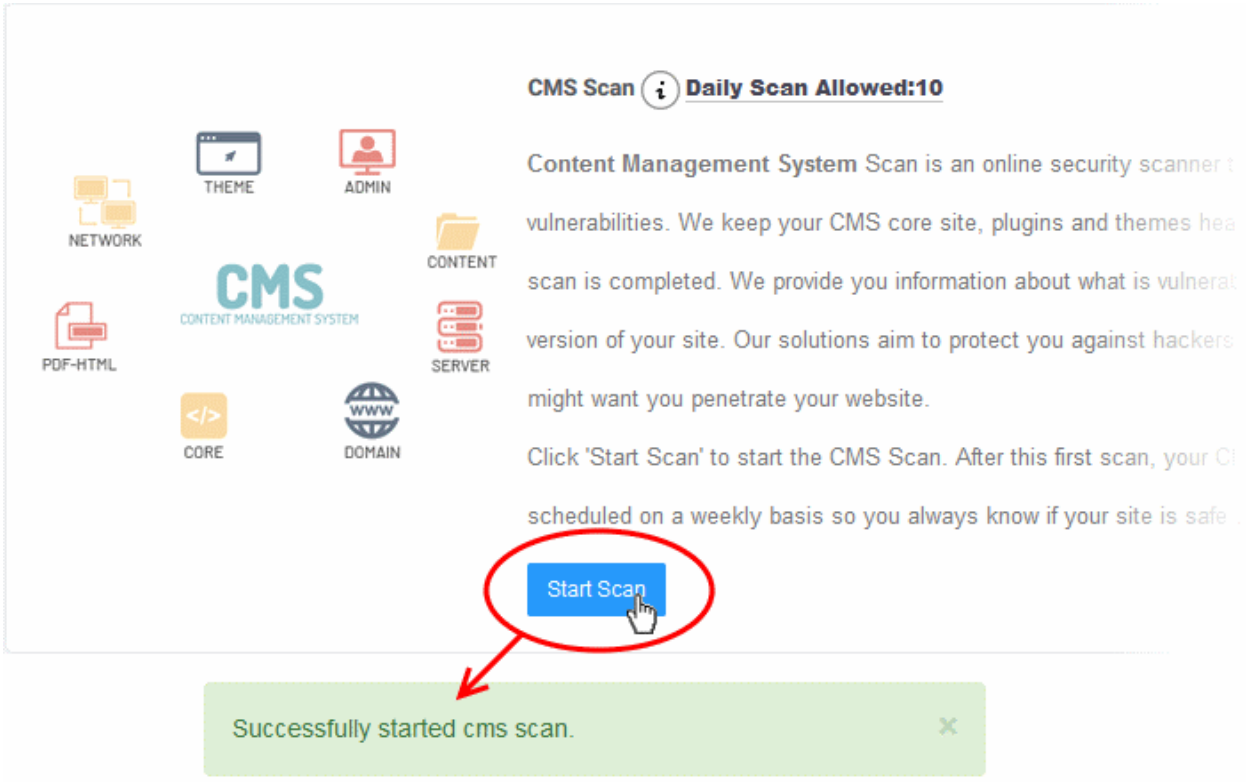
The pane lets you:

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

Start an on-demand CMS scan

You can manually start a CMS scan at anytime:

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Vulnerability' tab (or click the hamburger button and select 'Vulnerability')
- Click 'Start Scan' in the 'CMS Scan' pane:

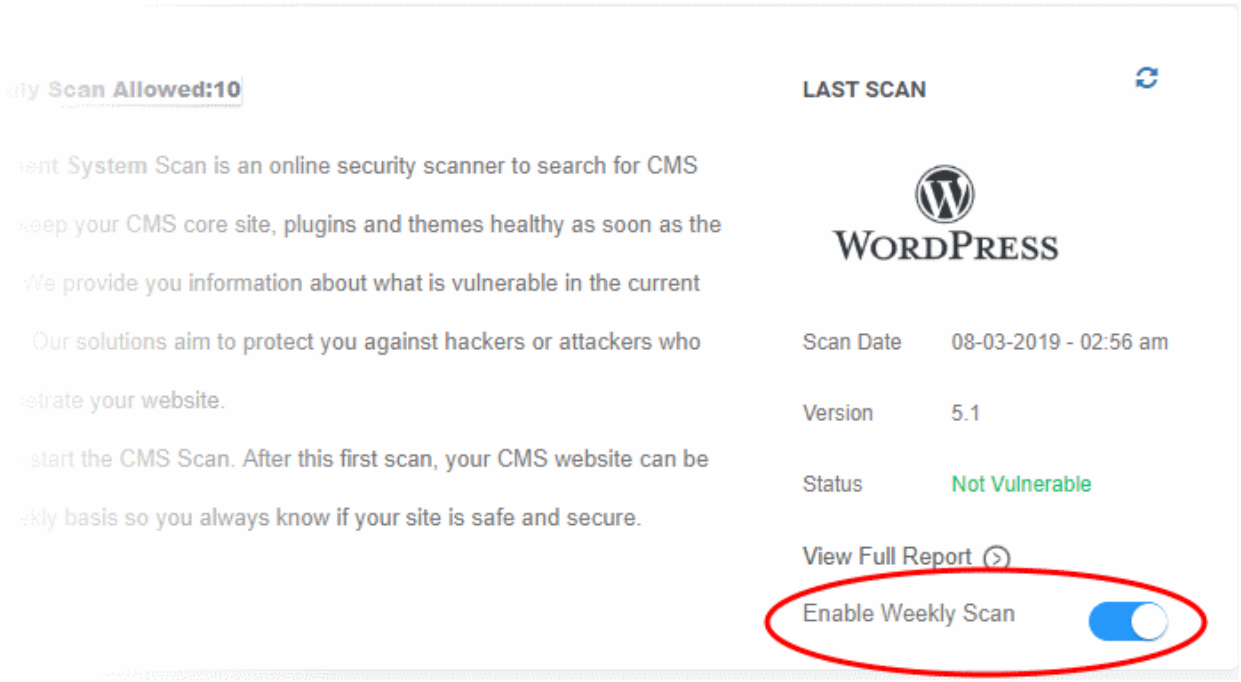


- cWatch will begin scanning the domain for CMS vulnerabilities.
- Scan results are shown in the 'Last Scan' box on the right
  - Click the 'Refresh' icon at top-right to reload the results of the scan
- Alerts will be generated if any vulnerabilities are found.
- Click 'View Full Report' for a comprehensive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

Schedule a scan

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

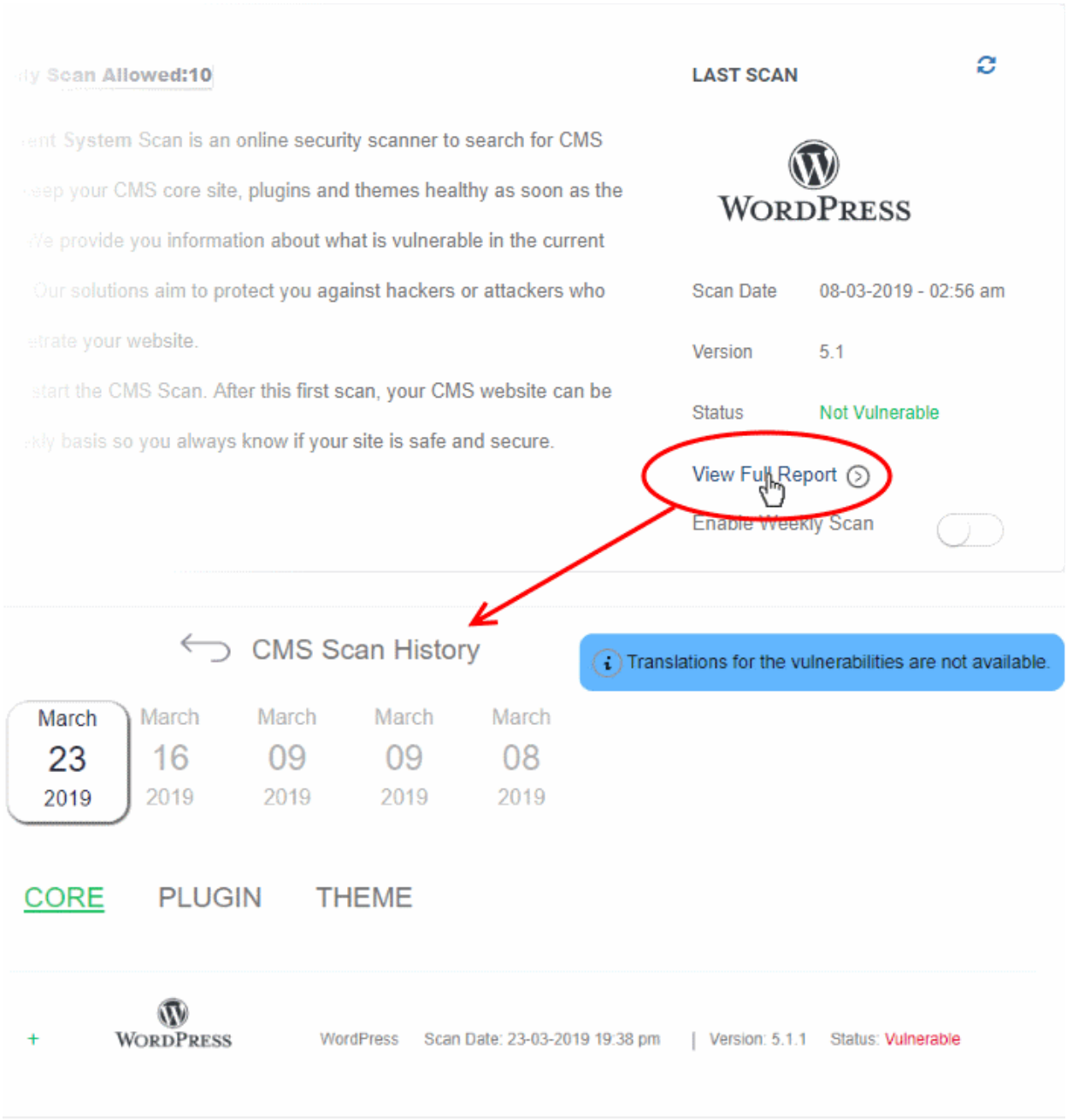
- Select the target website from the menu at top-left
- Click the 'Vulnerability' tab (or click the hamburger button and select 'Vulnerability')
- Select the 'Enable Weekly Scan' switch in the 'CMS Scan' pane as shown below:



- Weekly scans will start the next day. They will run on the same day, at the same 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

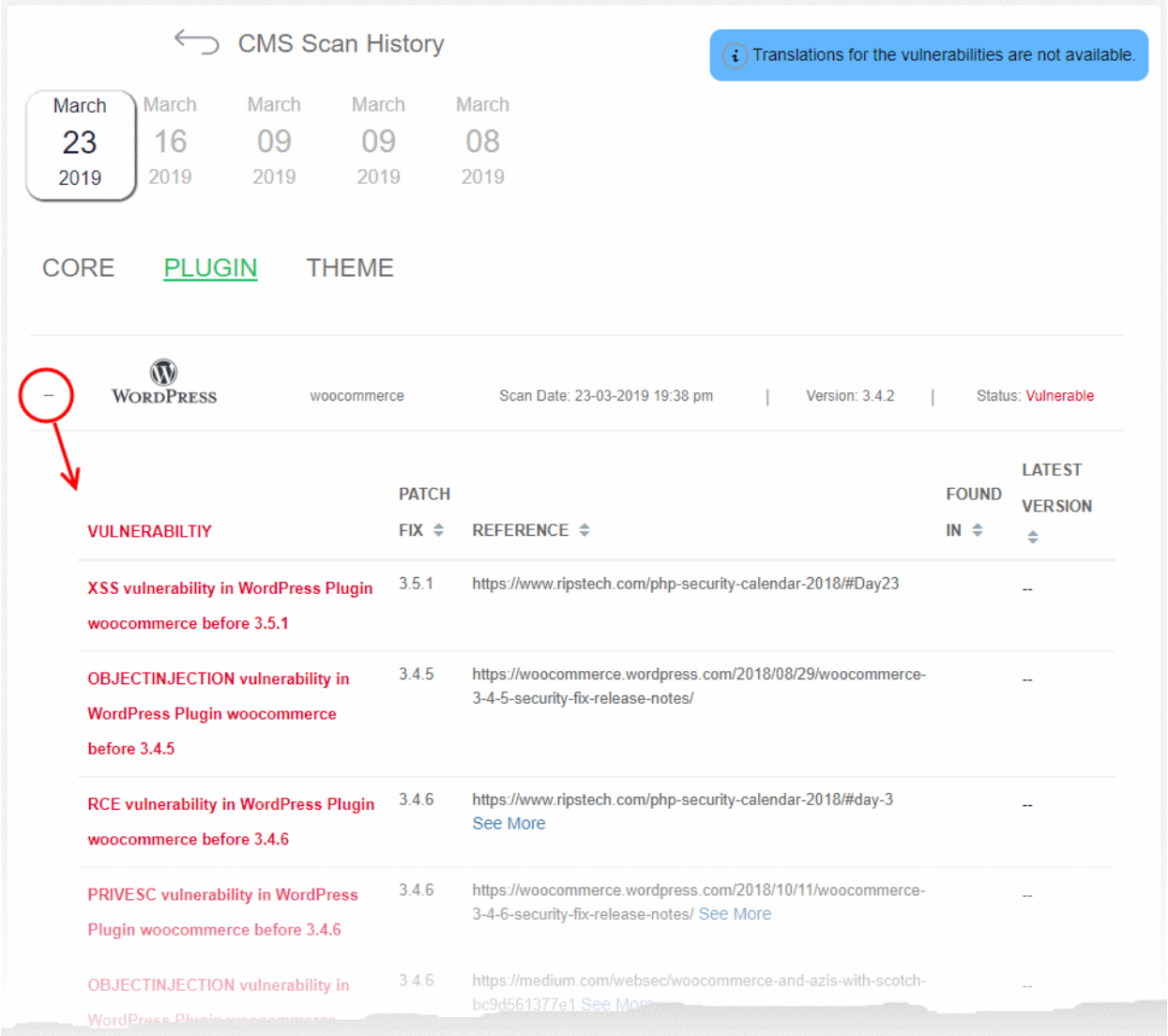
- Select the target website from the menu at top-left
- Click the 'Vulnerability' tab (or click the hamburger button and select 'Vulnerability')
- Click 'View Full Report' under 'Last Scan' in the CMS scan pane as shown below:



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:



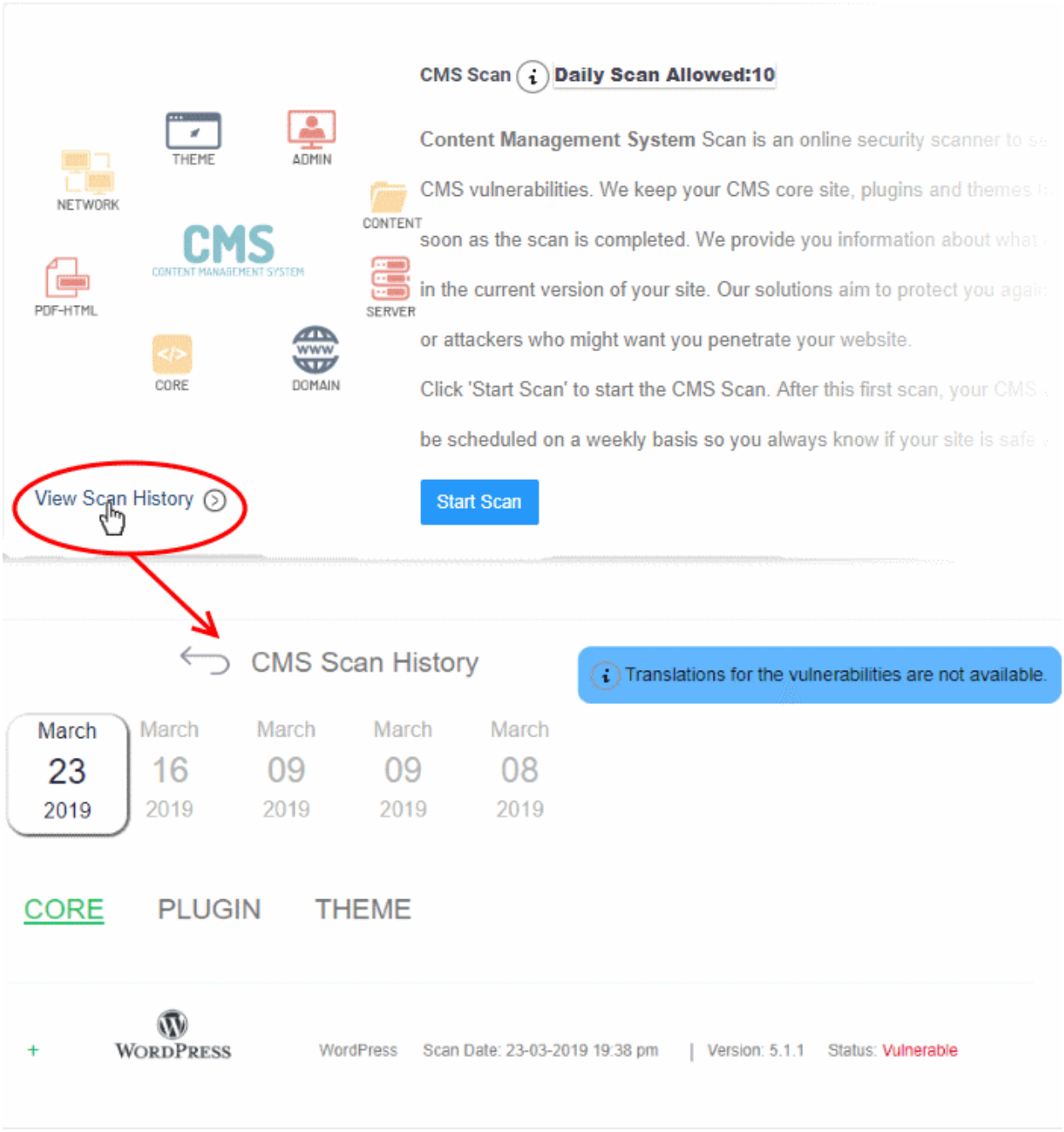
CMS Vulnerabilities - Column Descriptions	
Column Header	**Description**
Vulnerability	A short description of the weakness
Patch Fix	The version of the CMS in which the vulnerability was fixed. Update your CMS to this version to remove the vulnerability from your site.
Reference	Links to detailed information about the vulnerability and guidance to fix the issue. • Click 'See More' to view a list of reference pages
Found in	The version of the CMS in which the vulnerability was discovered. • Click 'See More' to view a list of versions in which the vulnerability is found
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 'Vulnerability' tab (or click the hamburger button and select 'Vulnerability')
- Click 'View Scan History' in the 'CMS Scan' pane



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

- Select a date to view detailed results from the scan run on that day

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

4.3.2 OWASP Top 10 Vulnerability Scans

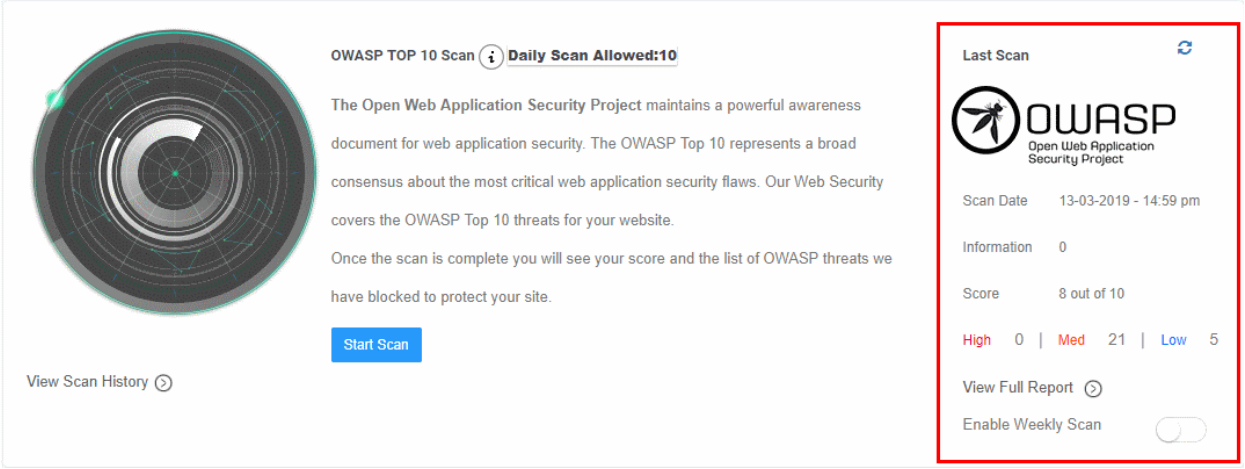
- Select a website from the drop-down at top-left and choose 'Vulnerability'
- cWatch scans your sites for the top-ten vulnerabilities published by the Open Web Application Security Project (OWASP).
- The results identify any weaknesses found on your site along with guidance to fix them.

- You can run OWASP scans on-demand, and/or schedule weekly scans. You can also view the results of the last ten scans.

Run OWASP top 10 vulnerability scans and view results

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

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

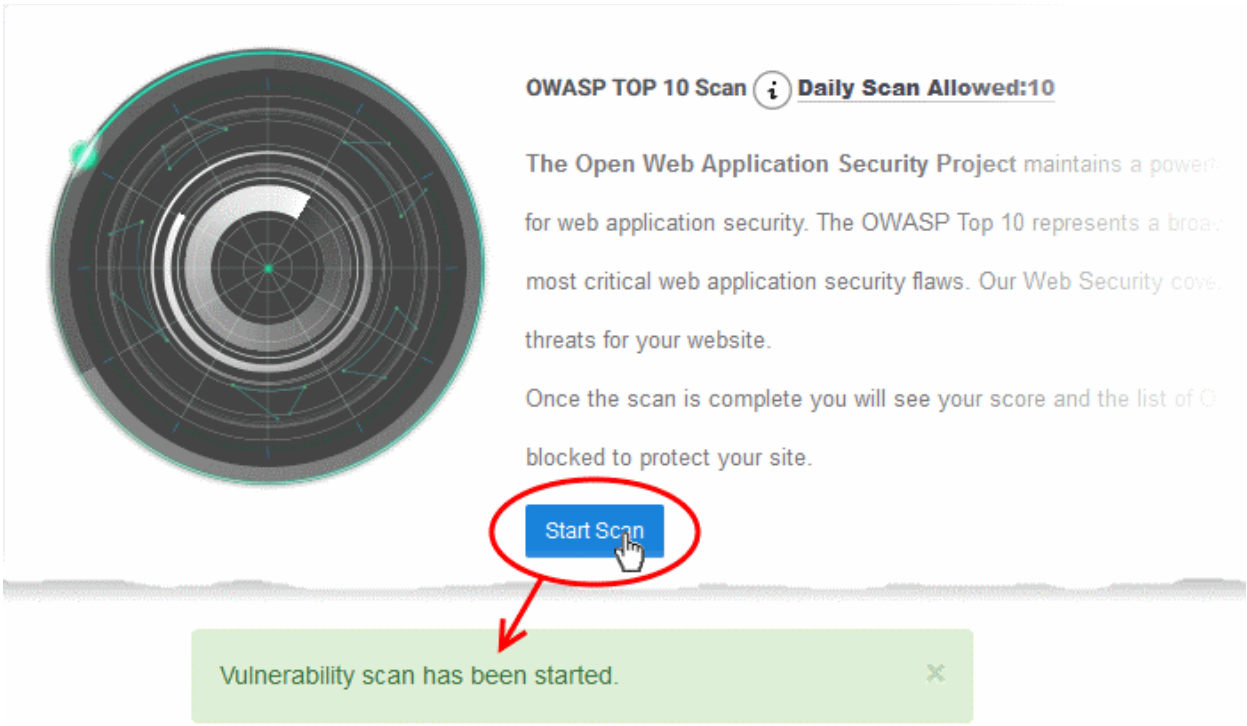
The pane lets you:

- **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 'Vulnerability' tab (or click the hamburger button and select 'Vulnerability')
- Click 'Start Scan' in the 'OWASP Top 10 Scan' pane:

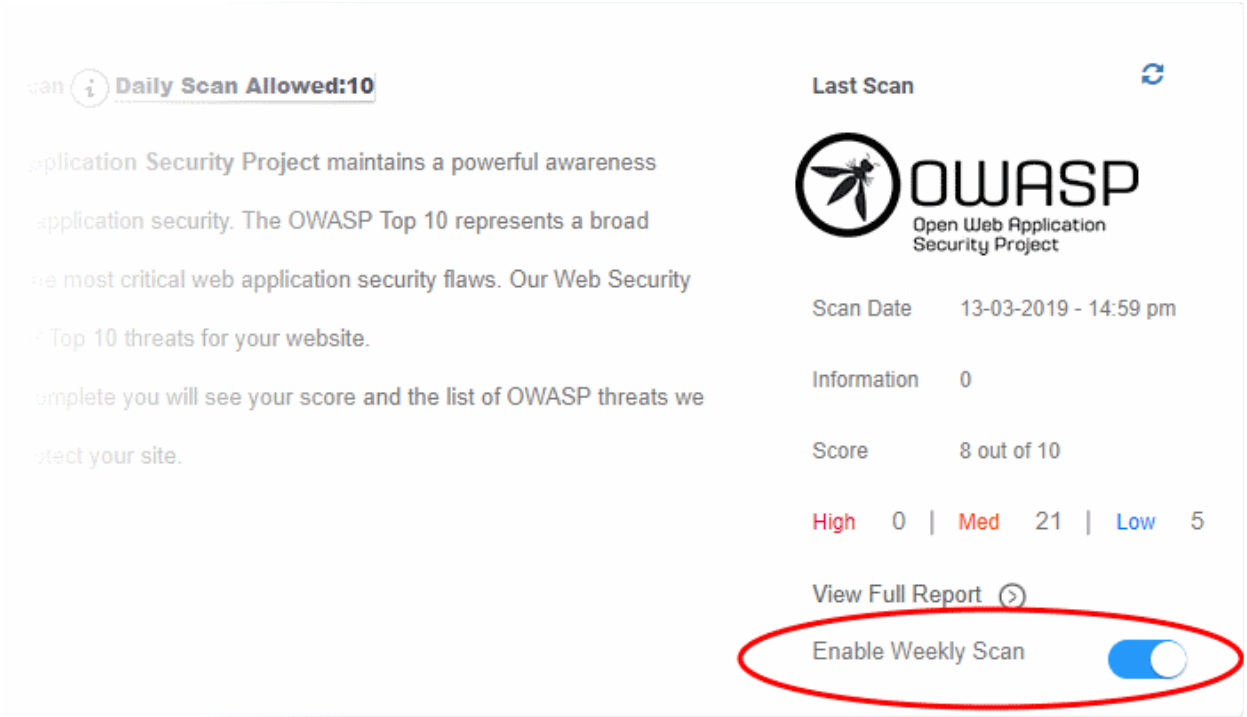


- cWatch will begin scanning the domain for OWASP top 10 vulnerabilities.
- Scan results are shown in the 'Last Scan' box on the right
- Click the 'Refresh' icon at top-right to reload the results of the scan
- Alerts will be generated if any vulnerabilities are found.
- Click 'View Full Report' for 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 'Vulnerability' tab (or click the hamburger button and select 'Vulnerability')
- Use the switch in the OWASP pane to enable the weekly scan, as shown in the screenshot below:



- 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 'Vulnerability' tab (or click the hamburger button and select '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.

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. • Click the number to view the complete details of the threat, list of files affected and guidance to fix the issue • See **View Details of Identified Vulnerabilities** for more details

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.

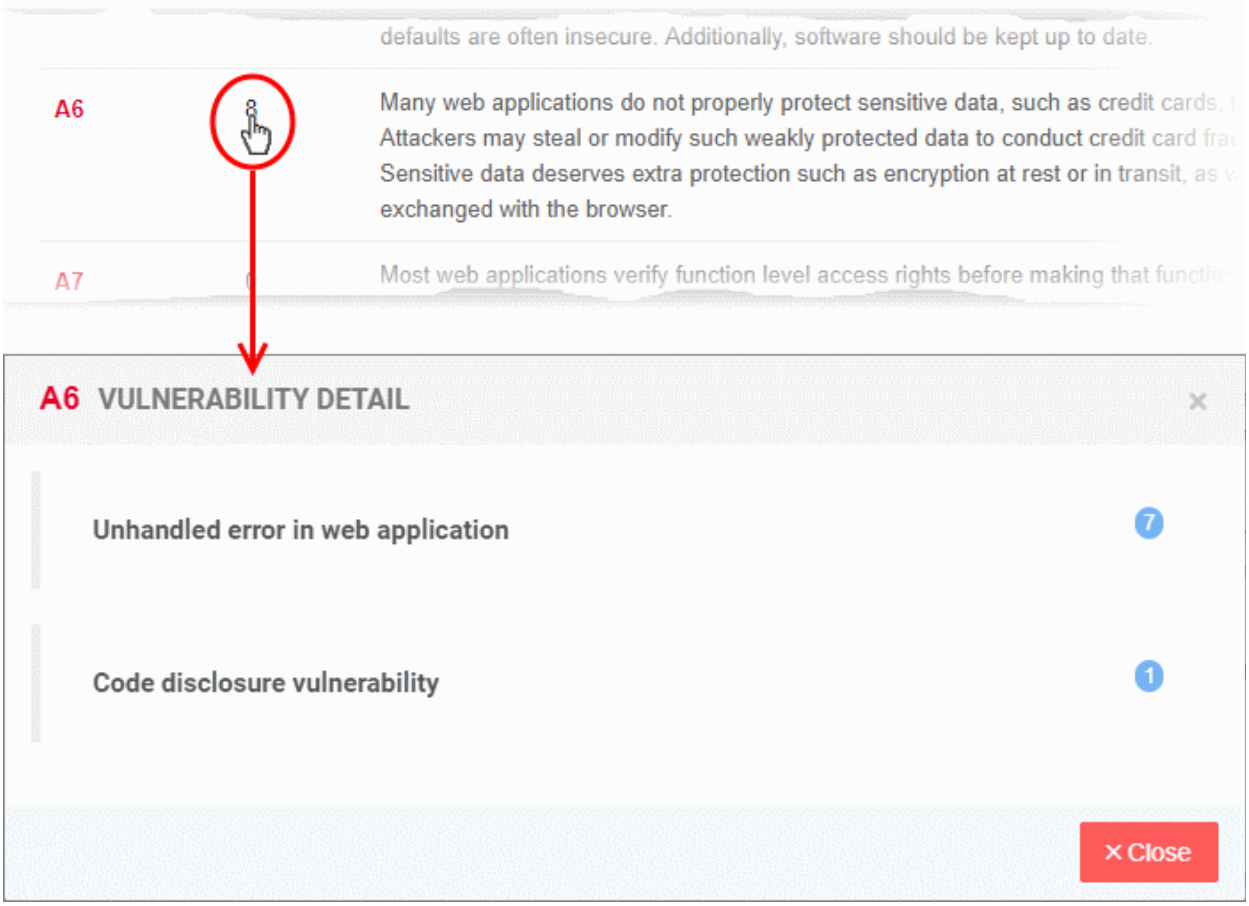
Tip: You can also submit a request for Comodo specialists to manually remove the threats. Manual removal is only available for domains with a premium license.

View detailed vulnerability information

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

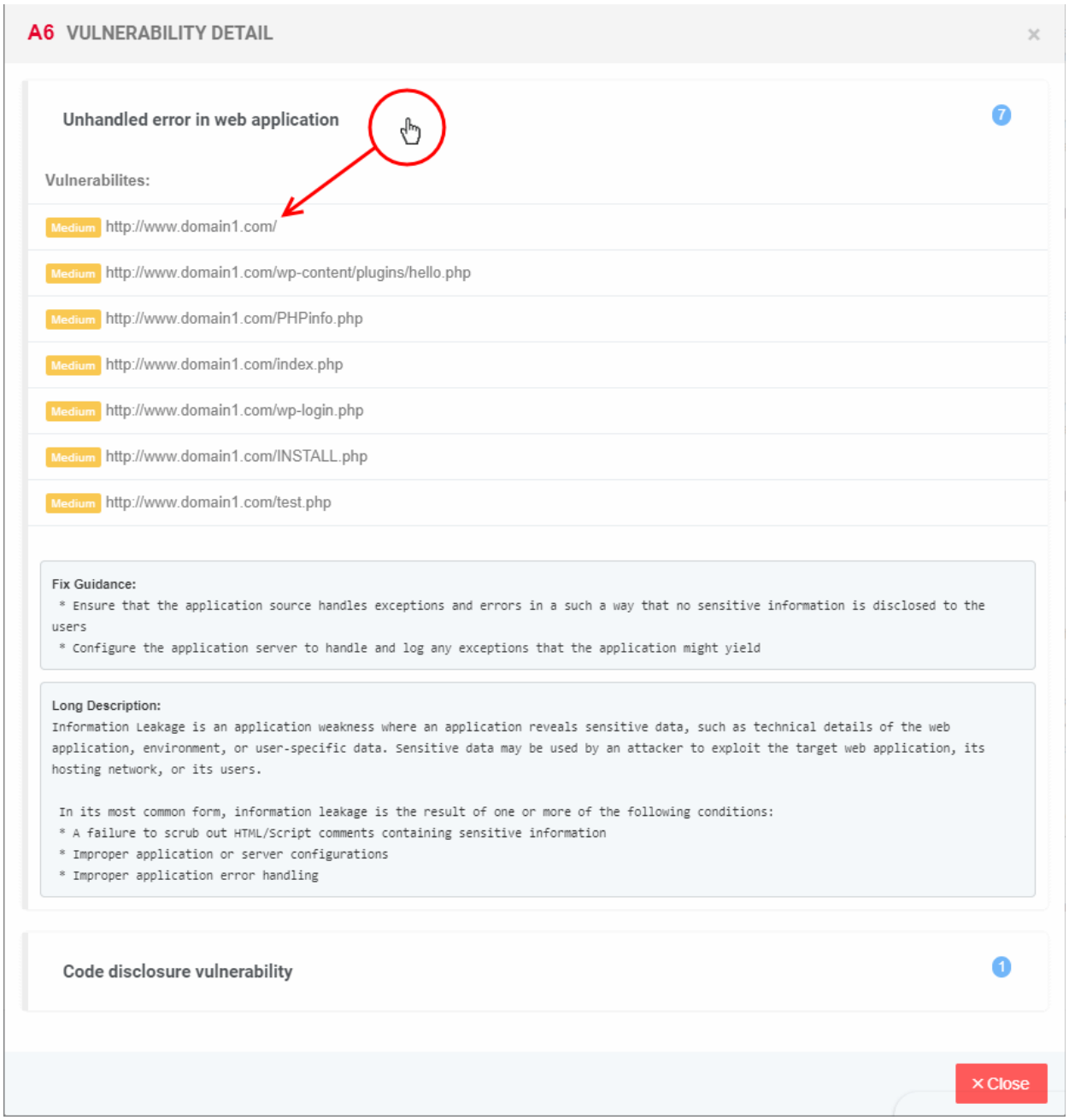
The numbers of vulnerabilities identified in each of the top ten OWASP vulnerability categories is shown as a list.

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



The 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:

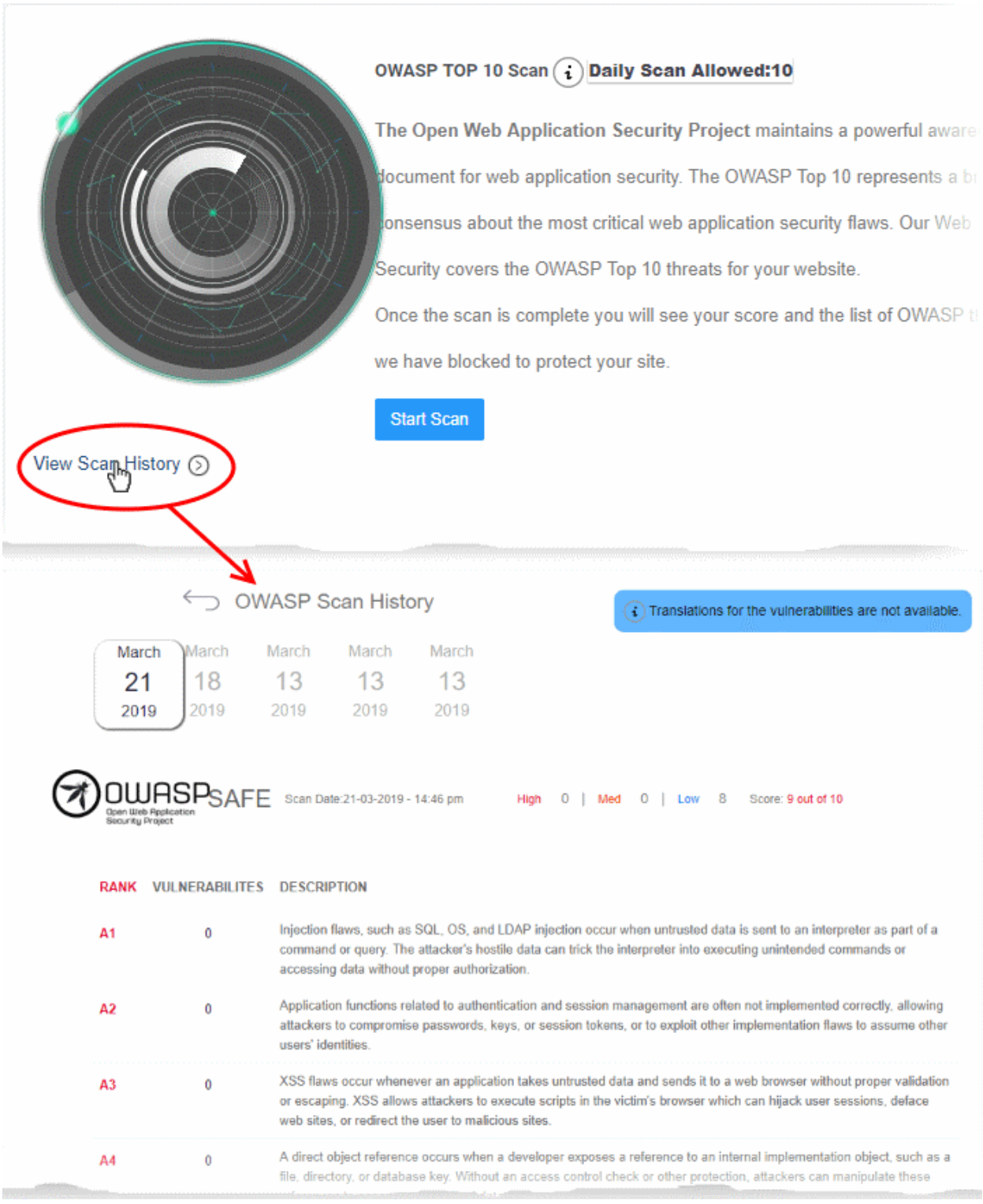


- The 'Vulnerabilities' pane shows a list of affected files with their risk level.
- The 'Fix Guidance' pane summarizes the fix recommendations.
- The 'Long Description' pane contains detailed background information on the threat

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 'Vulnerability' tab (or click the hamburger button and select 'Vulnerability')
- Click 'View Scan History' in the 'OWASP Top Scan' pane



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

- Select a date to view detailed results from the scan run on that day

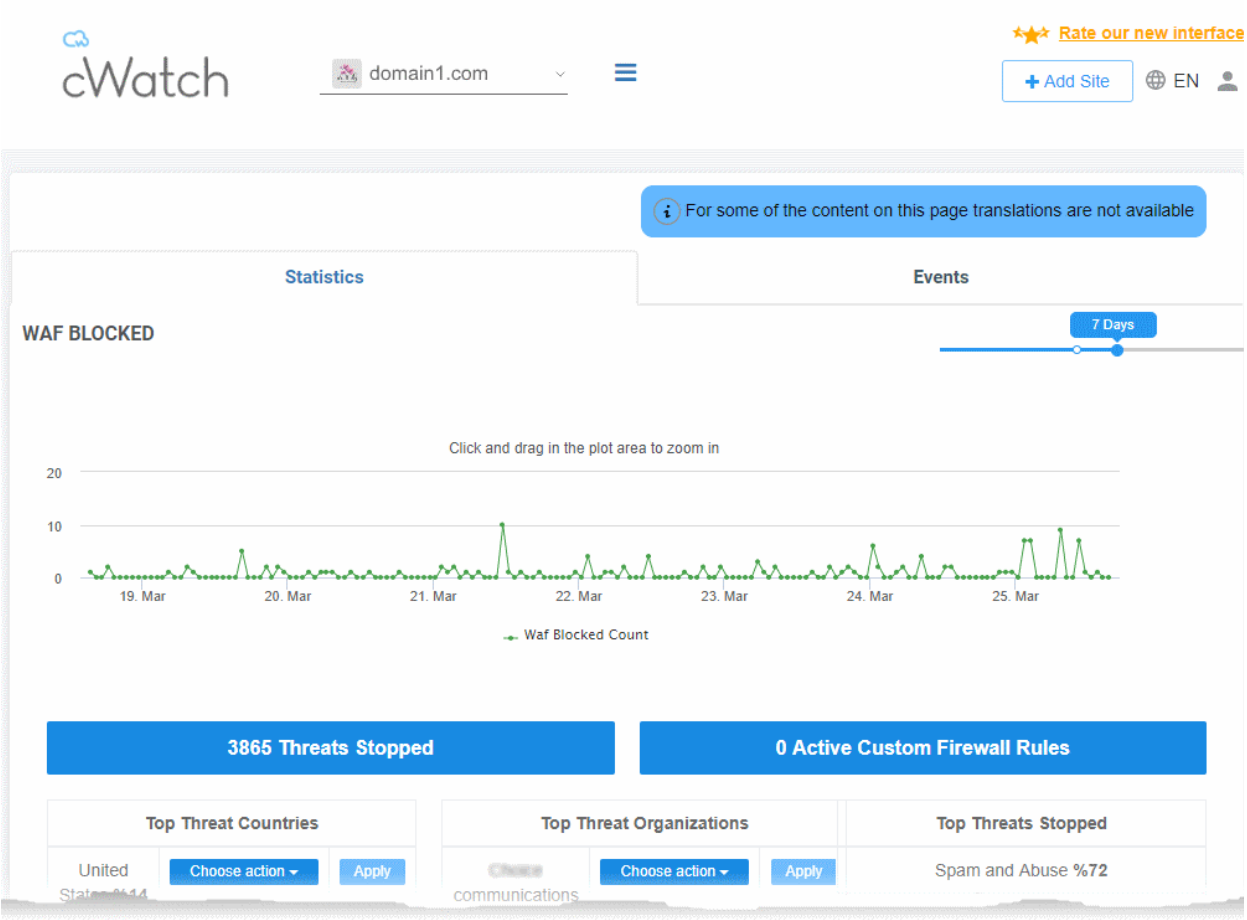
See **View detailed results of the last scan** if you need more help with this.

4.4 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 to our users.
- The CSOC interface shows detailed stats about attacks that were blocked on your site. It also lets you choose an action that cWatch should take if a similar attack takes place.

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.

4.4.1 WAF Statistics

- Choose a website from the drop-down at top-left
- Click 'Cyber Security' > 'Statistics' tab

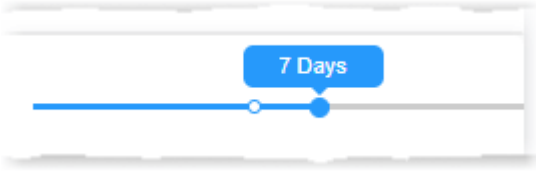
- The statistics page shows attacks identified and blocked by the Web Application Firewall (WAF). This includes the top 5 attack types and top 5 attack sources.
- You can also choose the action taken on future threats from the same source. cWatch updates your WAF rules accordingly.

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 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.

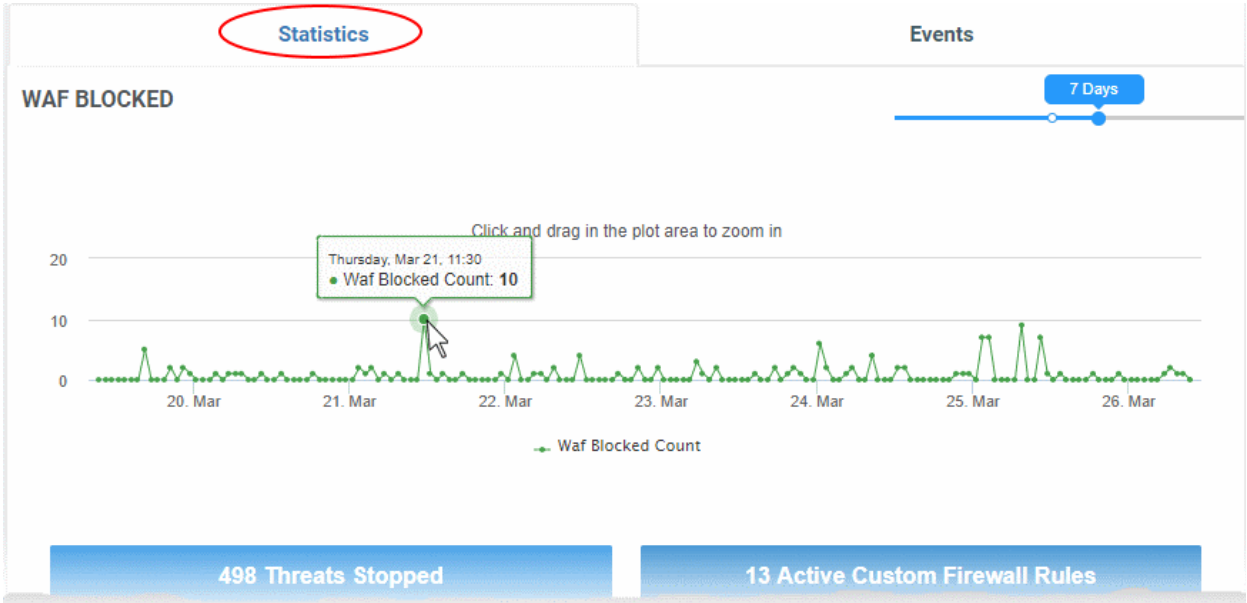
View WAF statistics

- 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.

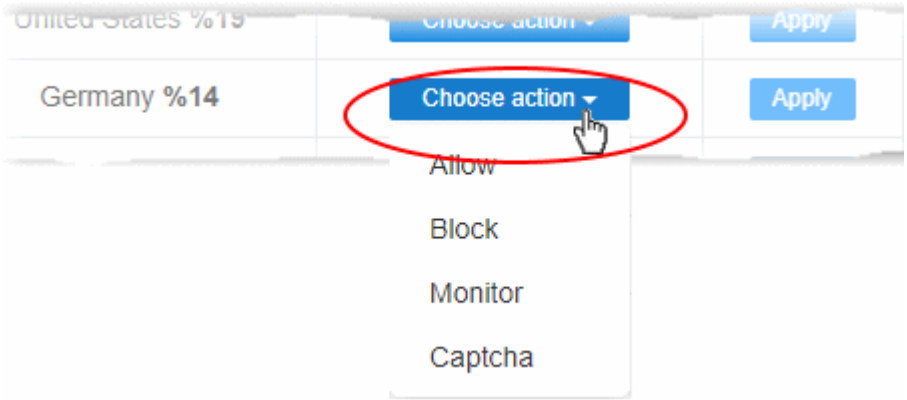
- **<NN> Threats Stopped** - Click to view a list of the threats blocked. See **WAF Events** for more details.
- **<NN> Active Custom Firewall Rules** - Click to view and manage the WAF rules active on the site. See **Manage Custom Firewall Rules** for more details.

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.

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.

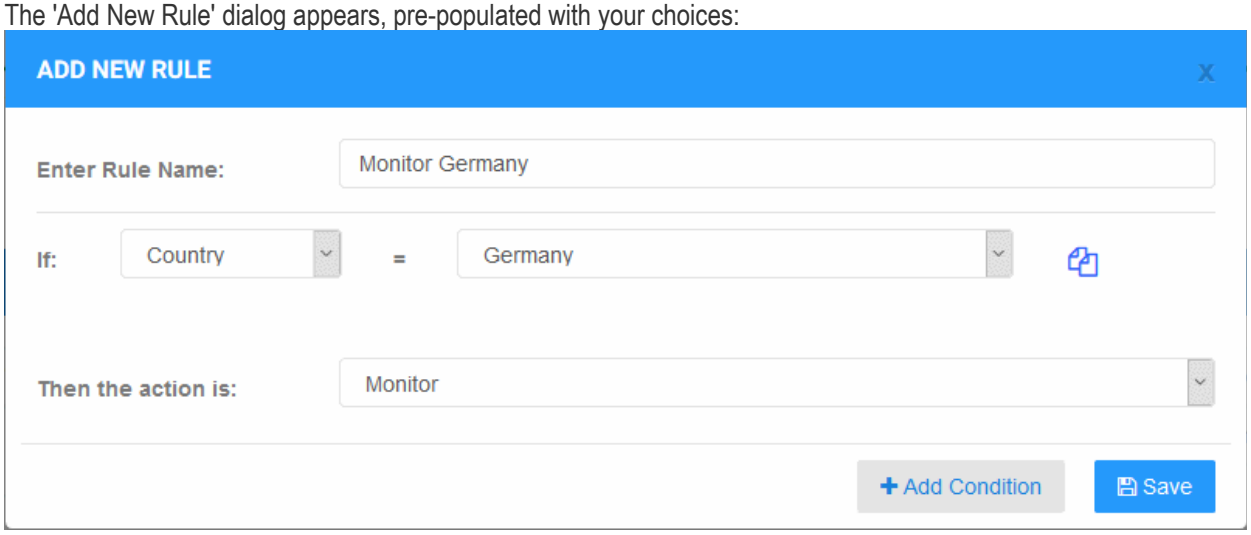


- **Allow** - All traffic from the country is permitted. This includes legitimate traffic, bots, malicious traffic etc.
- **Block** - No traffic is allowed from the country. An error message is shown to users.
- **Monitor** - Traffic from the country is recorded. This action is particularly useful for 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:

- 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		
[redacted] %35	Choose action	Apply
[redacted] %10	Choose action	Apply
[redacted] %10	Choose action	Apply
[redacted] %4	Choose action	Apply
[redacted] %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.

4.4.2 WAF Events

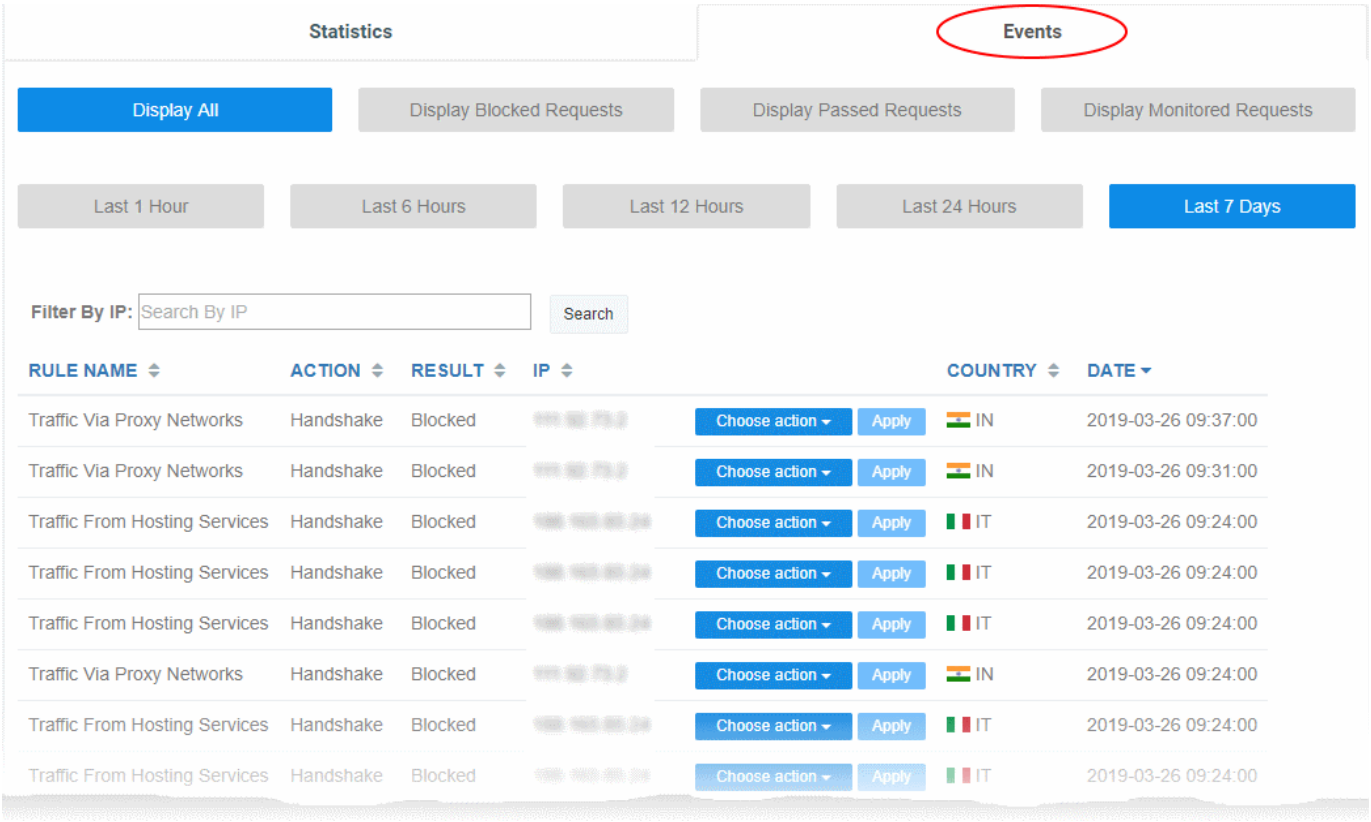
- Choose a website from the drop-down at top-left
- Click 'Cyber Security' > 'Events' tab
- The 'Events' page lists all access attempts intercepted by Web Application Firewall (WAF) rules. This includes both built-in and custom firewall rules
- Details include the source IP of the attempt, the rule that 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.

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 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

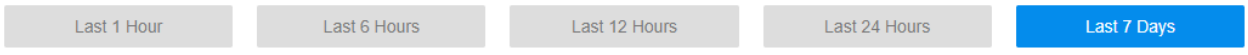


WAF Events - Column Descriptions	
Column Header	**Description**
Rule Name	The label of the firewall rule that intercepted the access request
Action	The activity of the access request on the website
Result	Whether the traffic was blocked, allowed, monitored, or allowed with captcha verification
IP	The 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

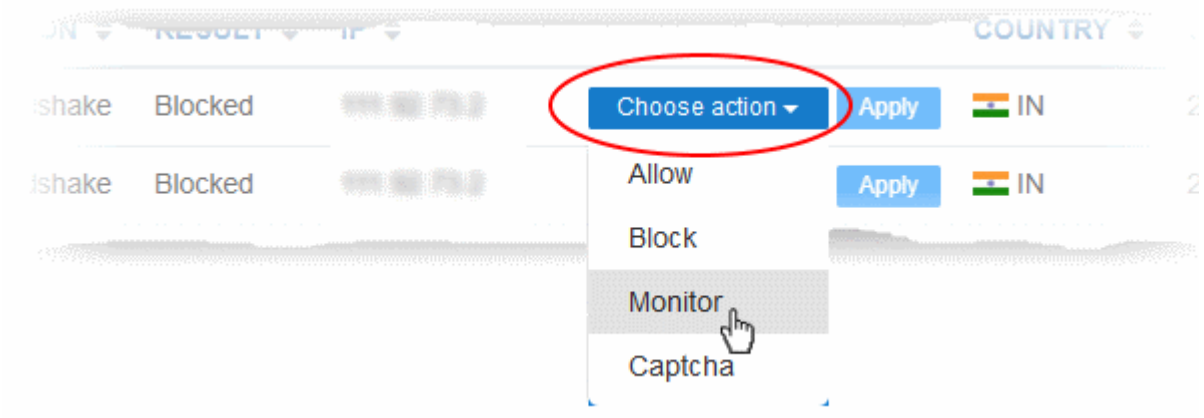


- Search box - Enter an IP to find access requests from a specific address

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.

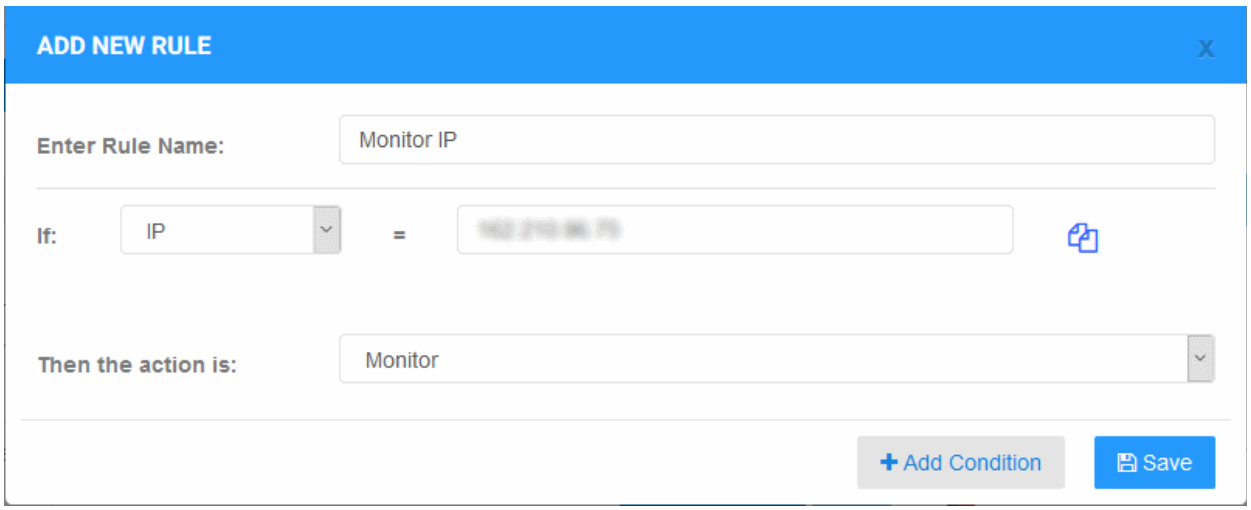
- The action you choose here will create a custom firewall rule for traffic from the IP:



- **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:



- 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:

- See **Manage Custom Firewall Rules** for help with custom firewall rules.

4.5 Content Delivery Network

- Select a website from the drop-down at top-left
- Choose 'CDN'
- Your cWatch license includes a content delivery network (CDN) service for your websites. The service will improve page load-times for your customers and improve the reliability/uptime of your site.
- You can configure your sites to use the service by changing your domain's authoritative DNS to Comodo, or by adding a CNAME entry to your DNS records.
- Comodo Authoritative DNS name server (NS) details are provided in '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 to identify anomalous behavior and threats.
- Provide Comodo web application firewall protection for your domains. The CSOC team constantly improves the Mod Security rules in Comodo web application firewall to provide cutting edge protection for our customers.

See the following sections for more help on CDN configuration:

- **Activate CDN for a Website**
- **Configure CDN Settings**
- **View CDN Metrics**

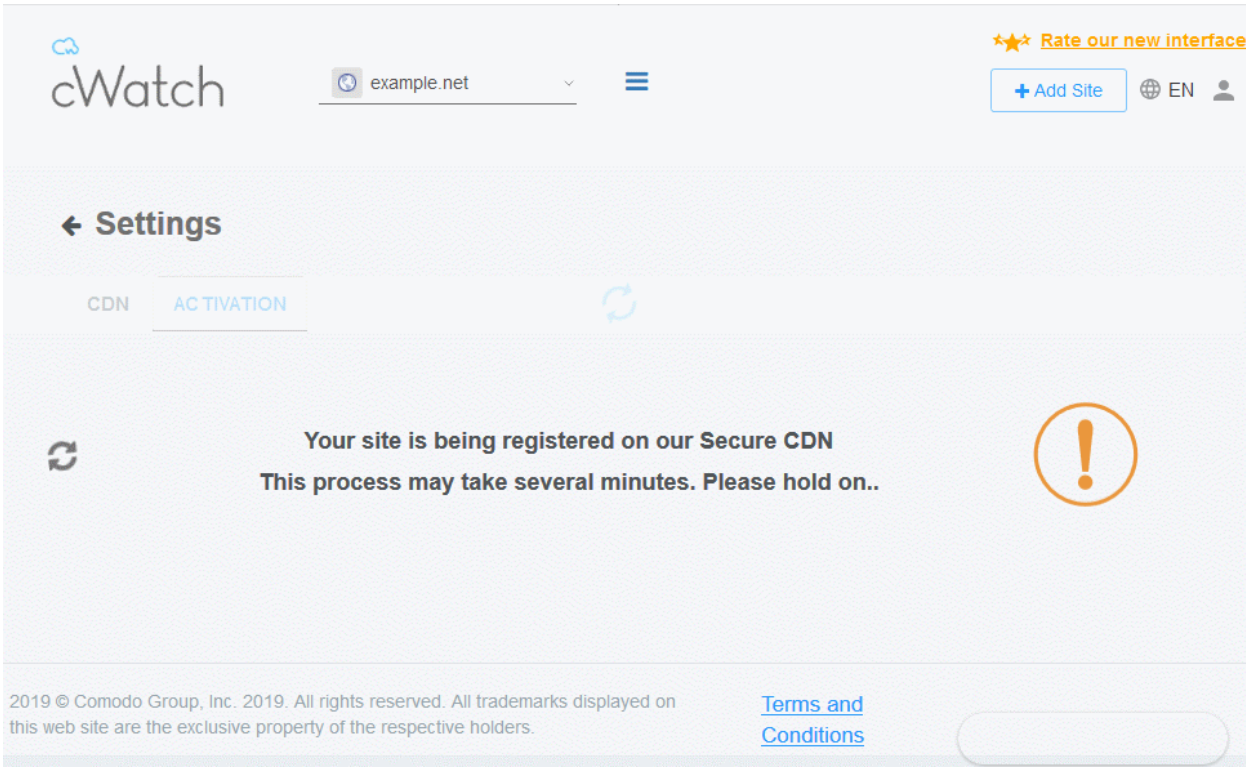
4.5.1 Activate CDN for a Website

- 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.

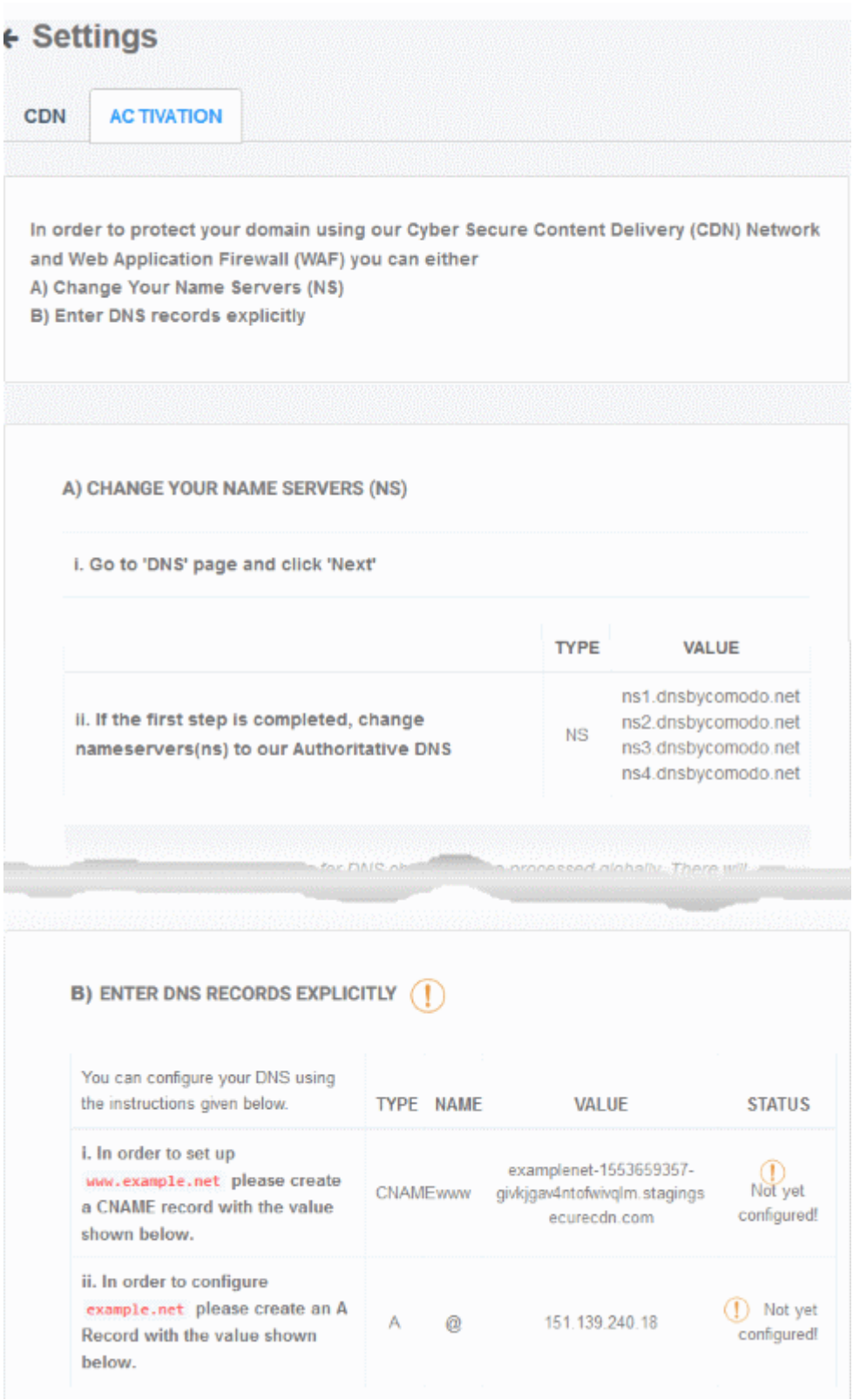
Configure DNS settings of your website

- 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:

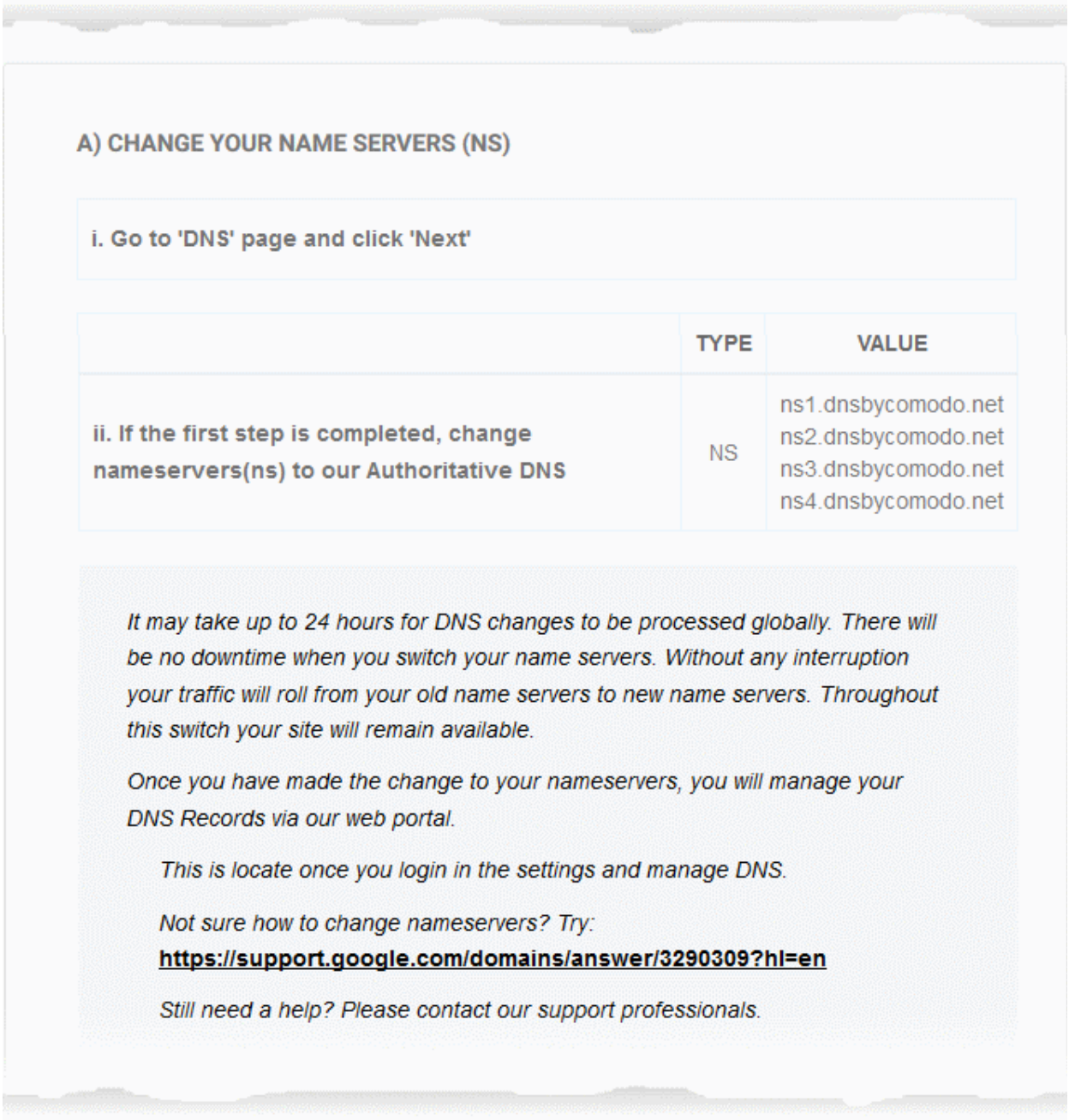


- There are two ways to configure your site to use our DNS:
  - **Change your domain's authoritative DNS servers to Comodo DNS**
  - **Enter DNS records explicitly**

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

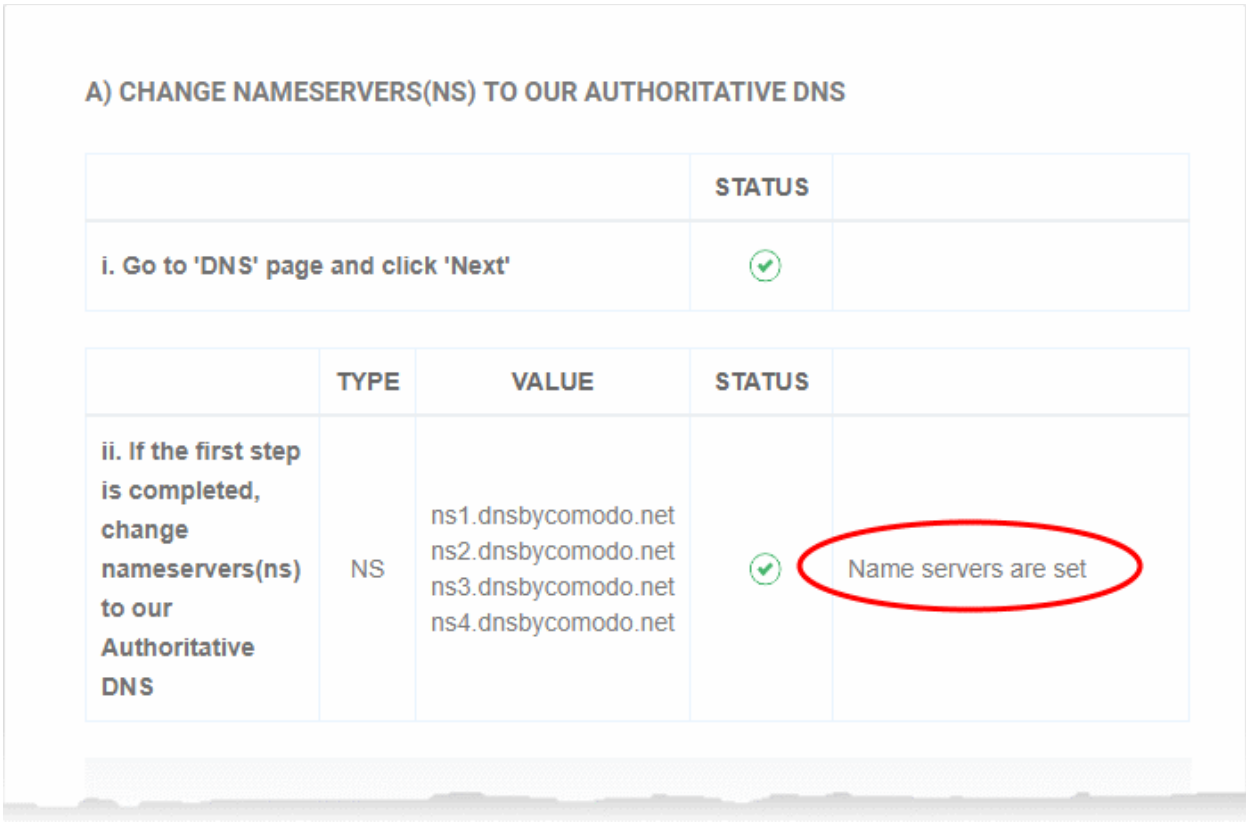
Name server (NS) details are shown in the 'CDN' > 'Settings' > 'Activation' page:



- 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...':



- 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.

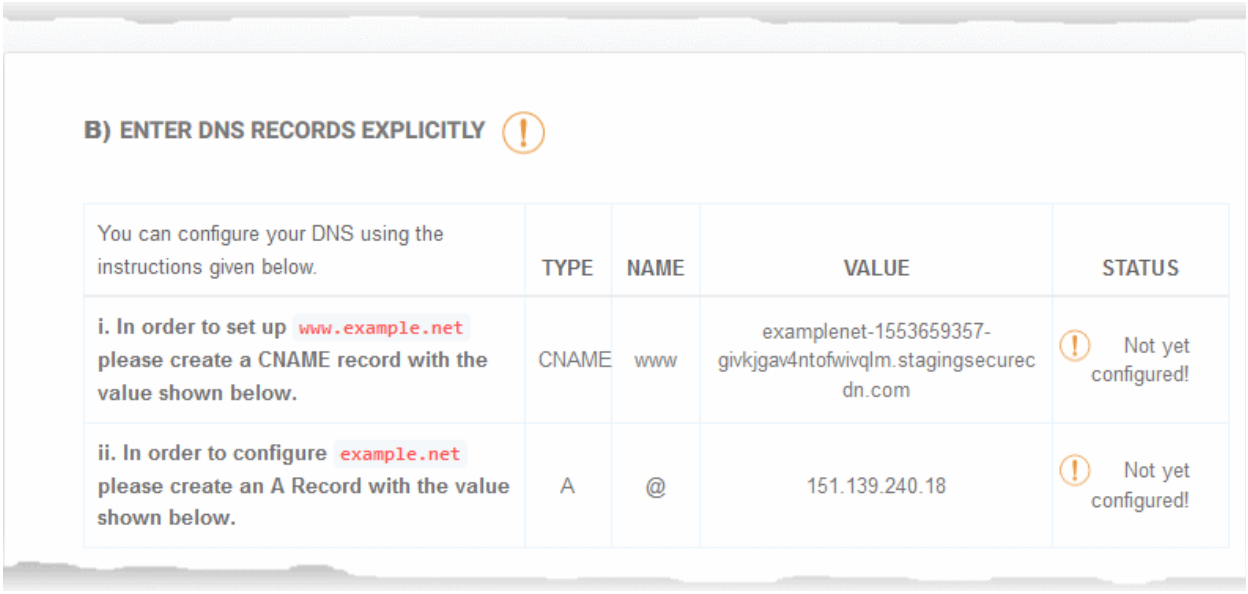
Note:

- 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':



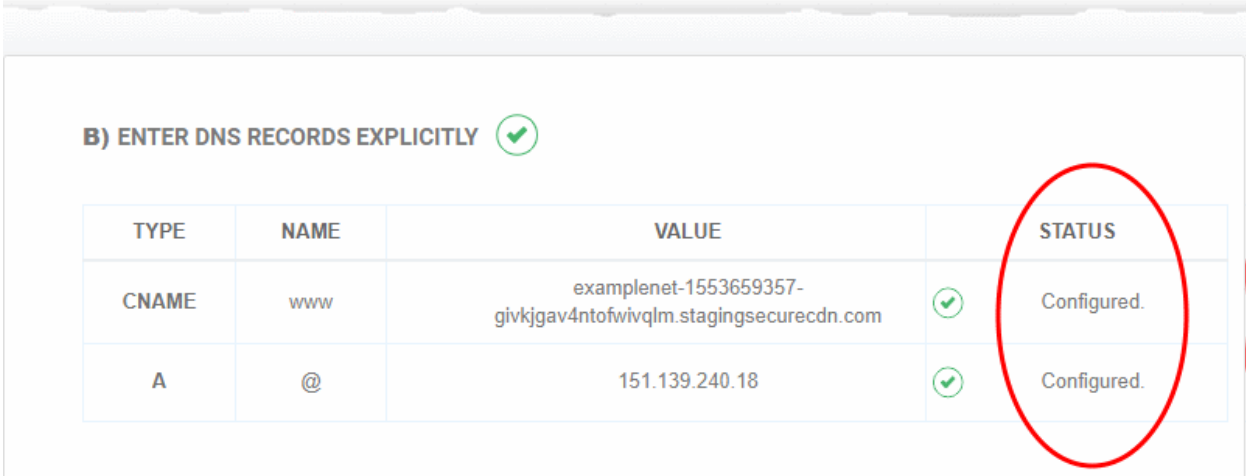
B) ENTER DNS RECORDS EXPLICITLY

You can configure your DNS using the instructions given below.	TYPE	NAME	VALUE	STATUS
i. In order to set up `www.example.net` 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 `example.net` 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.

4.5.2 Configure CDN Settings

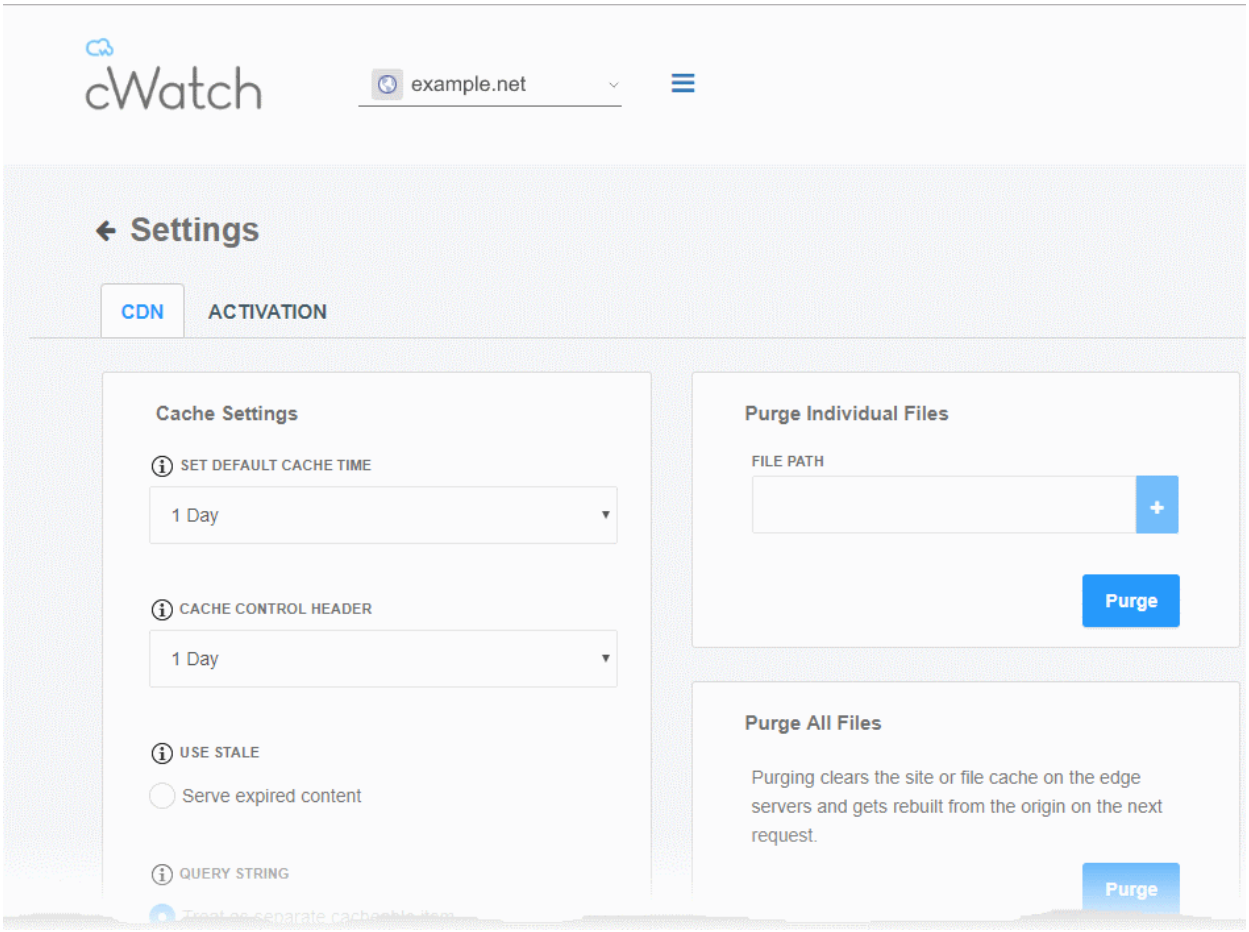
- Choose a website from the drop-down at top-left and select 'CDN'

- Click 'Settings' > 'CDN'

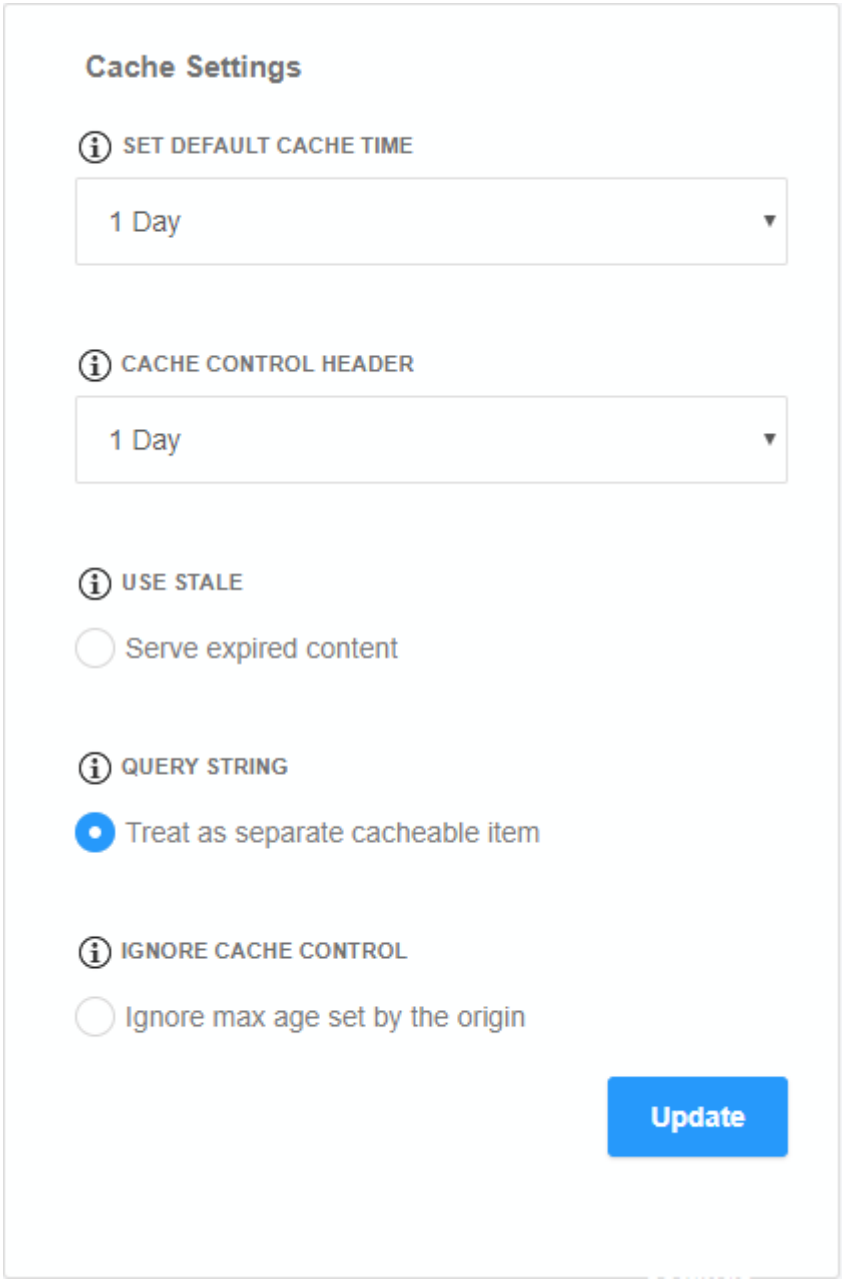
The 'CDN Settings' page lets you configure how the website data are to be cached and rendered by the CDN edge servers, clear cache, configure site settings and more.

Configure CDN settings

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



Cache Settings

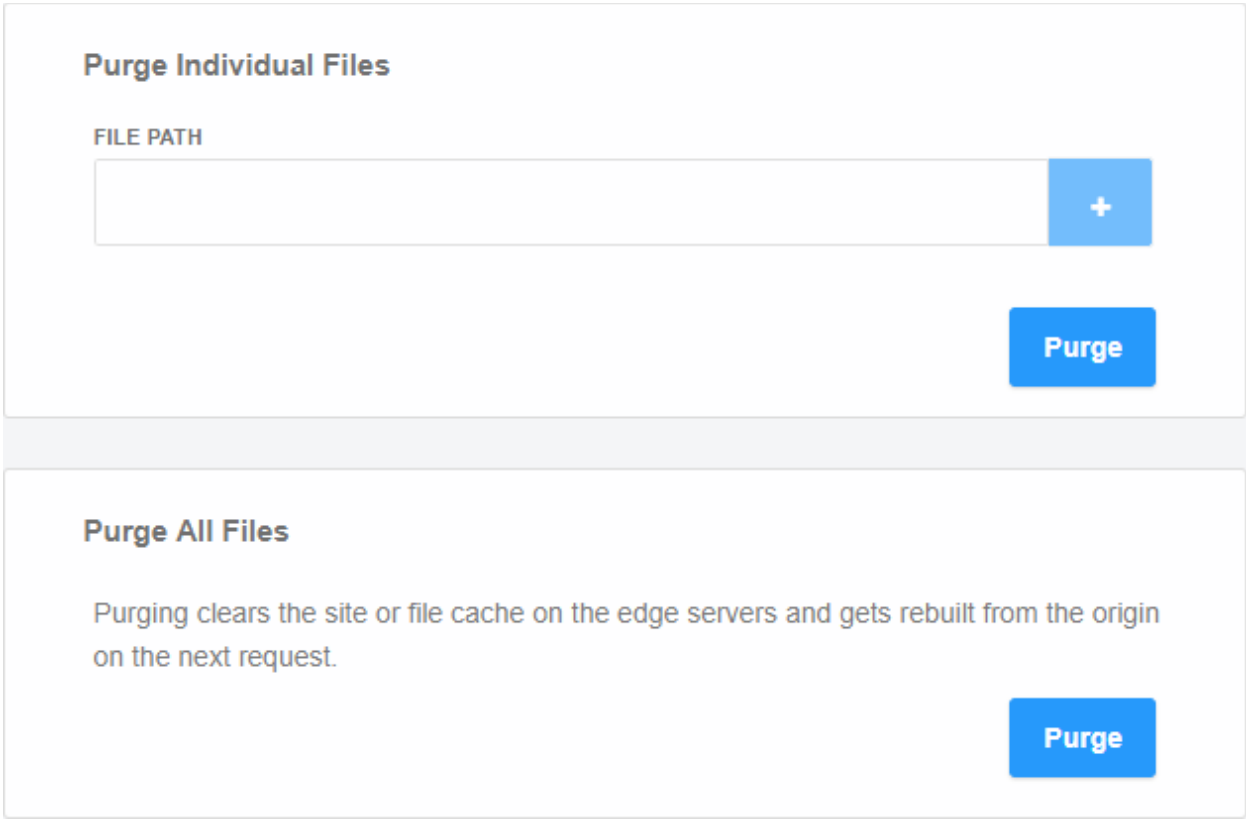


Cache Settings - Table of Parameters	
Parameter	**Description**
Set Default Cache Time	Define how long content fetched from your web servers should remain in the CDN cache. Cached content is used to accelerate site loading times for your visitors. The CDN will collect refreshed content from your site when this period expires. 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.
Cache Control Header	Defines how long cached content in the web browser can be reused without checking the web server for updates. **Background Note:** Cache control headers are used to specify how long content fetched from site should remain in the browser's cache. The local cache is used by the browser to render the site when it is re-visited by the user, avoiding the need to fetch the content repeatedly from the server.
Use State	Select 'Serve expired content' if you want the CDN to deliver cached content when:

	• The CDN is currently checking the website for updated content • Your website is down.
Query String	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.

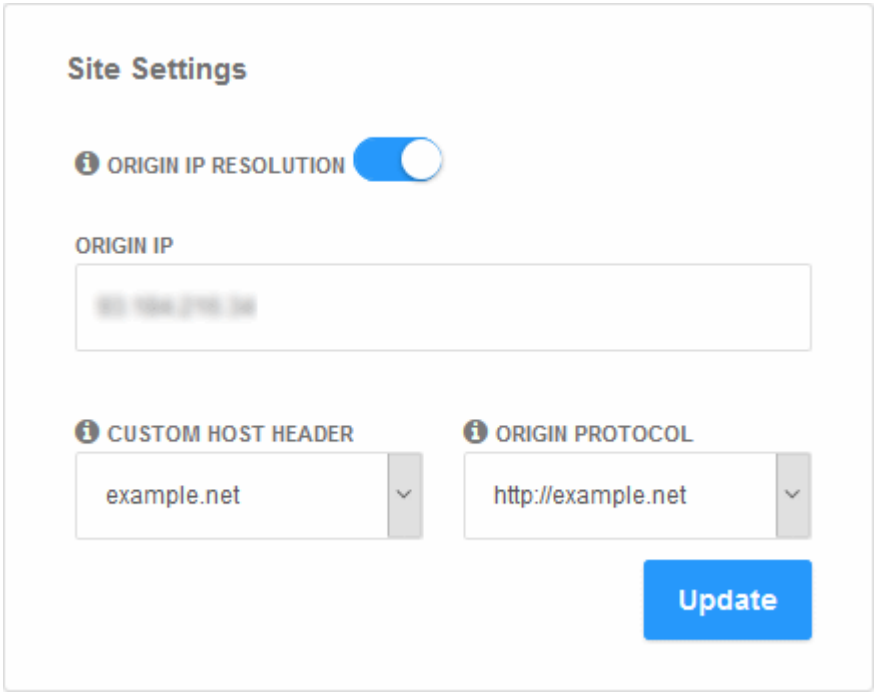
- Click 'Update Cache Settings' for your changes to take effect.

Purge Files



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

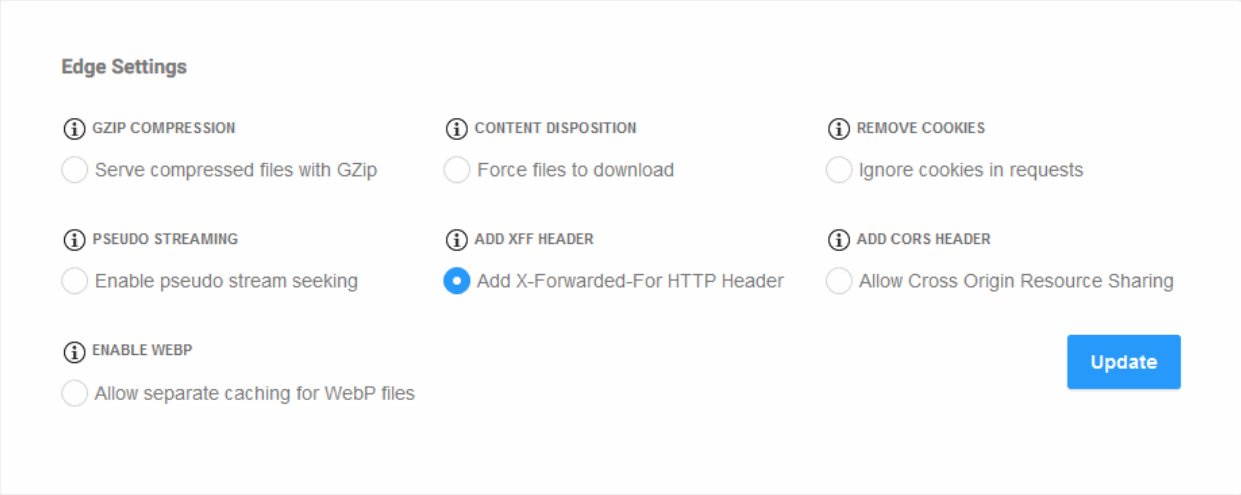
Site Settings



Site Settings	
Origin IP Resolution	Choose whether or not the CDN should use DNS servers to resolve the IP address of your web server. This depends on whether your server uses a static or dynamic IP address. • If your server uses a static IP address, enable 'Origin IP Resolution'. The CDN will fetch your IP address by domain look-up, save it and display it in the 'Origin IP' field. The CDN will use this IP address to fetch the files from your web server. This will save time for content delivery to your website visitors. • If your server uses dynamic IP address, disable this option. The CDN will use DNS services to resolve your IP address.
Custom Host Header	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 - 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.

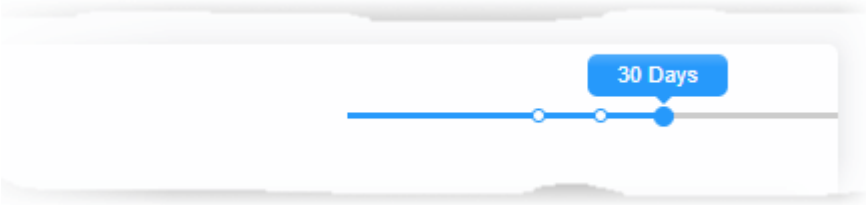
4.5.3 View CDN Metrics

- Select a website from the drop-down at top-left and choose 'CDN'
- The CDN metrics page shows your site's CDN usage and traffic throughput.

View CDN metrics

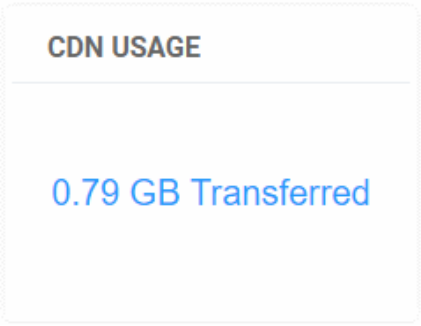
- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'CDN' tab (or click the hamburger button and select 'CDN')

- Select the period for which you want to view the metrics from the slider at top-right:



The page contains the following charts:

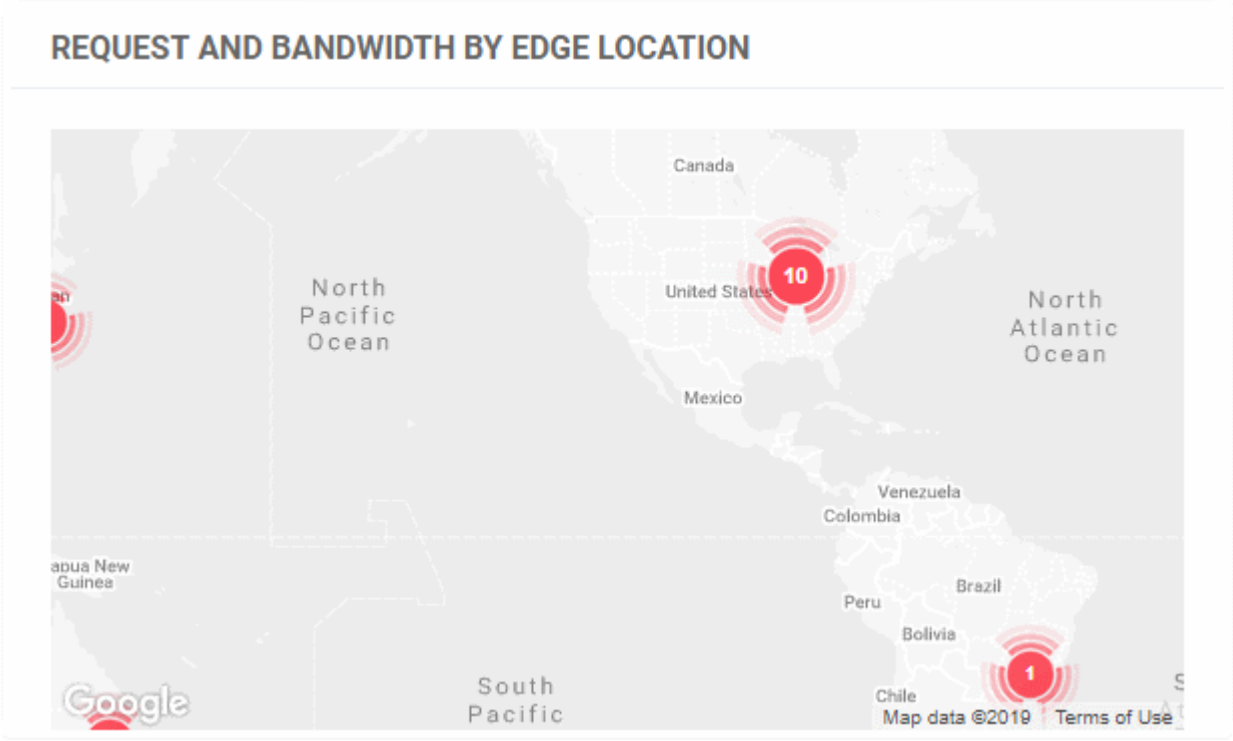
CDN Usage



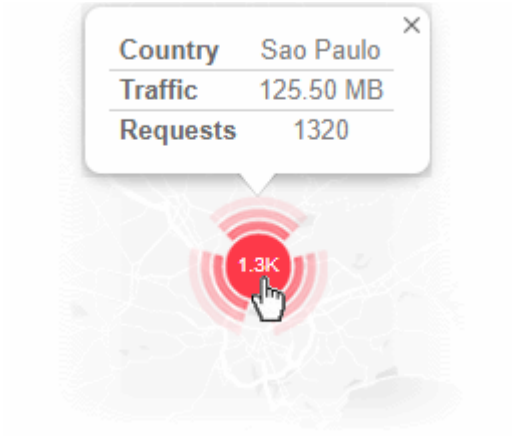
The 'CDN Usage' field shows how much CDN data your website has used.

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.

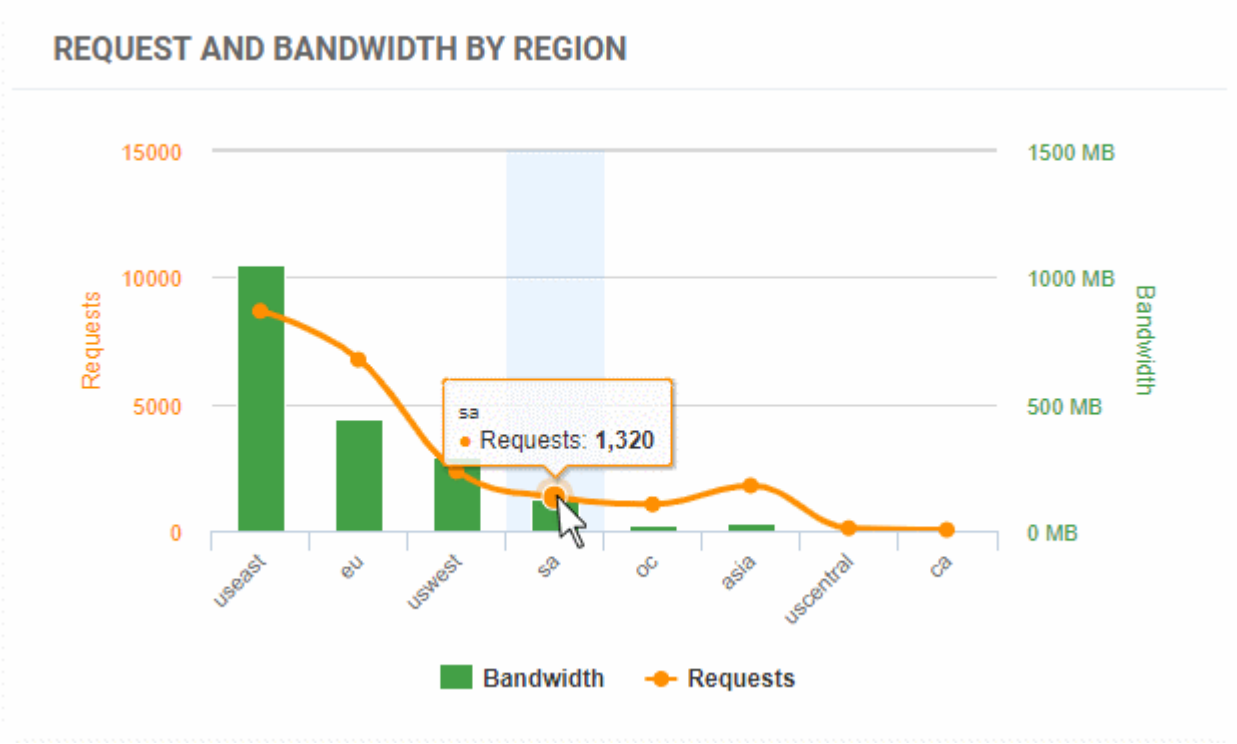


- Click on an regional hot-spot to view the traffic and number of access requests from that area.



Request and Bandwidth by Region

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

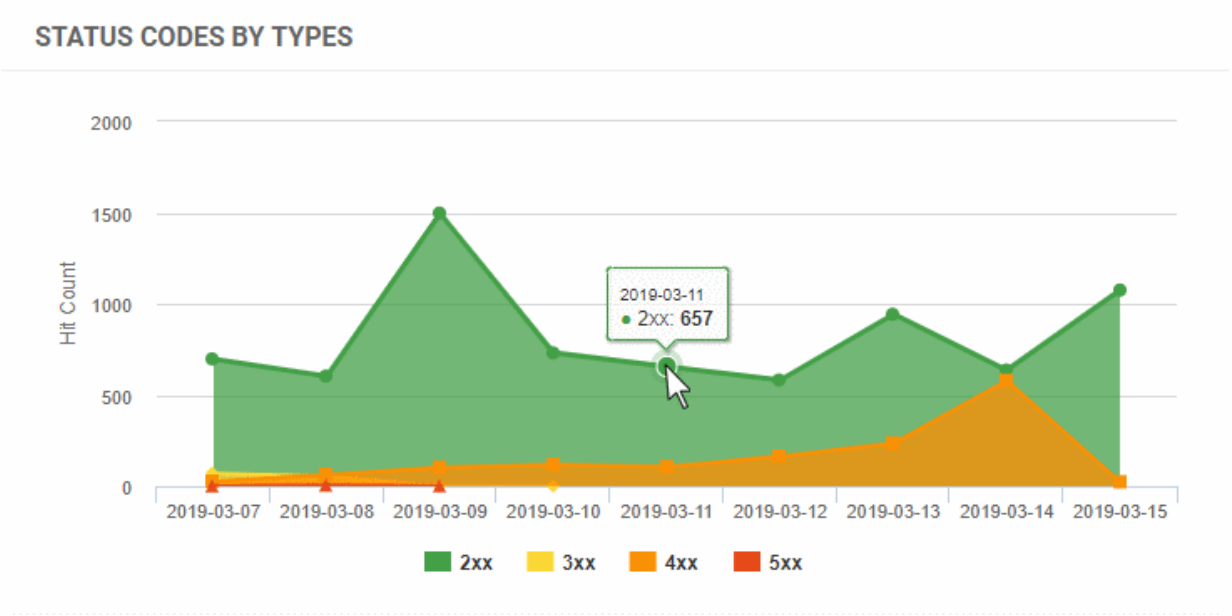


- Select a portion of the graph to zoom-in

- 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.



- 2xx = Success
- 3xx = Redirection
- 4xx = Client errors
- 5xx = Server errors

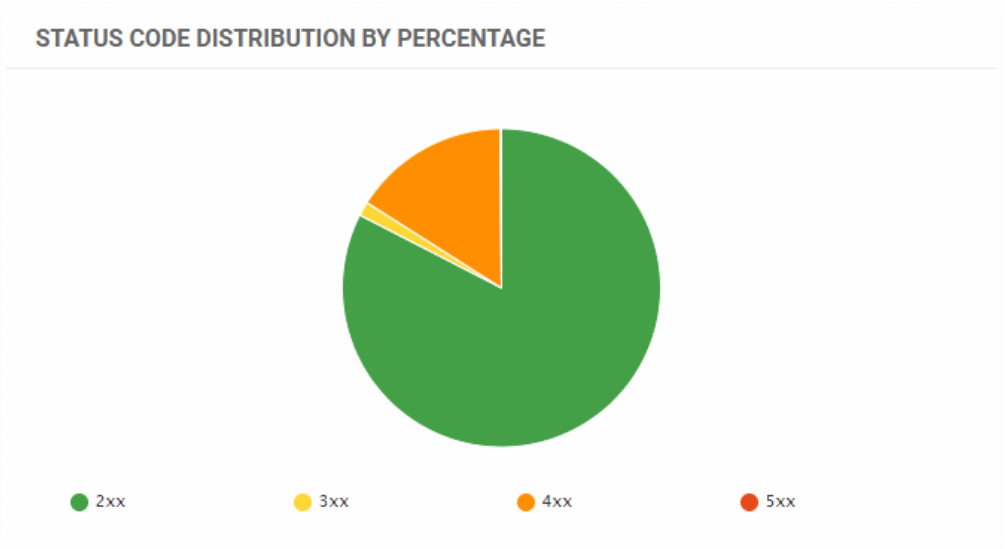
- You can choose the time period using the slider at top-right.
- Select a portion of the graph to zoom-in
- Place your mouse on the graph to view the number of responses of that type returned at that time point

Status Code Distribution by Percentage

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

  HTTP status codes are as follows:

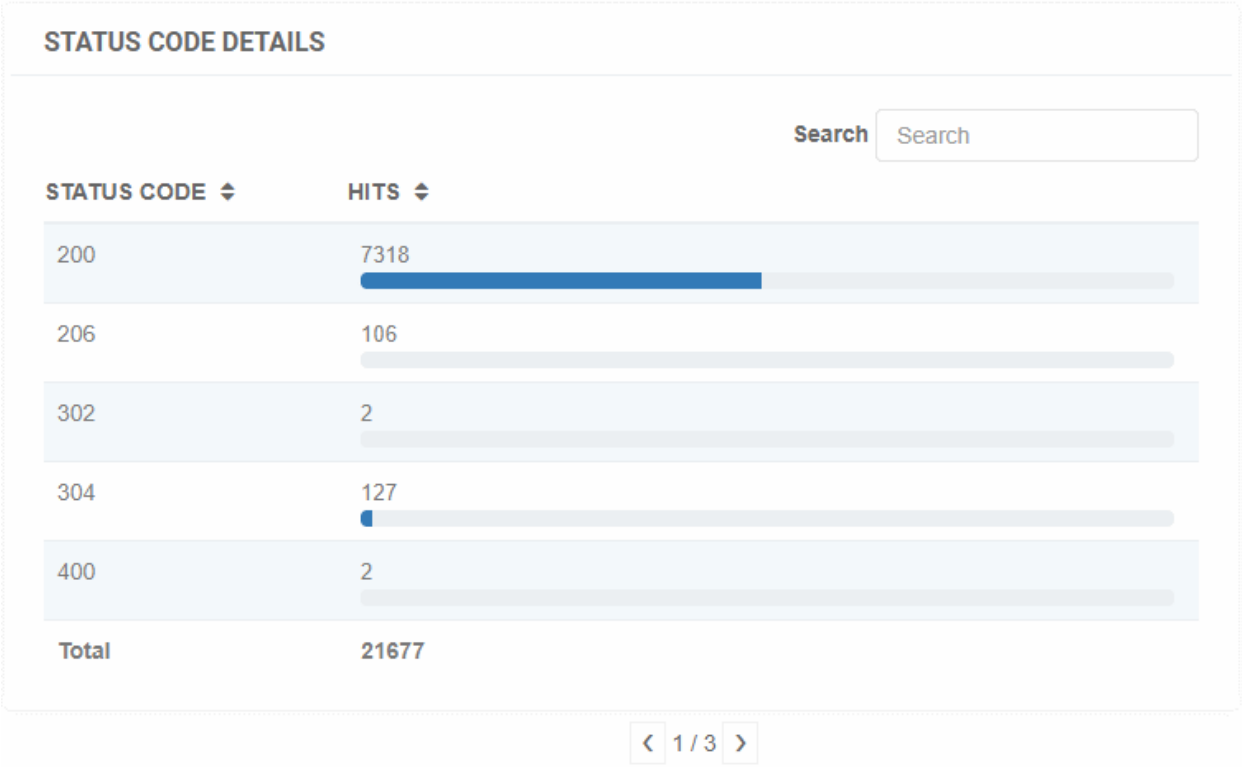
  - 1xx Informational responses.
  - 2xx Success.
  - 3xx Redirection.
  - 4xx Client errors.
  - 5xx Server errors.



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

Status Code Details

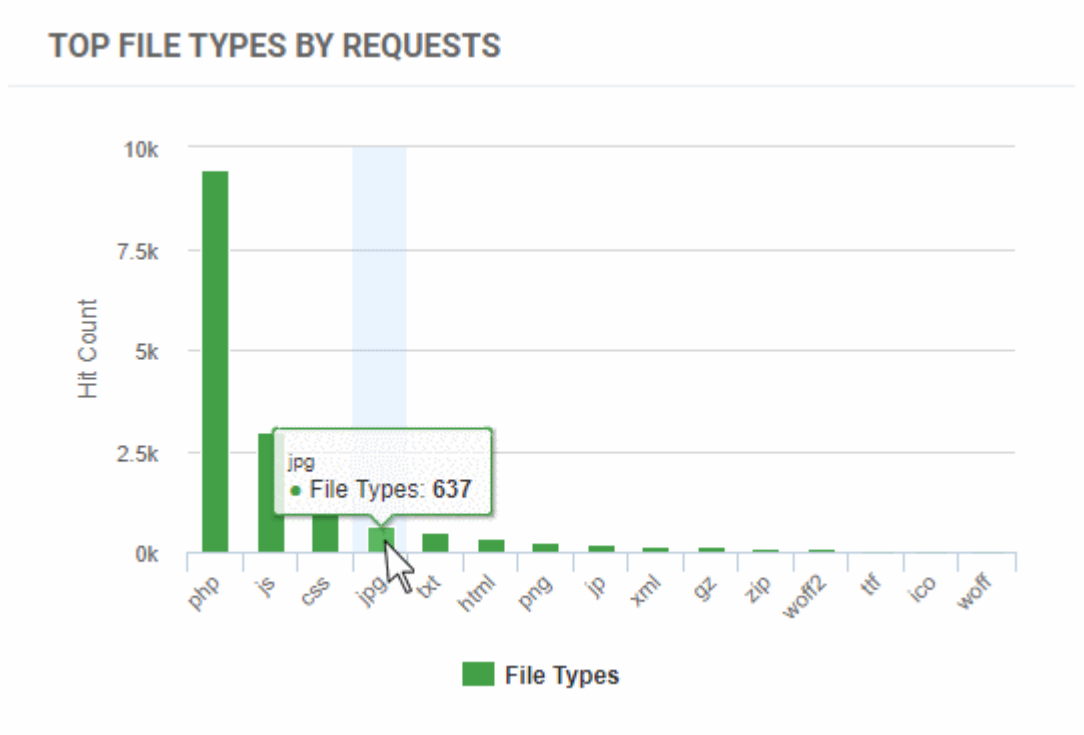
- Precise numbers of HTTP response status codes returned within the selected time period.
- A detailed explanation of each code is available at **https://en.wikipedia.org/wiki/List_of_HTTP_status_codes**.



- 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

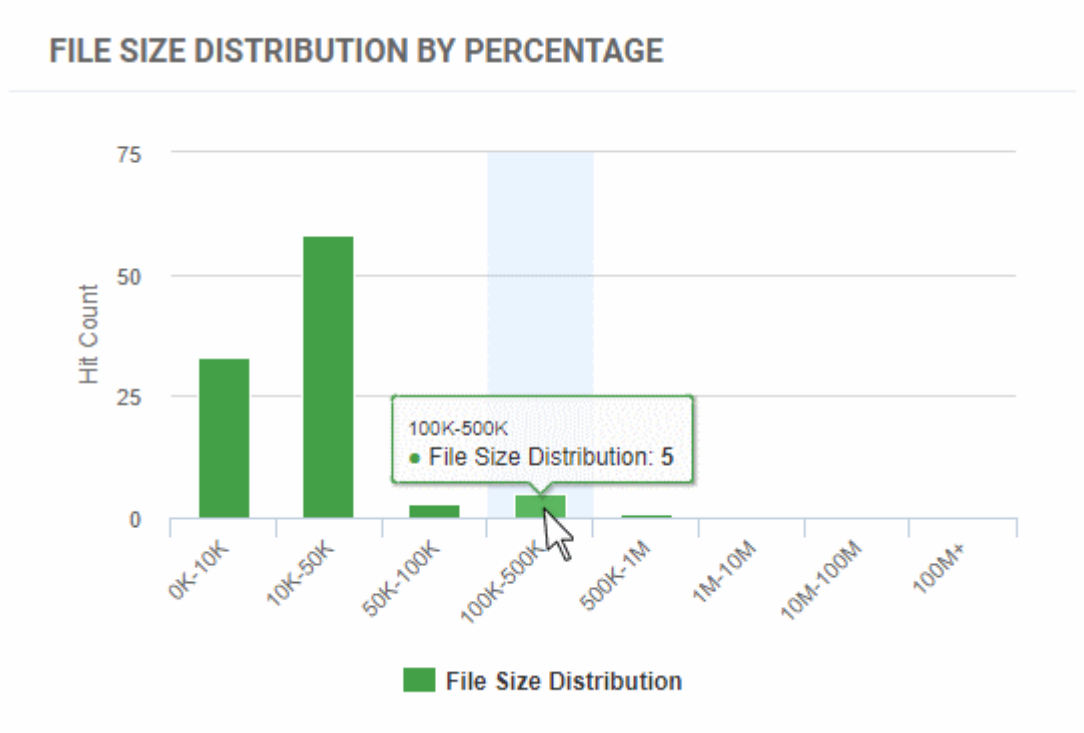
- Shows the different file types requested by your website visitors, and the quantities of each that were downloaded.



- 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

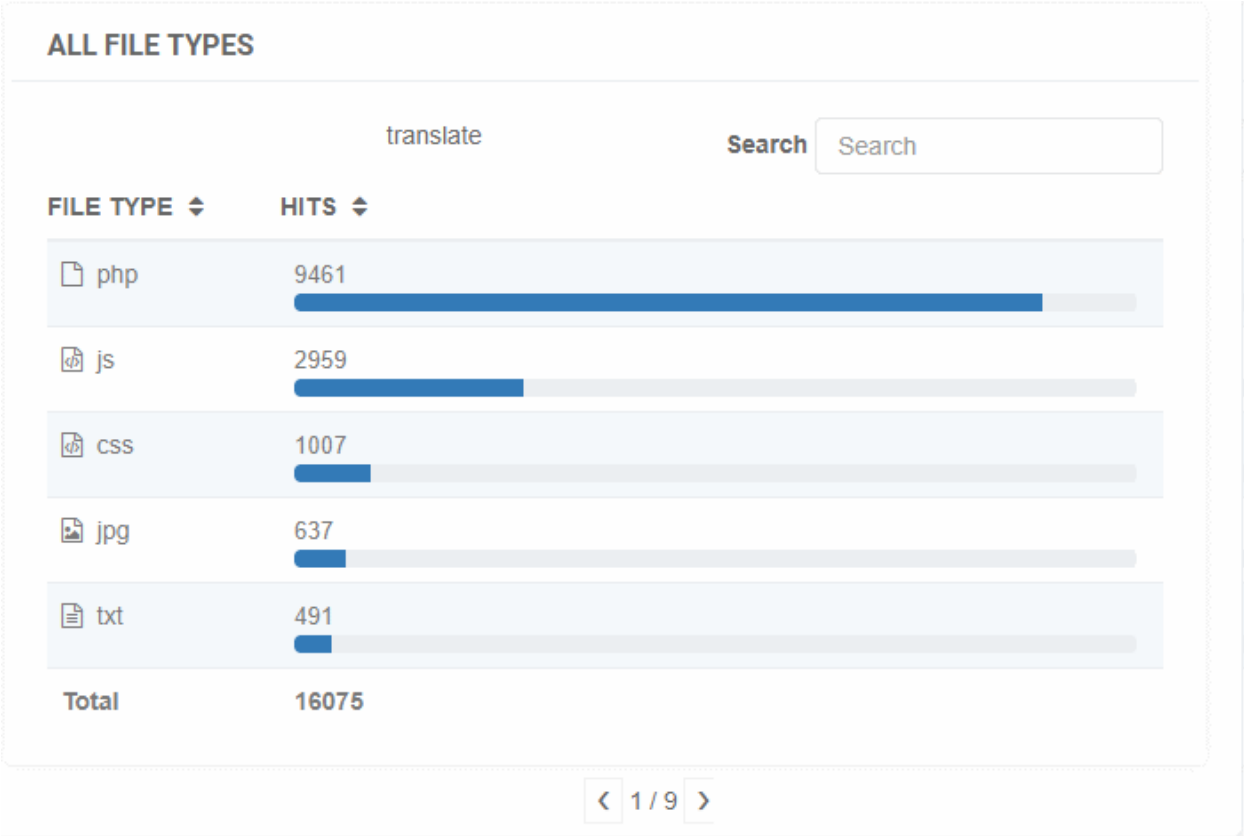
- Shows the number of files in a specific size-range that were requested by your visitors



- 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

4.6 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:

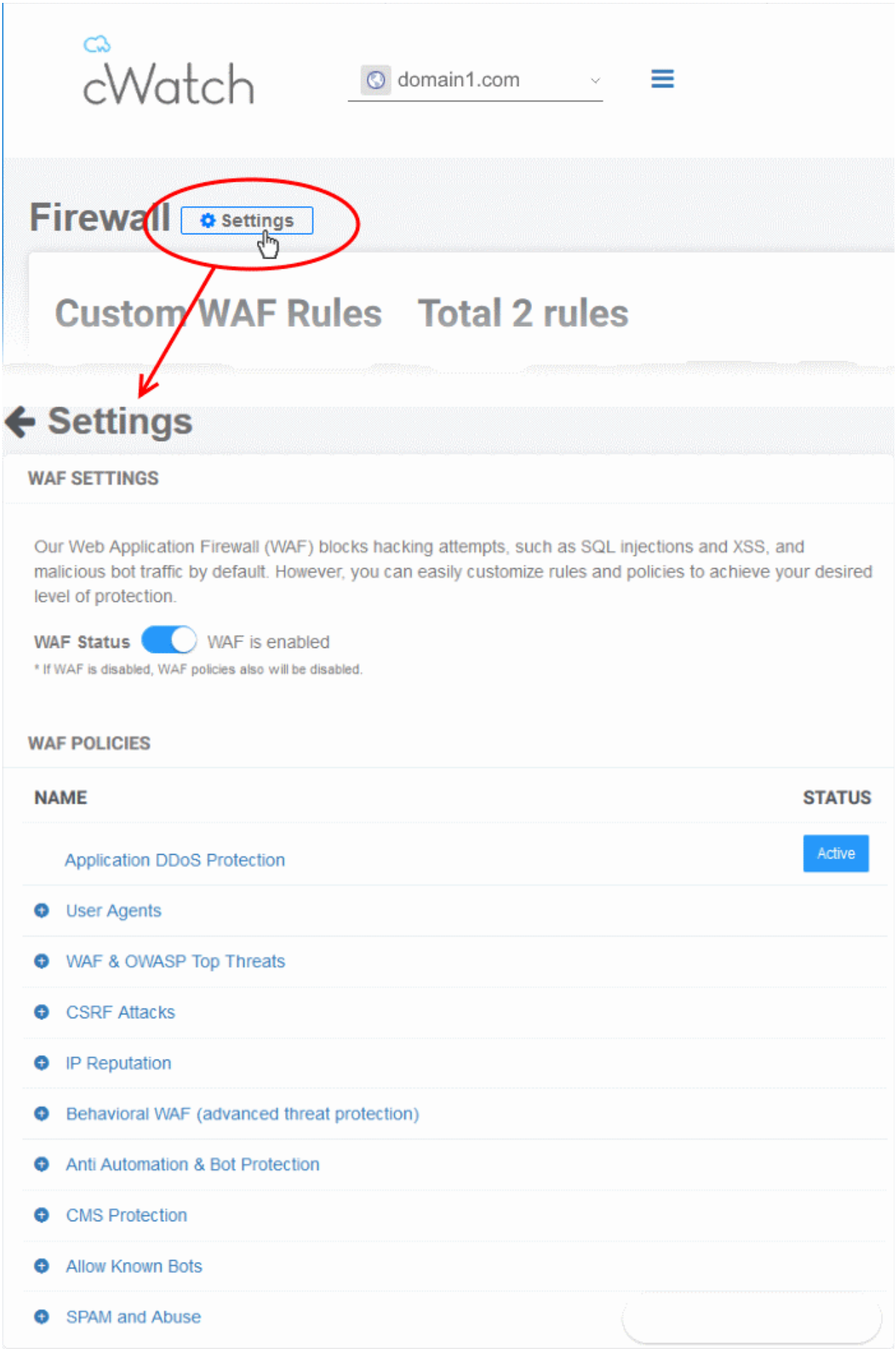
- **Configure WAF Policies**
- **Manage Custom Firewall Rules**

4.6.1 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 that filter traffic and take preventative measures when required. These rules are non-editable.
- You can enable or disable individual rules as required.

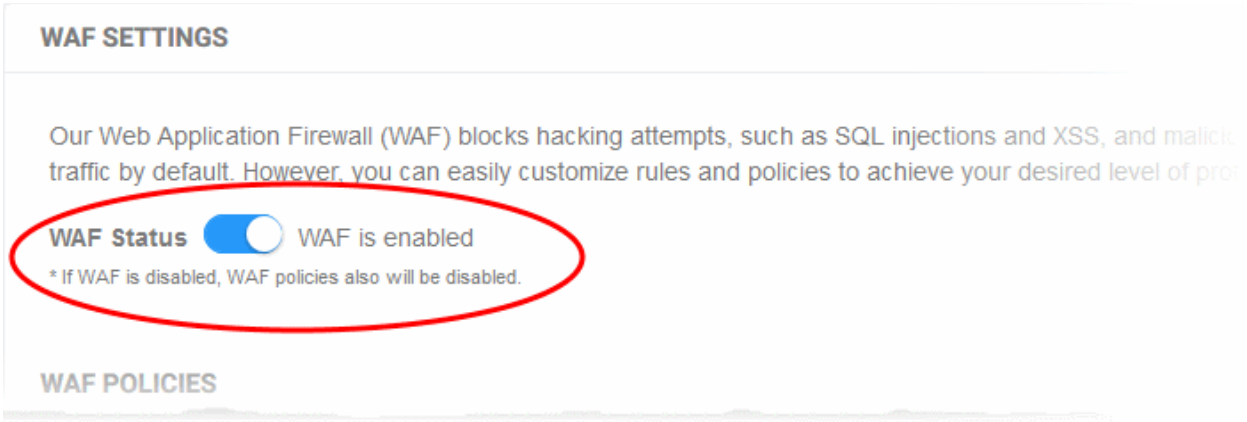
Configure WAF settings

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


cWatch
domain1.com
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

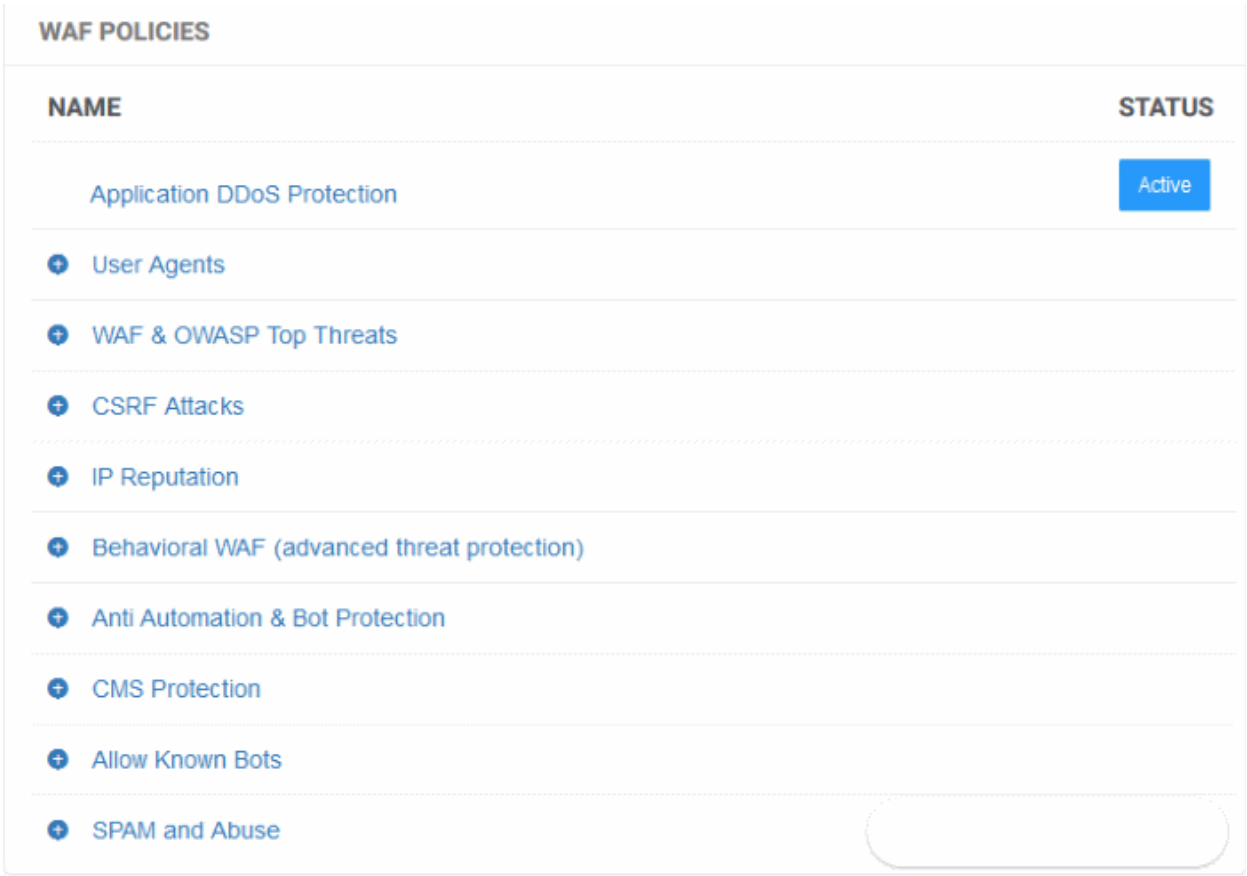
- Use the switch beside 'WAF Status' to enable or disable WAF protection:



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 Polices

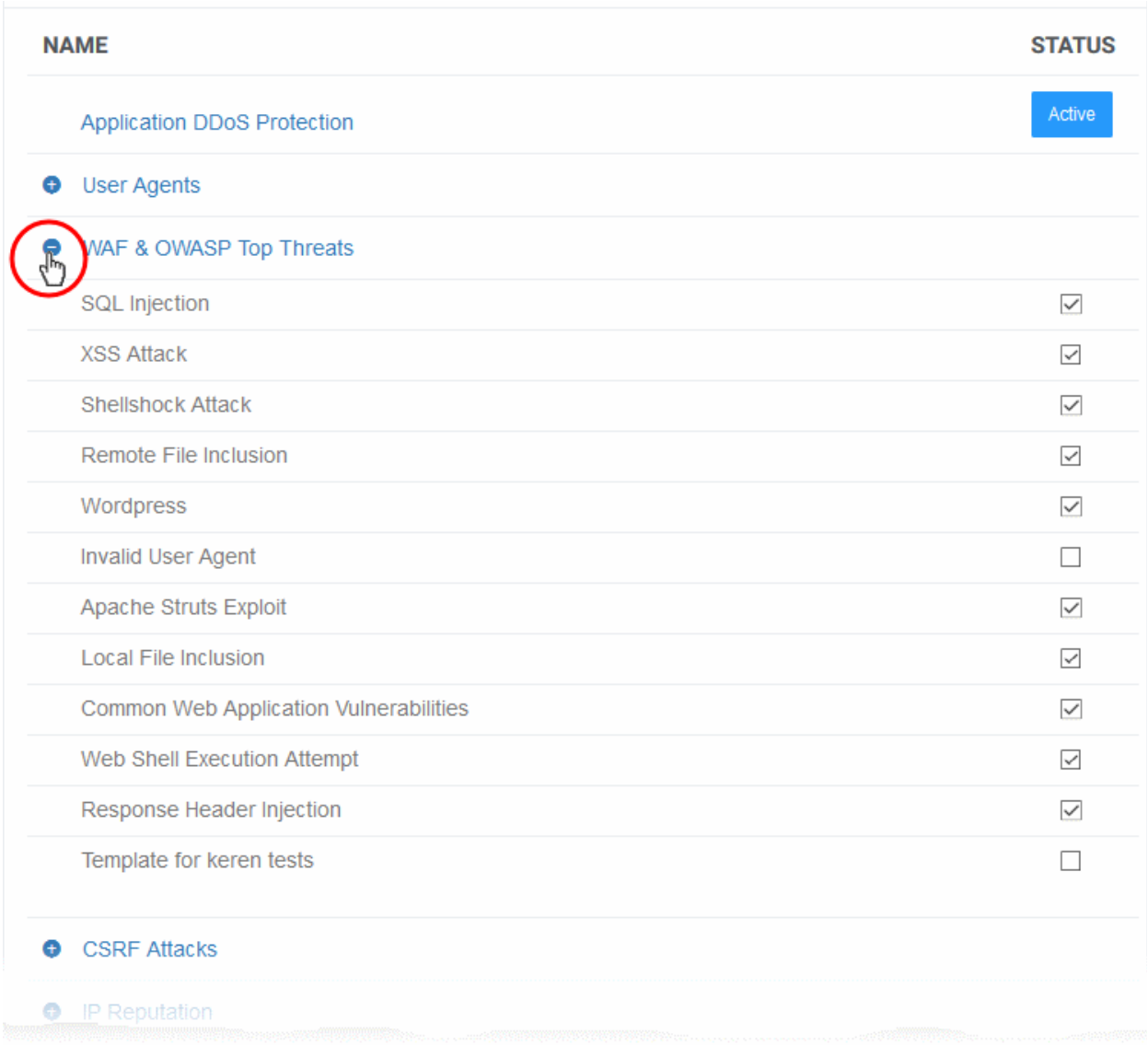
- The 'WAF Policies' area shows a list of all WAF policies.
- Click the '+' symbol to view the constituent rules in a policy. You can enable / disable rules as required.



- **Name** - 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:



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

4.6.2 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.
- These are in addition to the pre-configured firewall policies.
- 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 interface. Action priority is as follows:

1. Monitor
2. Allow
3. Block

4. Captcha

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

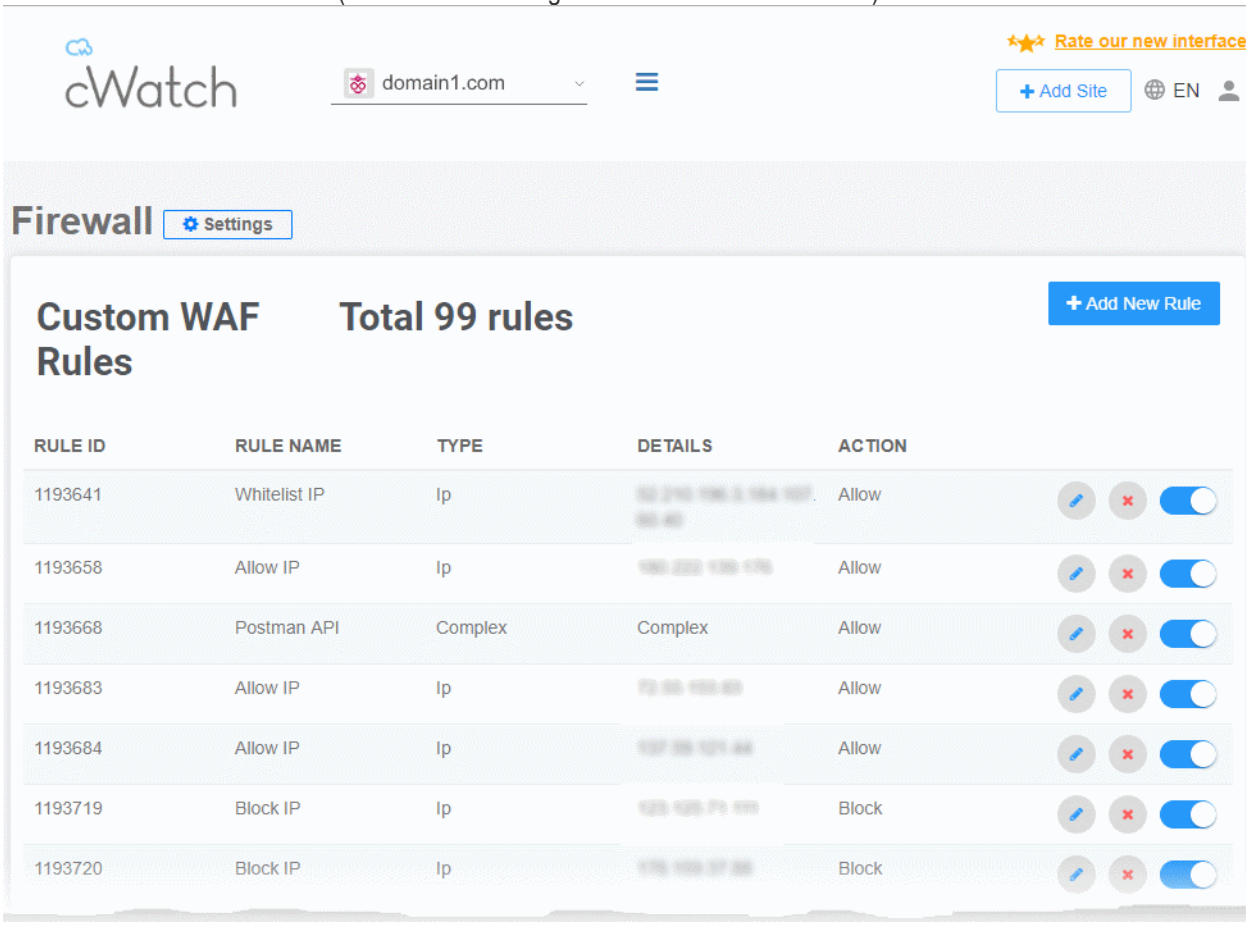
For example, suppose a piece of traffic is covered by three separate rules:

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

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

Open the Firewall 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

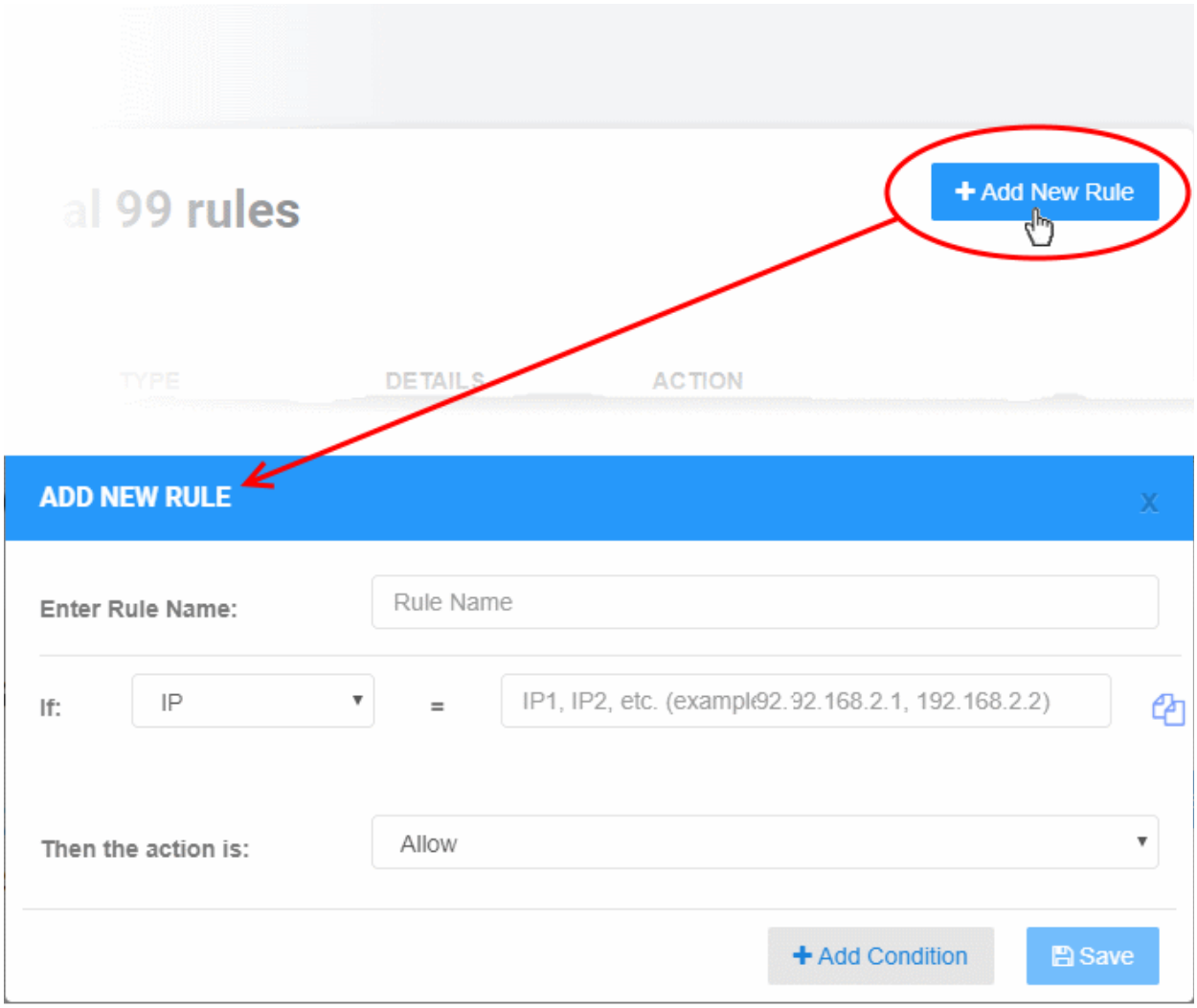
	column shows the two letter country code of the country.
Action	The process the firewall will execute on the target if rule conditions are met. Possible values are: • Allow • Block • Monitor • Captcha
Controls	 - Edit the firewall rule  - Remove the rule  - Enable / disable the rule

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



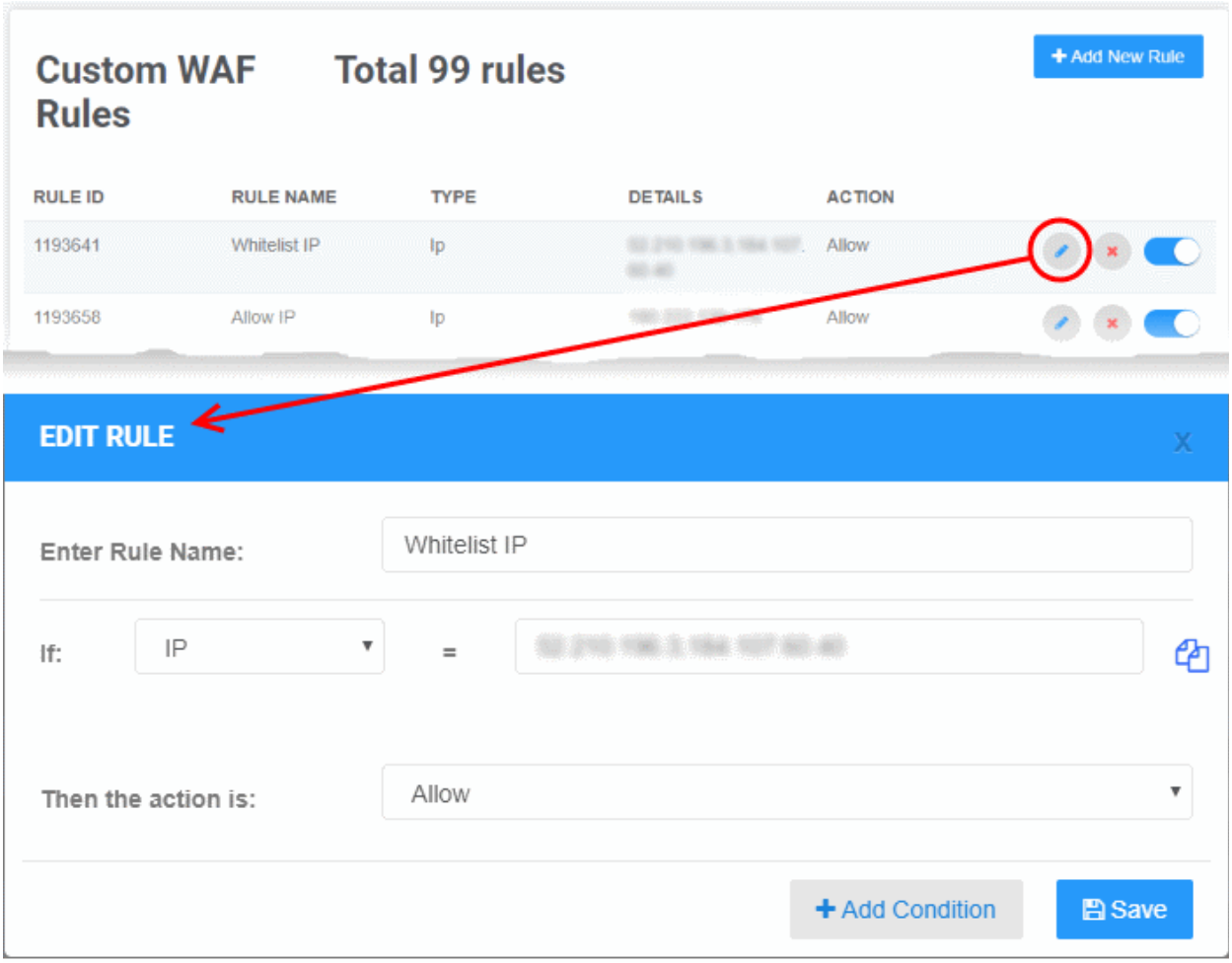
- **Rule Name** - Type a label which describes the rule.
- **Condition 'If'** - Choose the source of the traffic:
  - **IP** - Enter specific IP address(es). For example, 192.168.2.1,192.168.2.2
  - **IP Range** - Enter start and end IP addresses of the IP range to be covered in the 'From' and 'To 'fields
  - **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 '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

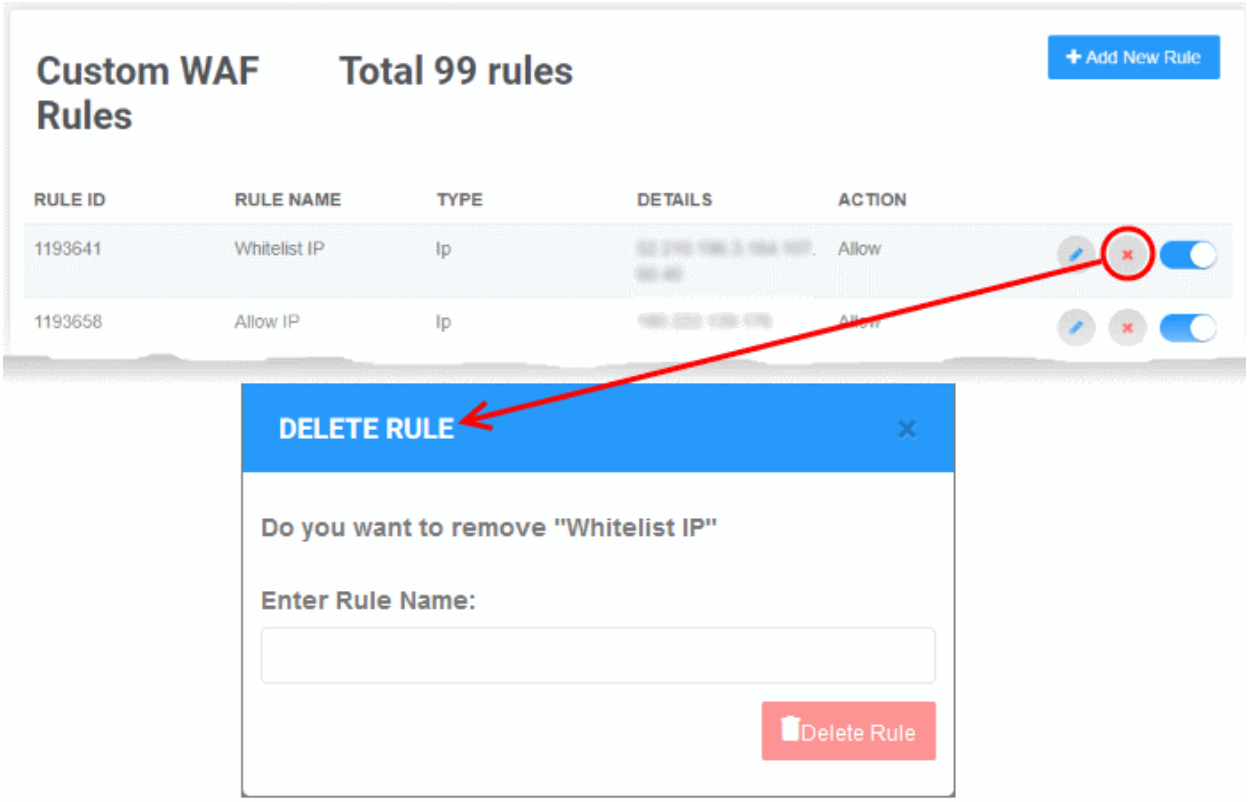
Any new custom firewall rule is enabled by default when added. Rules that need not be triggered can be disabled temporarily and can be enabled when required.

- 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



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

4.7 SSL Configuration

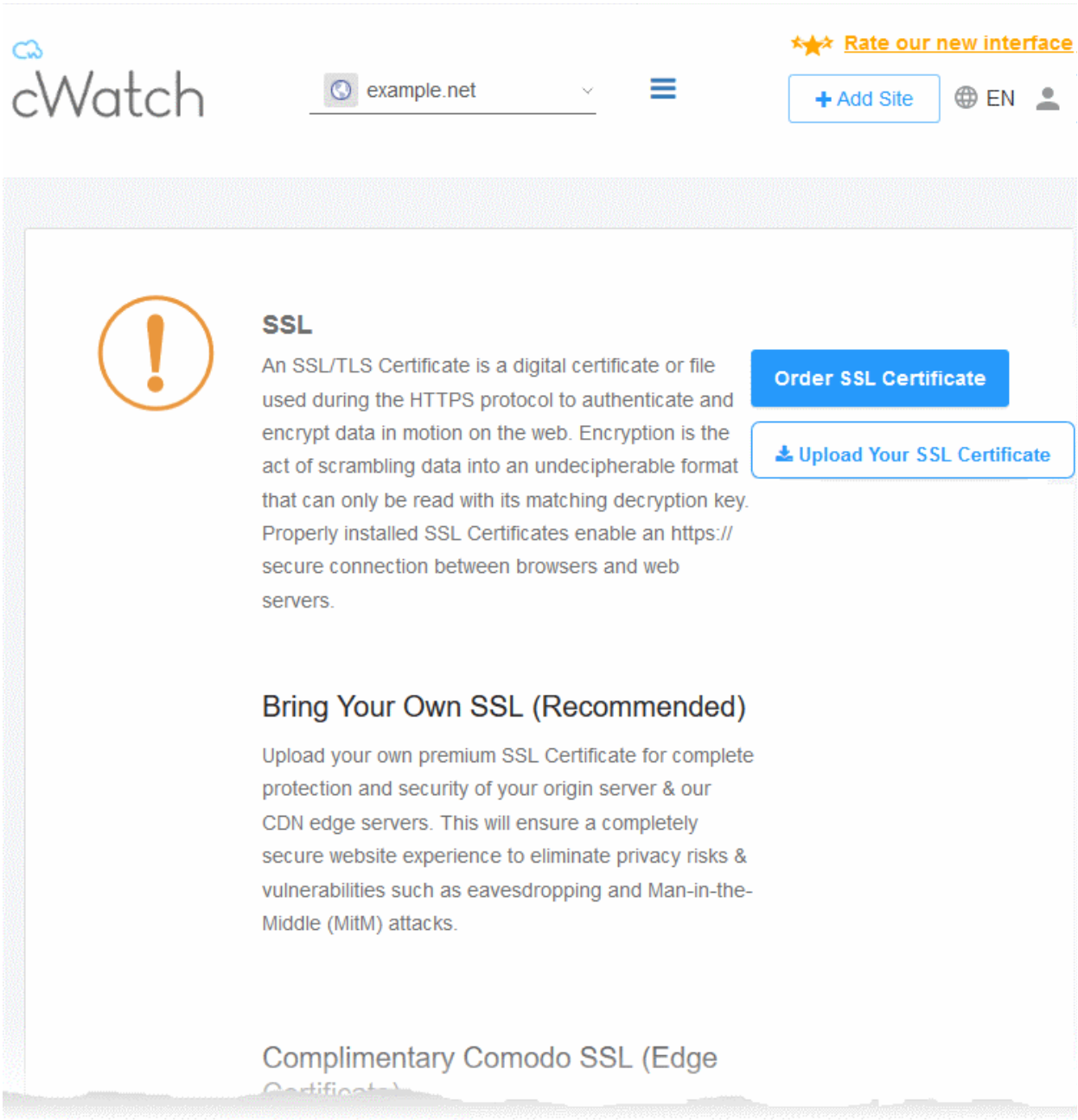
- Select a website from the drop-down at top-left and choose 'SSL'
- An SSL/TLS certificate is placed on a website to identify the domain owner, and to encrypt all data that passes between the site and a visitor's browser.
- Sites that use a SSL/TLS certificate have a URL that begins with HTTPS. For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

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

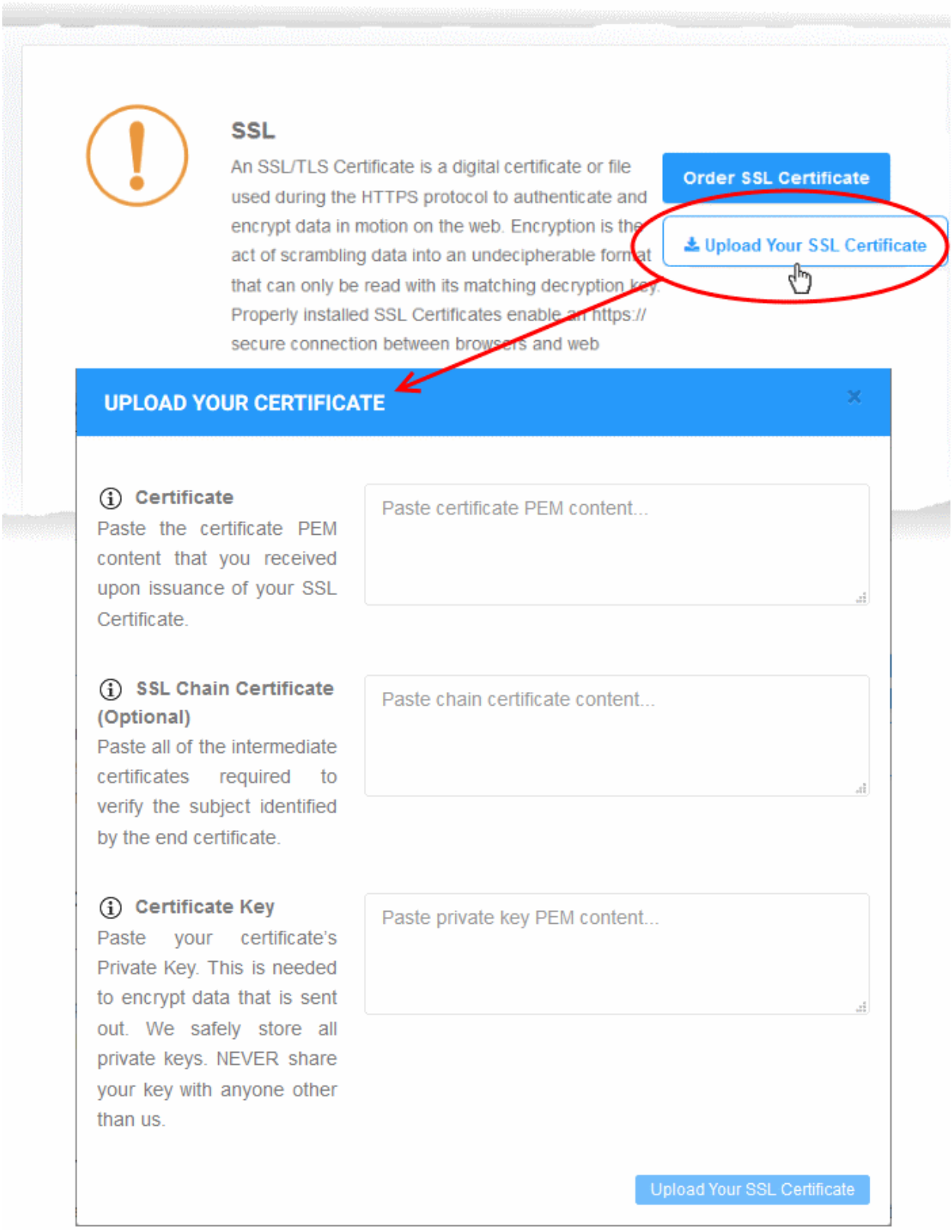
- Bring your own SSL
  - Upload the certificate used on your site to the cWatch CDN edge servers. Recommended for most customers.
  - This will secure the traffic between your site (the origin server) and the cWatch CDN.
  - See **Upload your own SSL Certificate** to find out how to deploy your certificate
- Complimentary Comodo SSL
  - Get a free SSL from Comodo deployed on the CDN Edge servers.
  - You need to configure your site to use Comodo DNS in order to get the free SSL certificate. This can be done in two ways:
    - Change your domain's authoritative DNS servers to Comodo DNS
    - Enter DNS records explicitly
    - Help to configure DNS is available in the section - **Activate CDN for a Website**.
- See **Install Complementary SSL Certificate** to find out how to deploy your free certificate

Upload your own SSL Certificate

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



- 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:



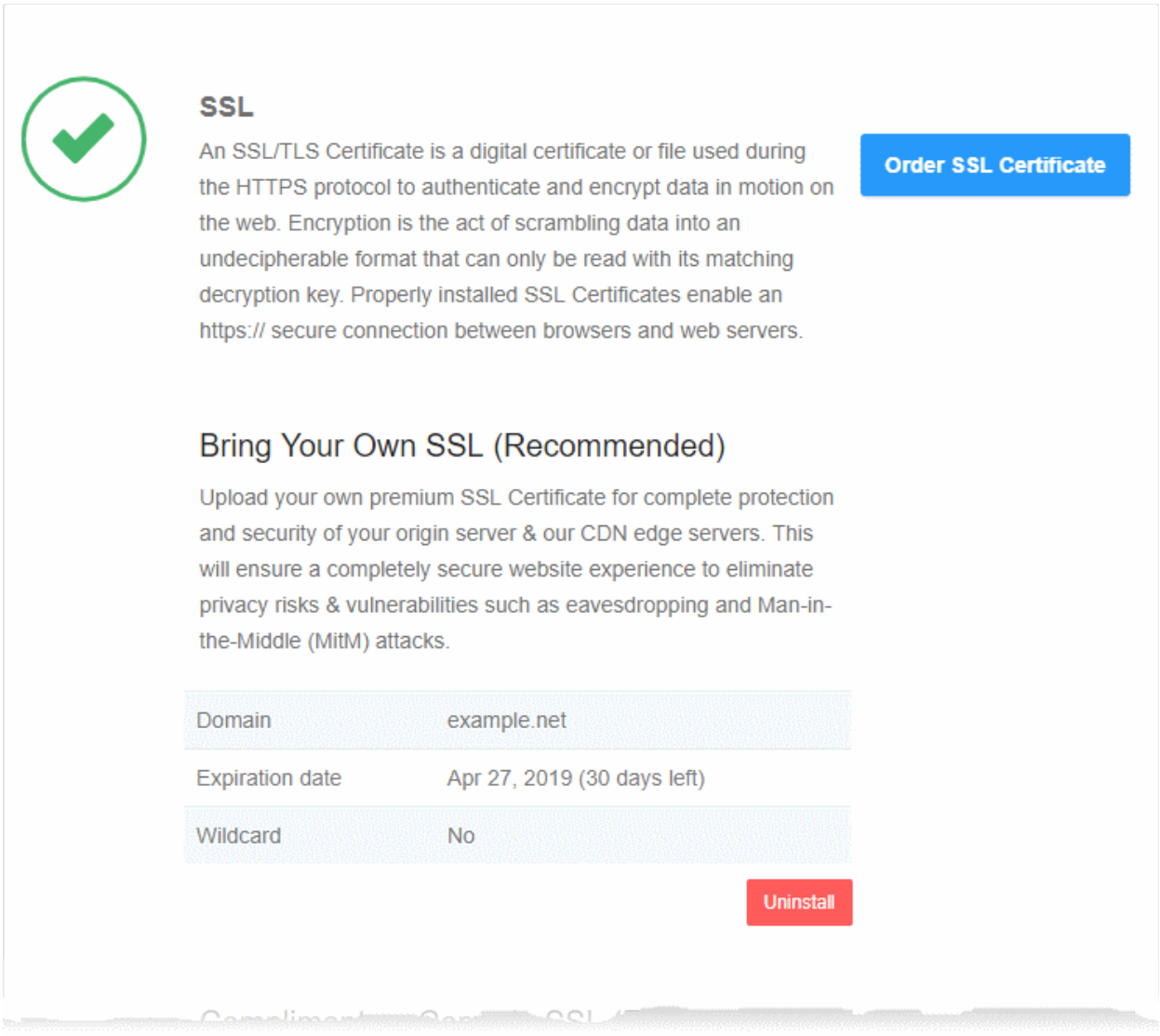
Upload Your Certificate - Form Parameters	
Parameter	**Description**

Certificate	Paste the content of your certificate. The content you are looking for is something like this:
	`-----BEGIN CERTIFICATE-----`
	`MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGE`

Upload Your Certificate - Form Parameters	
Parameter	**Description**
	wJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBAcTAkNOMQswCQYDVQQKEwJPTjELMAkGA 1UECxMC VU4xFDASBgNVBAMTC0hlcm9uZyBZYW5nMB4XDTA1MDcxNTIxMTk0N1oXD TA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAgTAlBOMQswCQYDV QQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTAlVOMRQwEgYDVQQDEwtIZXJvb mcgWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBe wKE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbMOoRcKK9vEcgMtcLFuQTWDl3RA gMBAAGj gbEwga4wHQYDVR0OBBYEFFXI70krXeQDxZgbaCQoR4jUDncEMH8GA1UdI wR4MHaA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMQswCQYDVQQGEwJDTjELM AkGA1UE CBMCUE4xCzAJBgNVBAcTAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECxMCV U4xFDAS BgNVBAMTC0hlcm9uZyBZYW5nggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIh vcNAQEE BQADQQA/ugzBrjjK9jcWnDVfGHlk3icNRq0oV7Ri32z/ +HQX67aRfgZu7KWdI+Ju Wm7DCfrPNGVwFWUQOmsPue9rZBgO -----END CERTIFICATE-----
SSL Chain Certificate	If your certificate contains an intermediate certificate then paste it here. If not, leave this field blank.
Certificate Key	Private key of your certificate

- Click 'Upload Your SSL Certificate'

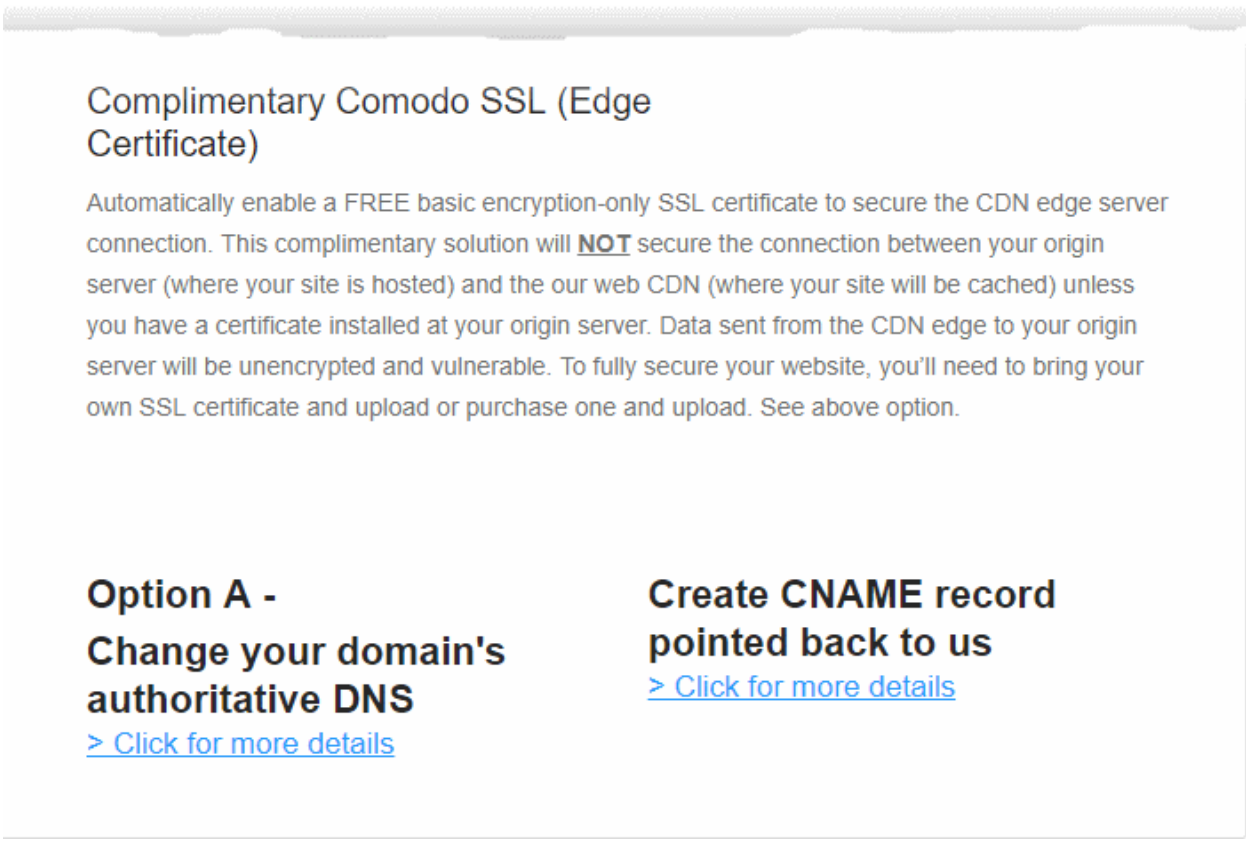
The SSL certificate will be uploaded to the CDN edge servers.



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)':



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

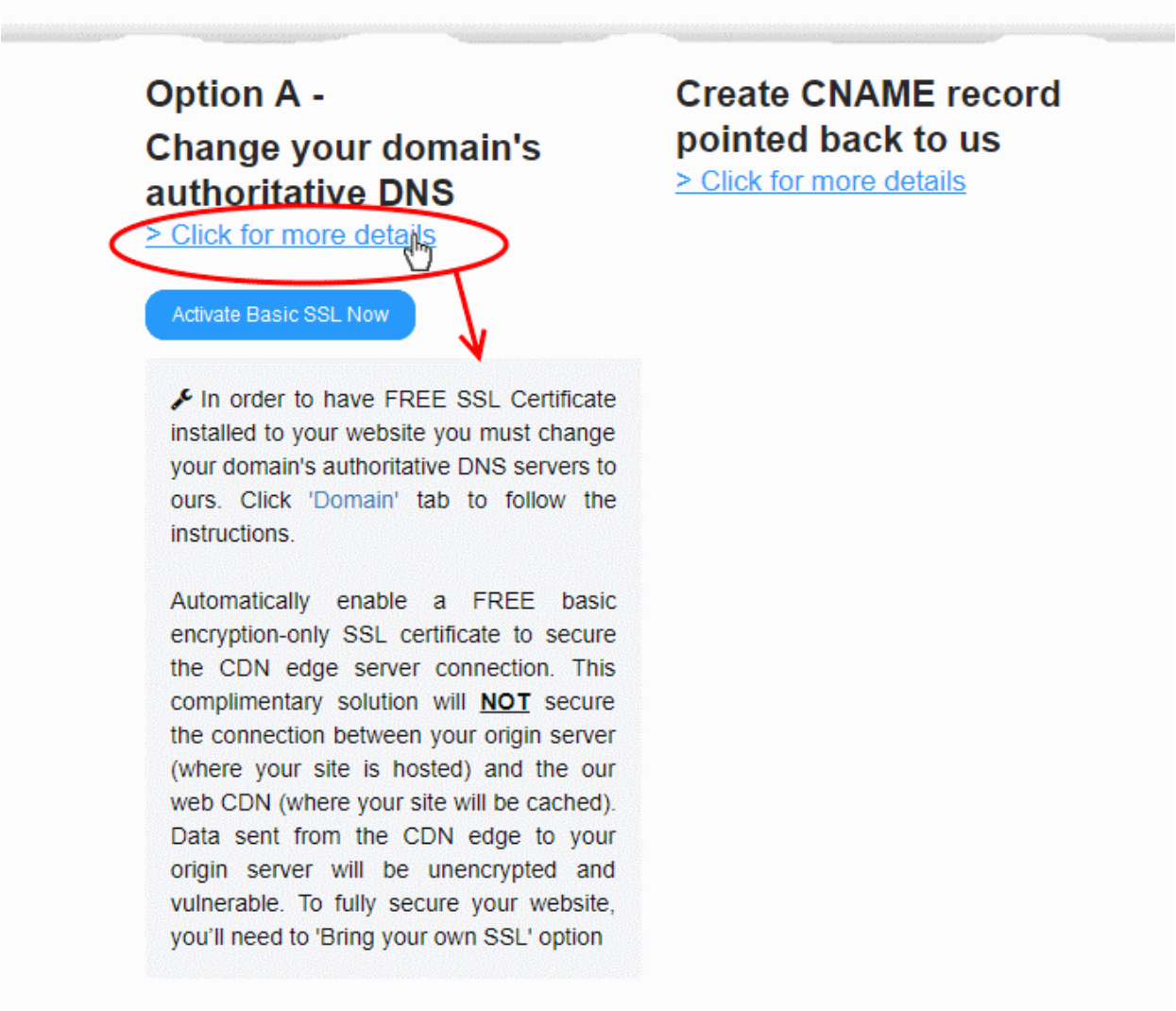
Option A - Change your domain's authoritative DNS servers to Comodo

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

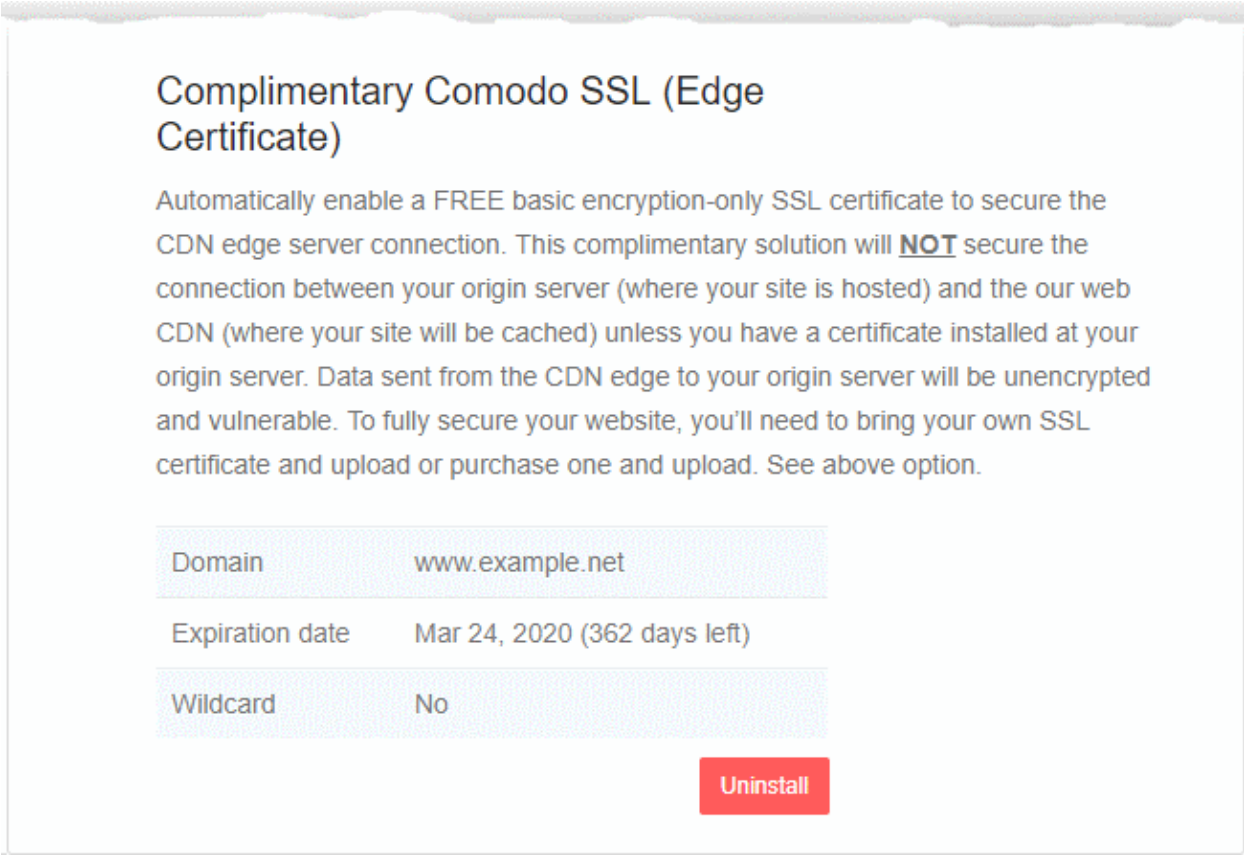
- The NS records are available in 'CDN' > 'Settings' > 'Activation', and in the 'DNS' pages of the site.

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'



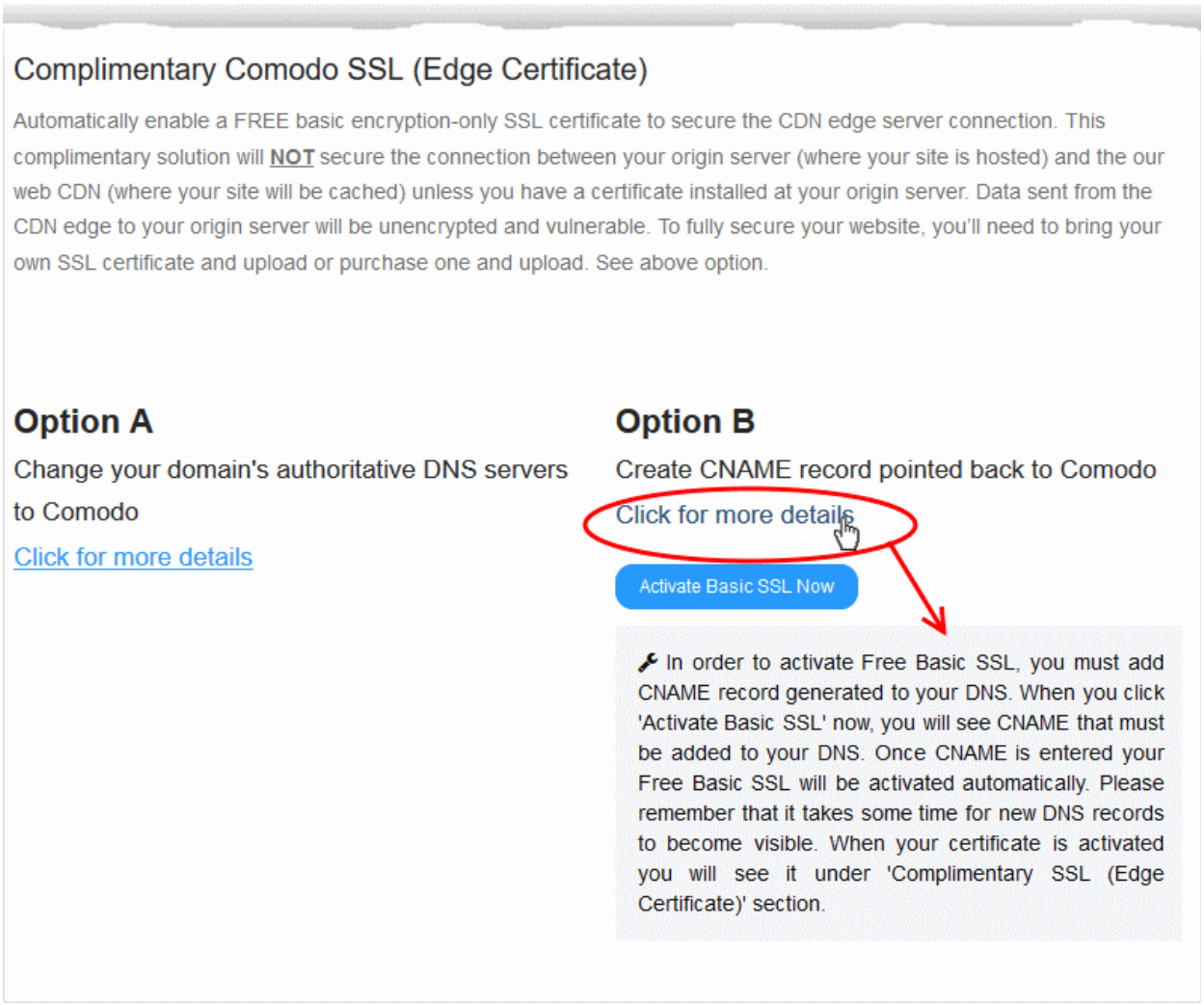
- Click the 'Activate Basic SSL Now' button
- The process will take a few minutes to complete.
- Once activated, you can see the certificate in 'Settings' > 'SSL', listed under 'Complimentary Comodo SSL (Edge Certificate)'.



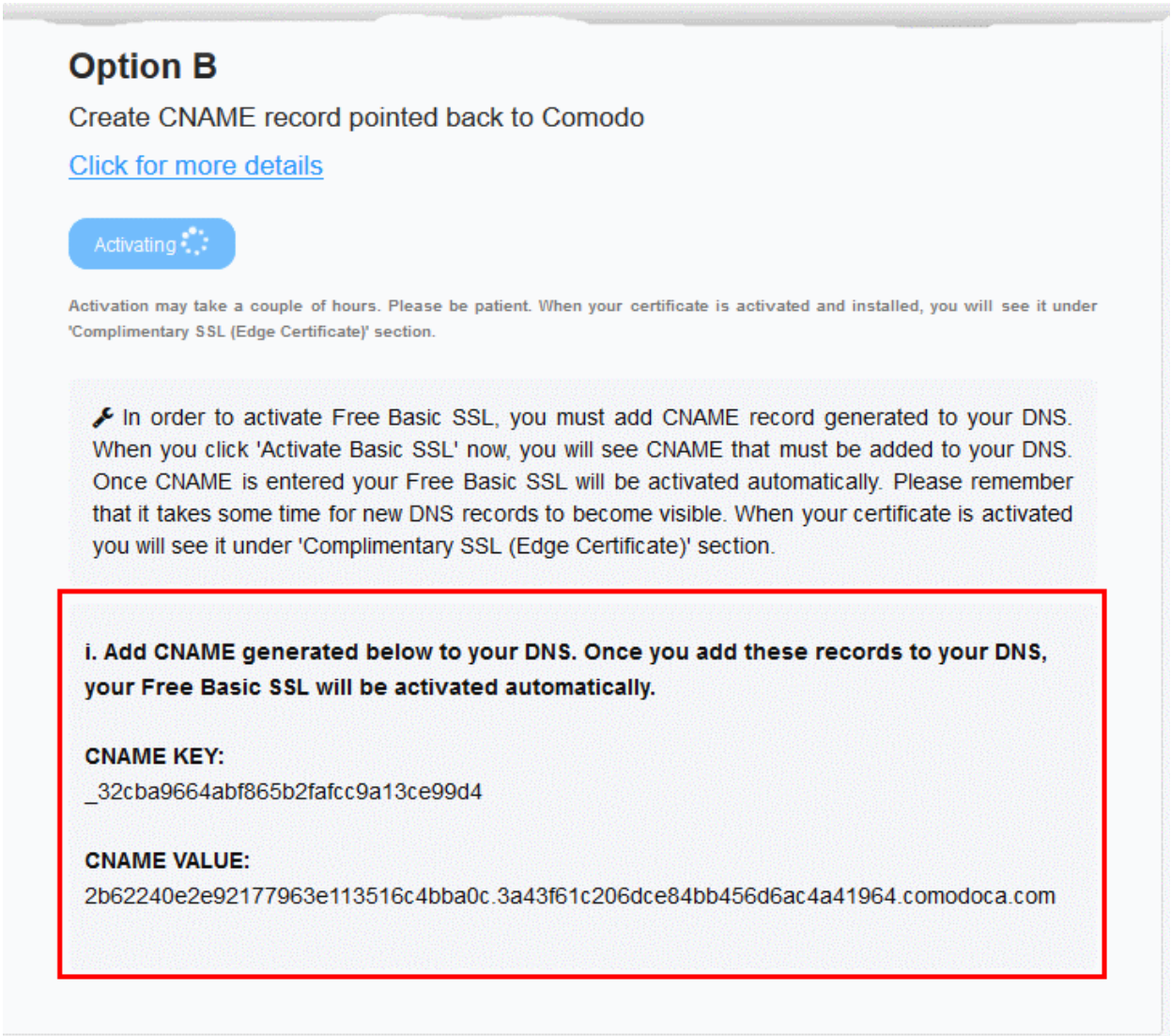
- The certificate is valid for one year and is set for auto-renewal.
- Note - This certificate encrypts the connection between the CDN servers, which host a copy of your site, and your website visitors.
- It does not encrypt the traffic between your web-server and the CDN edge servers.
- You need to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

Option B - Create a CNAME record which points to Comodo

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



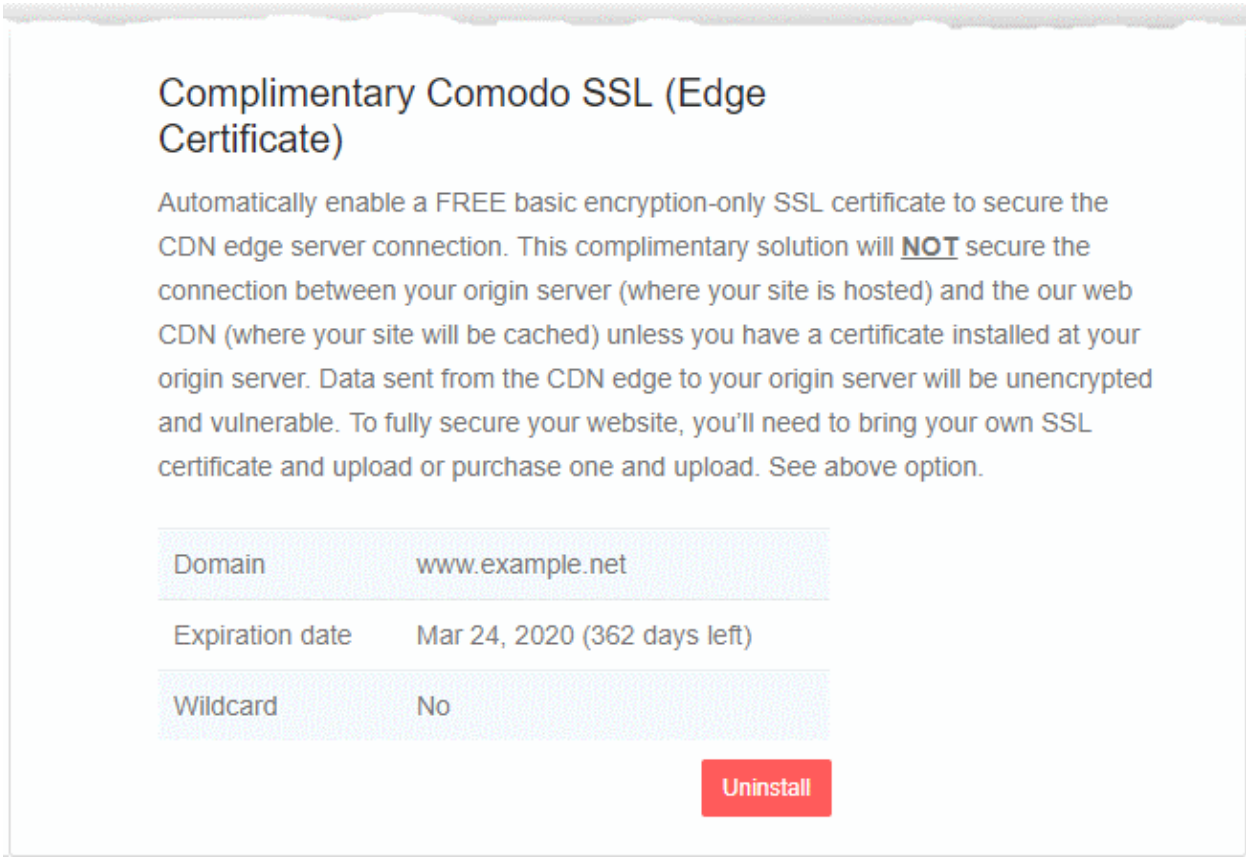
- Click the 'Activate Basic SSL Now' button:



cWatch generates a CNAME record for domain control validation.

- 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)'.



- 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.

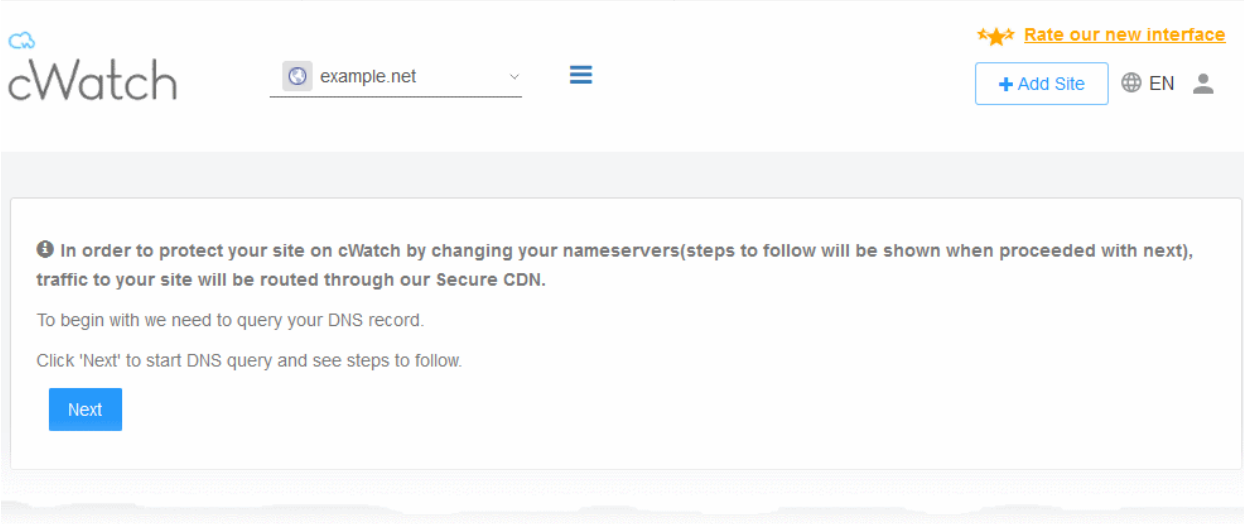
4.8 DNS Configuration

- 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 in order to enable cWatch protection, the content delivery network, and the Web Application Firewall (WAF).
    - The DNS page shows the authoritative name servers (NS) for your site. You can use these to configure the DNS settings.
- After switching to Comodo DNS, you should use this page for overall DNS management, instead of your web host's DNS management page. For example, you can add new 'CNAME' and 'A' records, change MX records and more.
- The following sections explain how to:
    - **Configure DNS settings of your website**
    - **Manage DNS Records of your website**

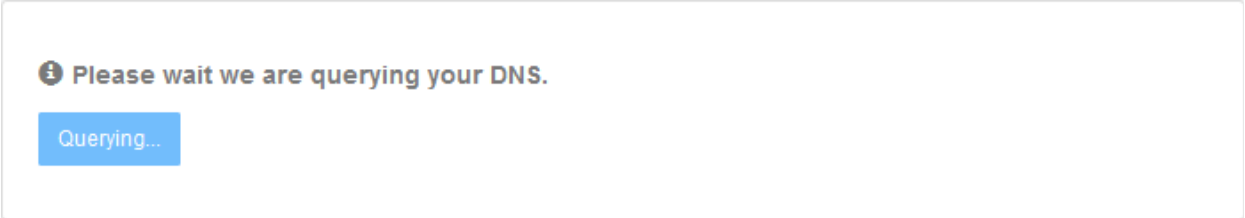
Configure DNS settings on your site

- 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')

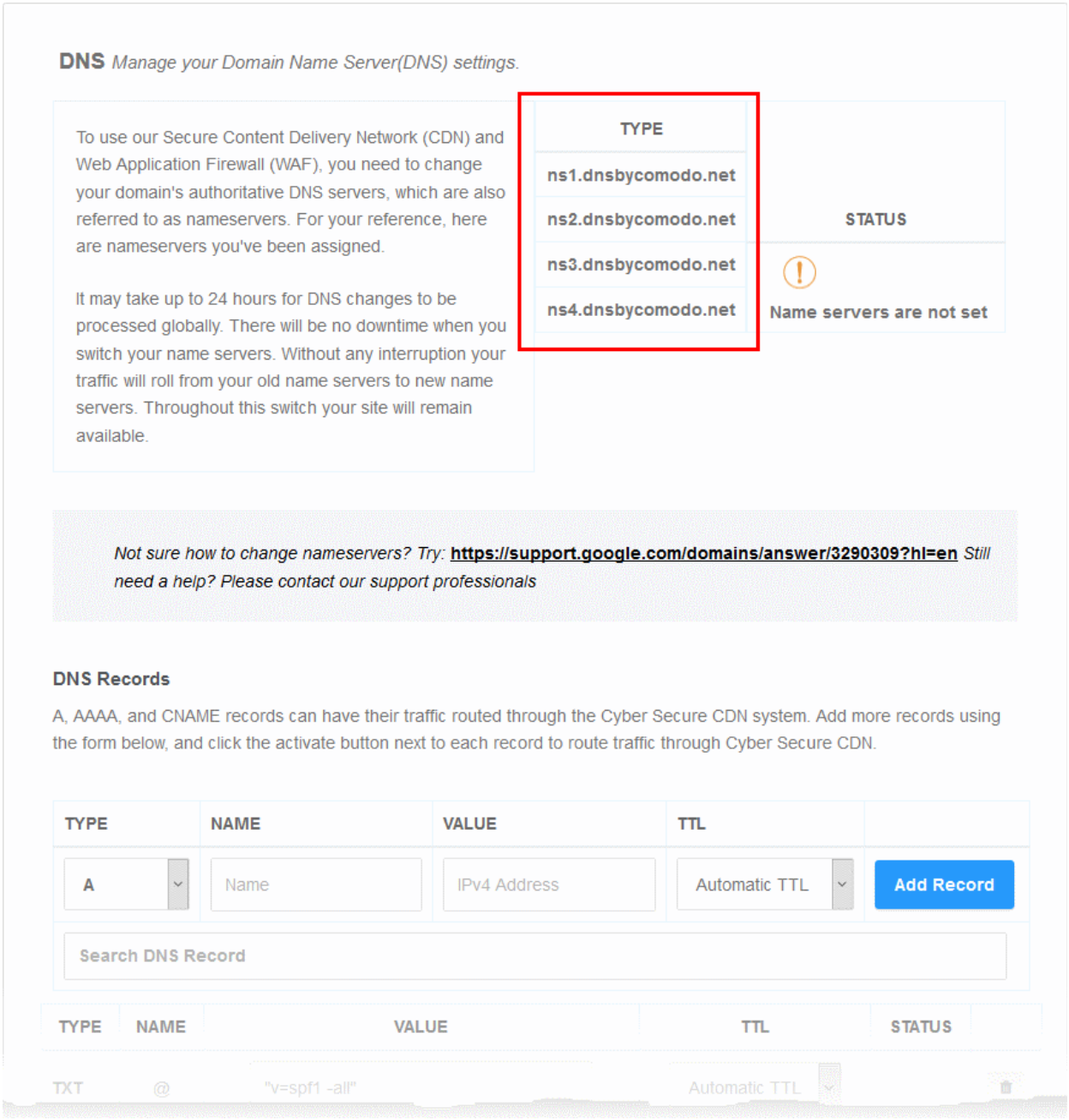
cWatch first queries your DNS servers to collect your existing records:



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



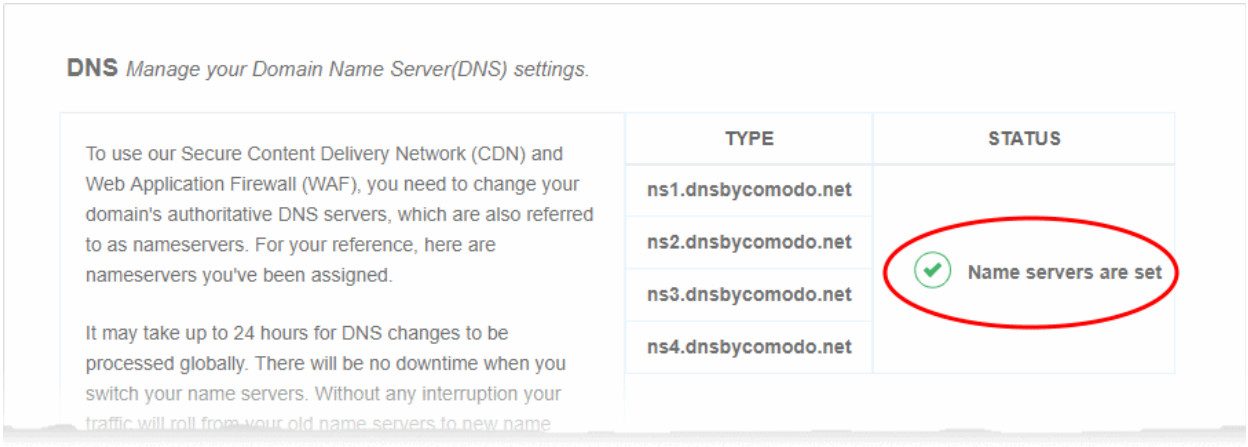
The DNS configuration page for the site will then load, complete with the site's name server (NS) details:



- 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:



- 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

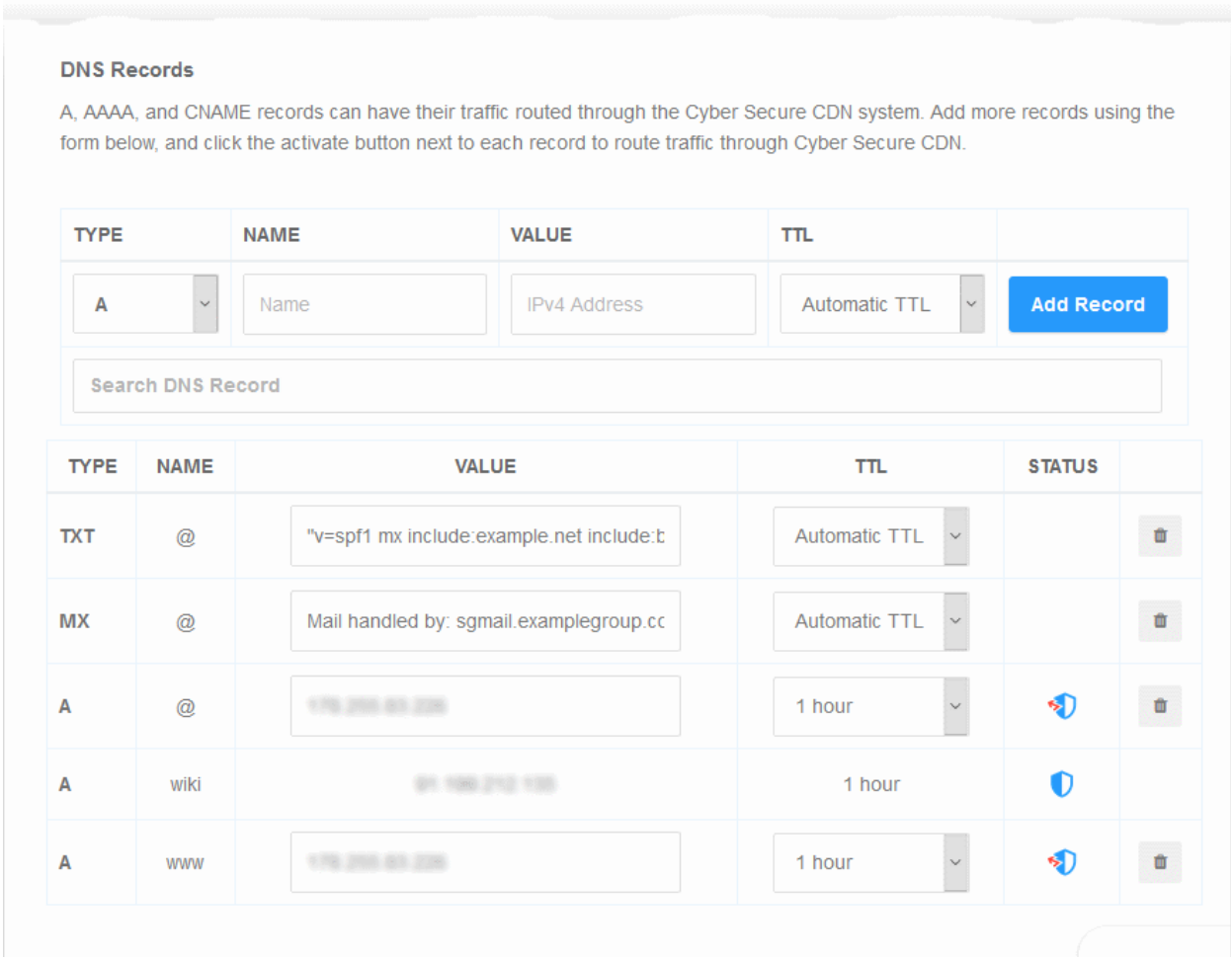
Note - you can only manage DNS records in cWatch if your nameservers are pointed to Comodo.

- 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 - 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	Whether the record is protected or not. - The record is protected. • Click the icon to remove the site from cWatch - The record is not protected. • Click the icon to add the record to cWatch for protection • See **Configure cWatch protection for a site** for guidance on this Note - protection is available for CNAME and A records if not already enrolled to cWatch.

Add a DNS record

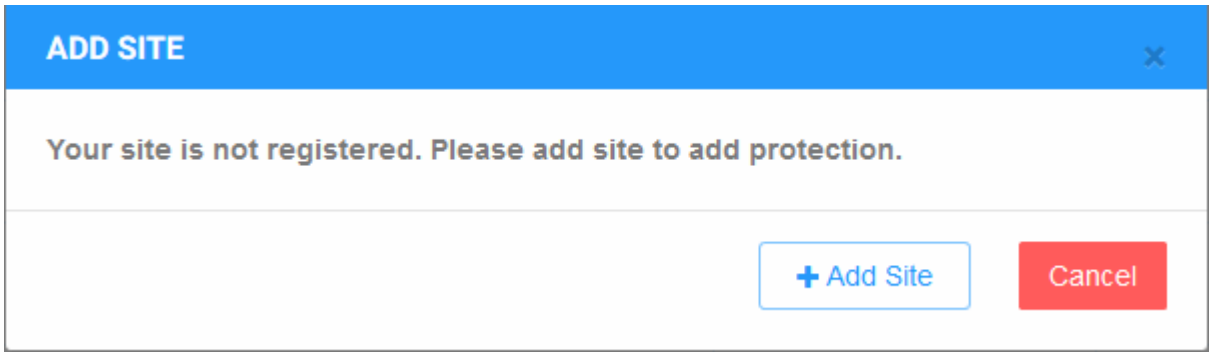
- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'DNS' tab (or click the hamburger button and select 'DNS')
- Scroll down to the 'DNS Records' pane
- Configure the following items:
  - Type - Select the kind of the DNS record from the drop-down
  - Name - 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.

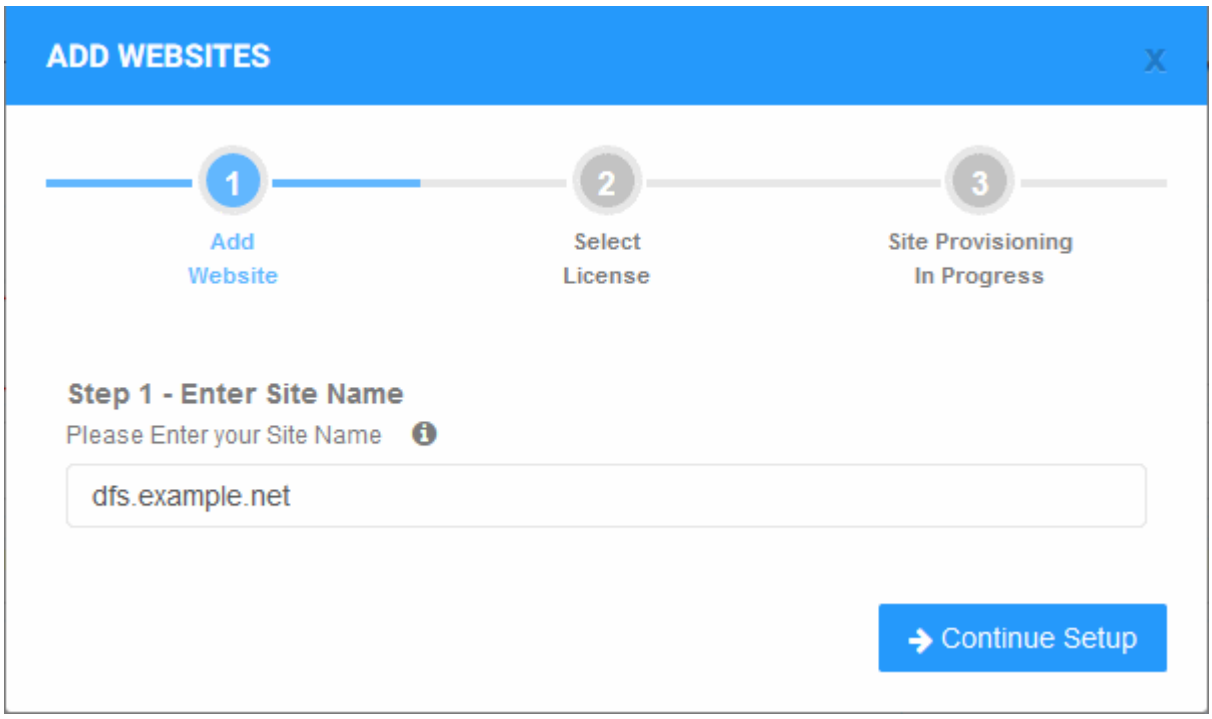
- See **https://support.google.com/domains/answer/3290309?hl=en** if you need more help to change nameservers.

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.

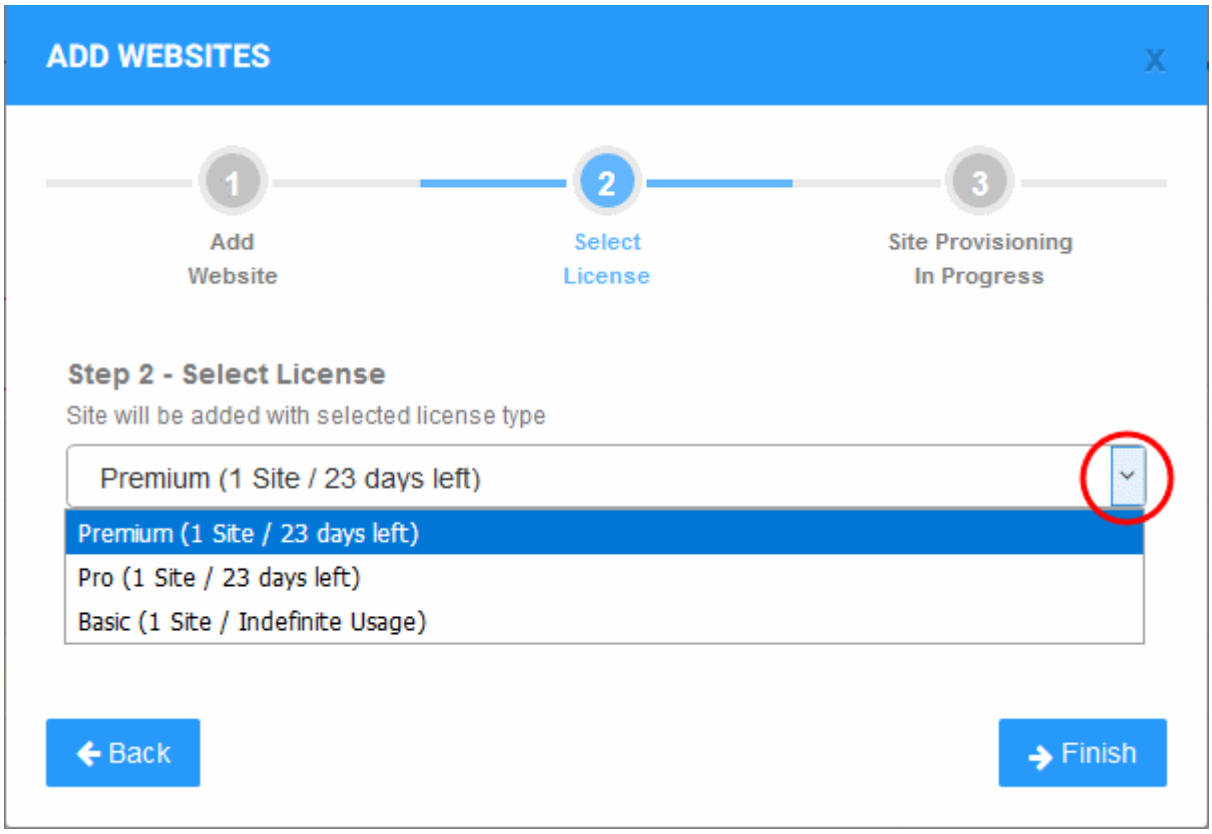


- Click 'Add Site' to start the 'Add Websites' wizard.

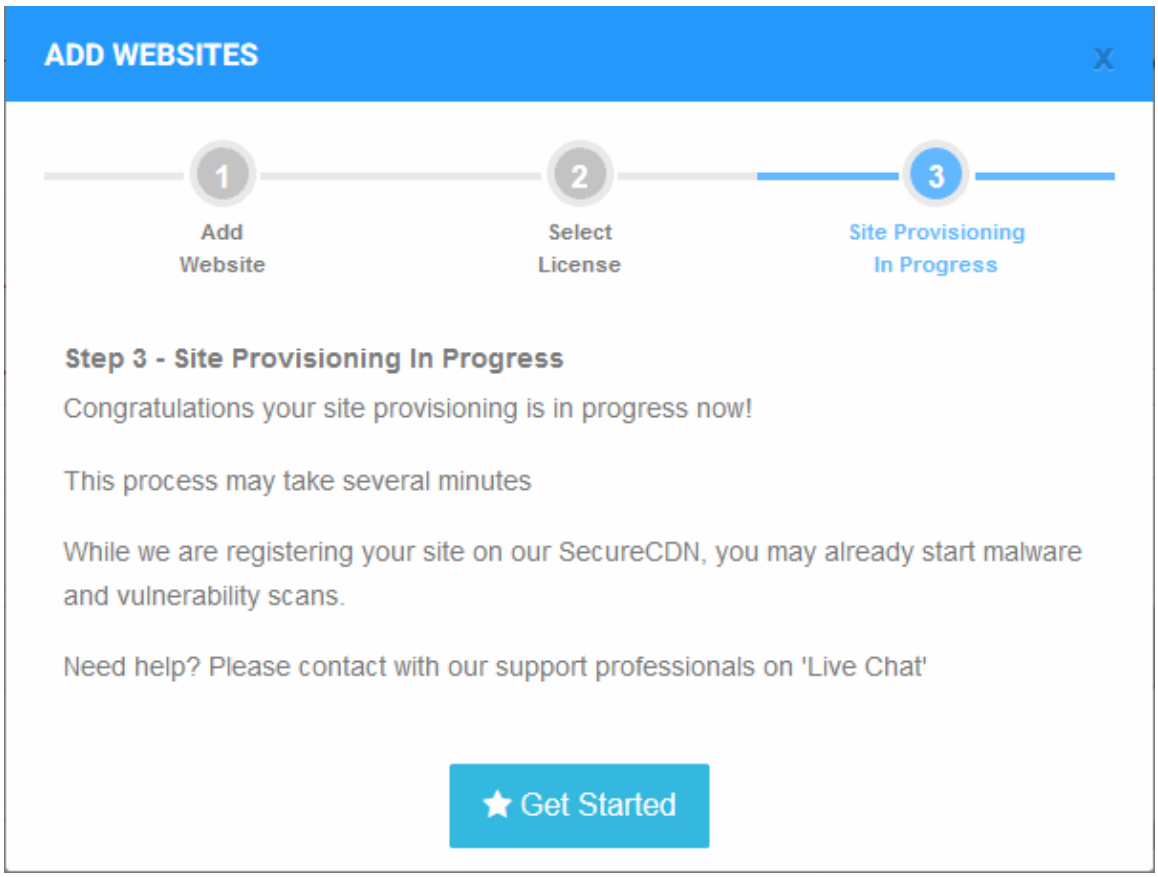


The website name is pre-populated.

- 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.

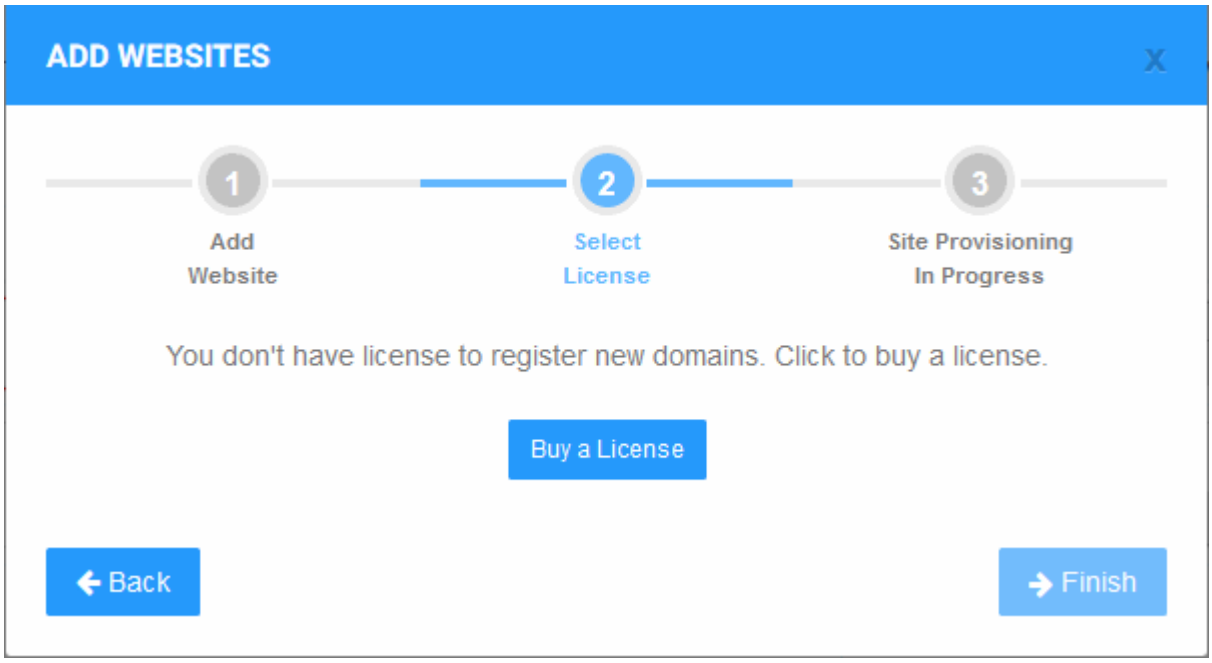


- Click 'Finish' to apply the license. The site will be registered.
- cWatch will validate your request then show the following confirmation message:

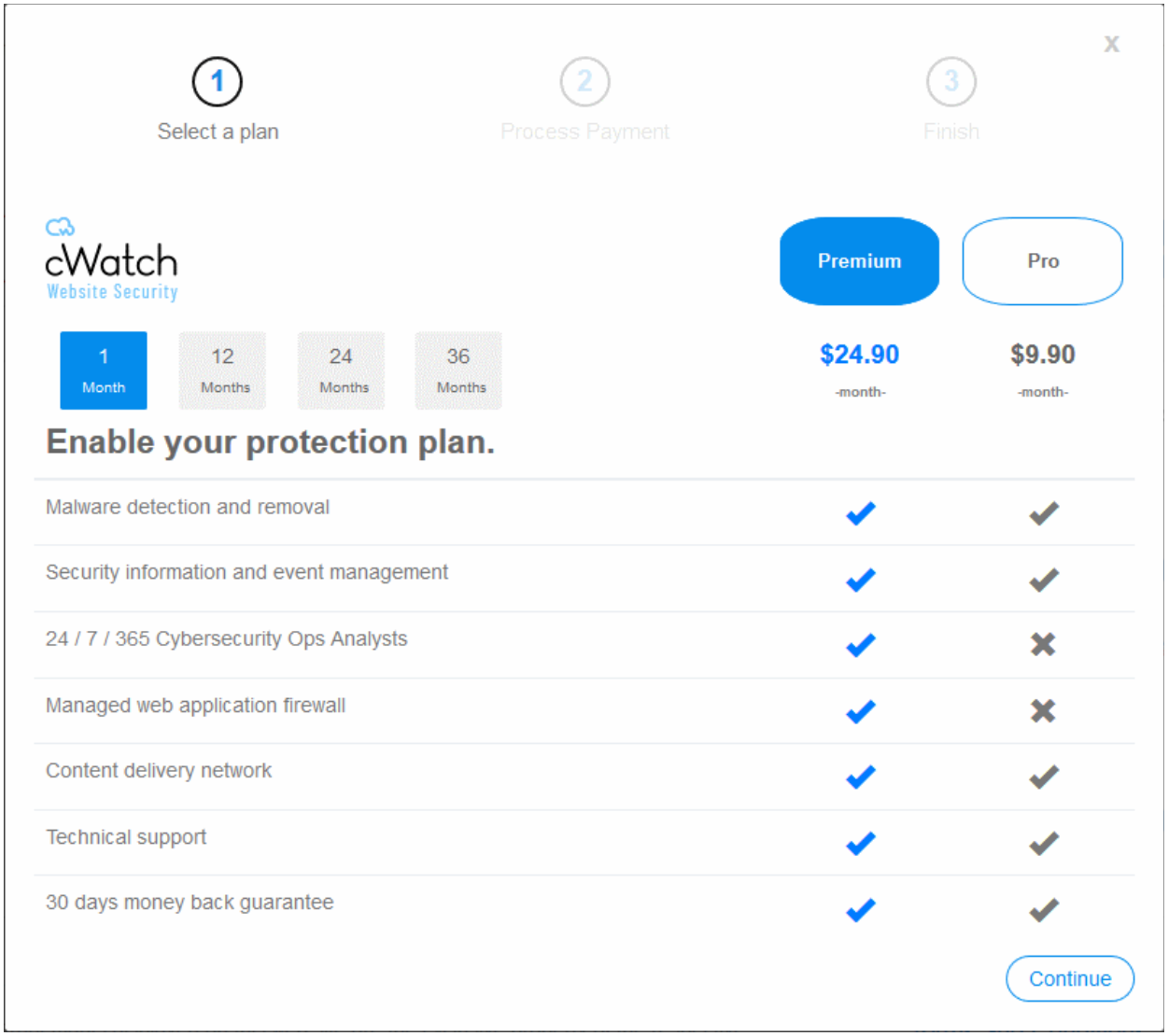


- Click 'Get Started' to activate cWatch protection.

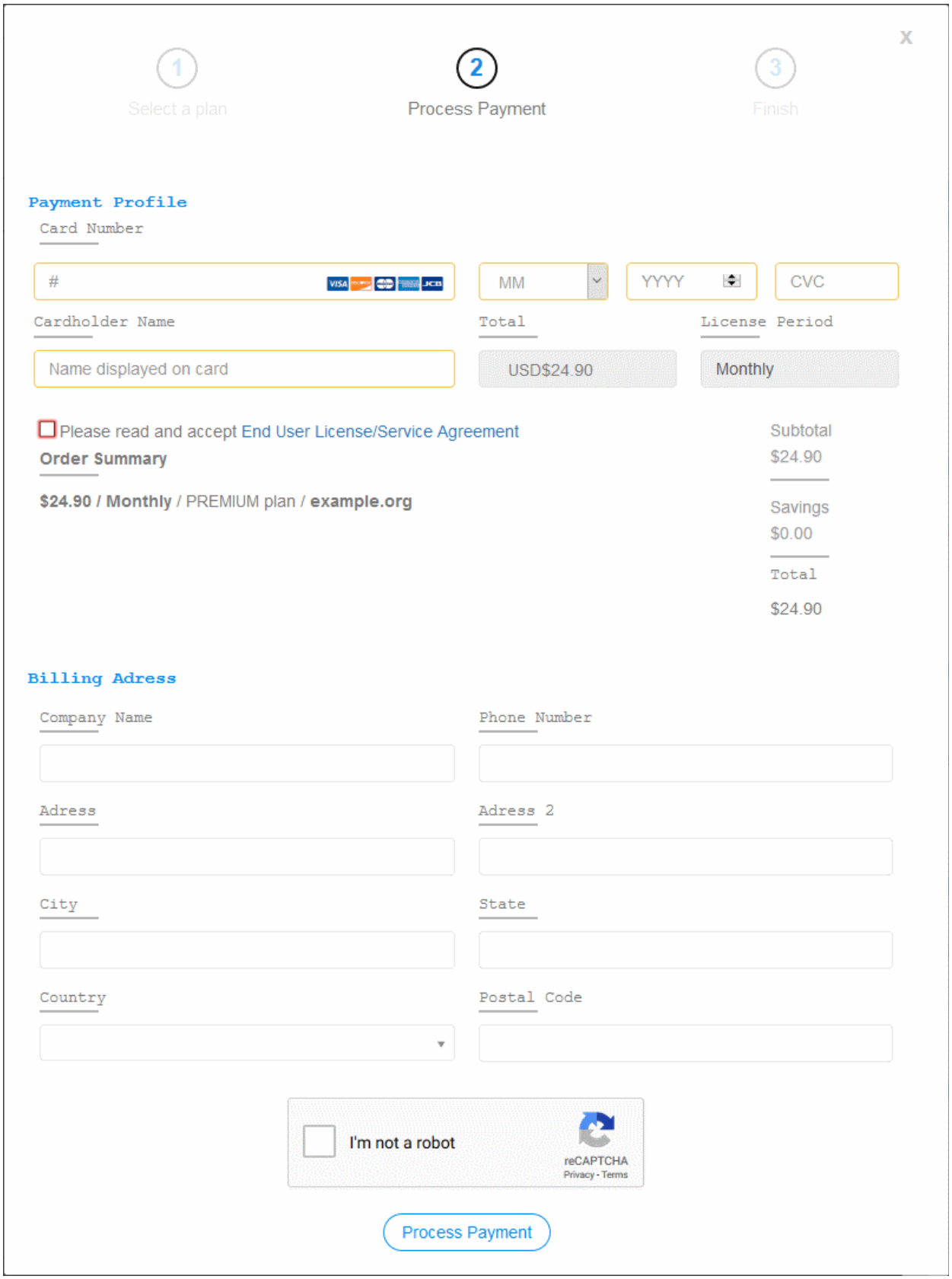
- If you do not have any licenses available then you will be asked to purchase a license:



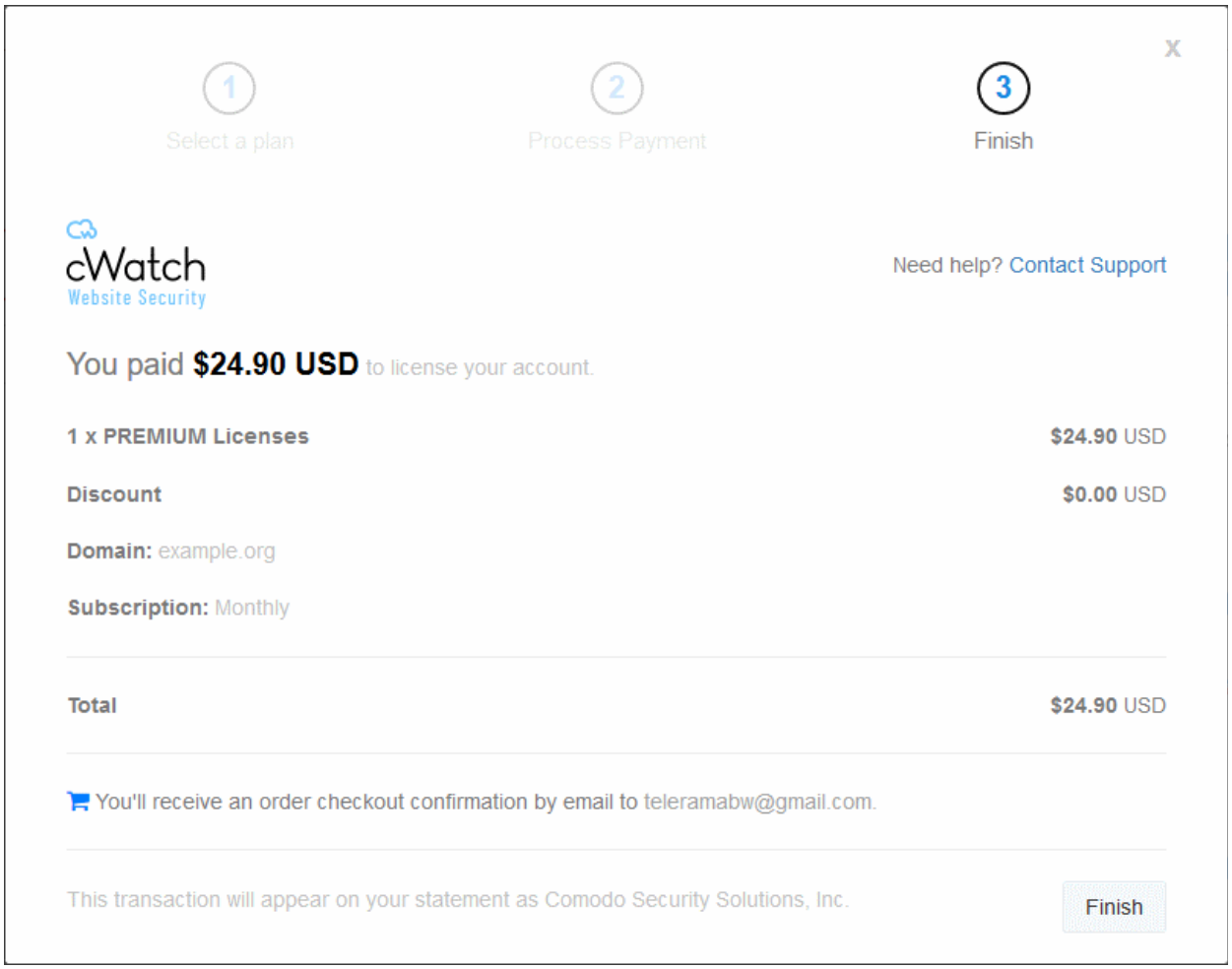
- Click 'Buy a License'.
- You will be taken to the license purchase page:



- Select the license period and type. See **License Types** if you want to read more about the features of each license.
- Click 'Continue'



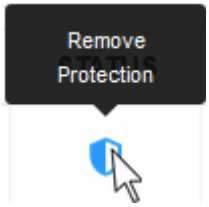
- Complete the payment details section
- Read the 'End User License/Subscriber Agreement' and tick the checkbox to agree
- Enter your billing address
- Complete the captcha verification and click 'Process Payment'



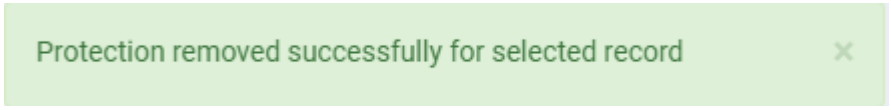
- The new license is added to your account and can be applied to the site in cWatch.
- Restart the process to add protection to the DNS record.

Remove protection from a site

- Click the shield icon beside the record:

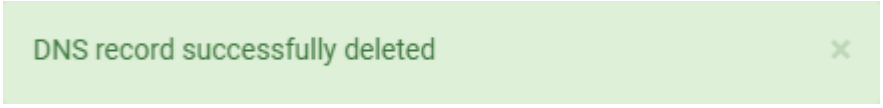


You will see the following confirmation message:



Remove a DNS record

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

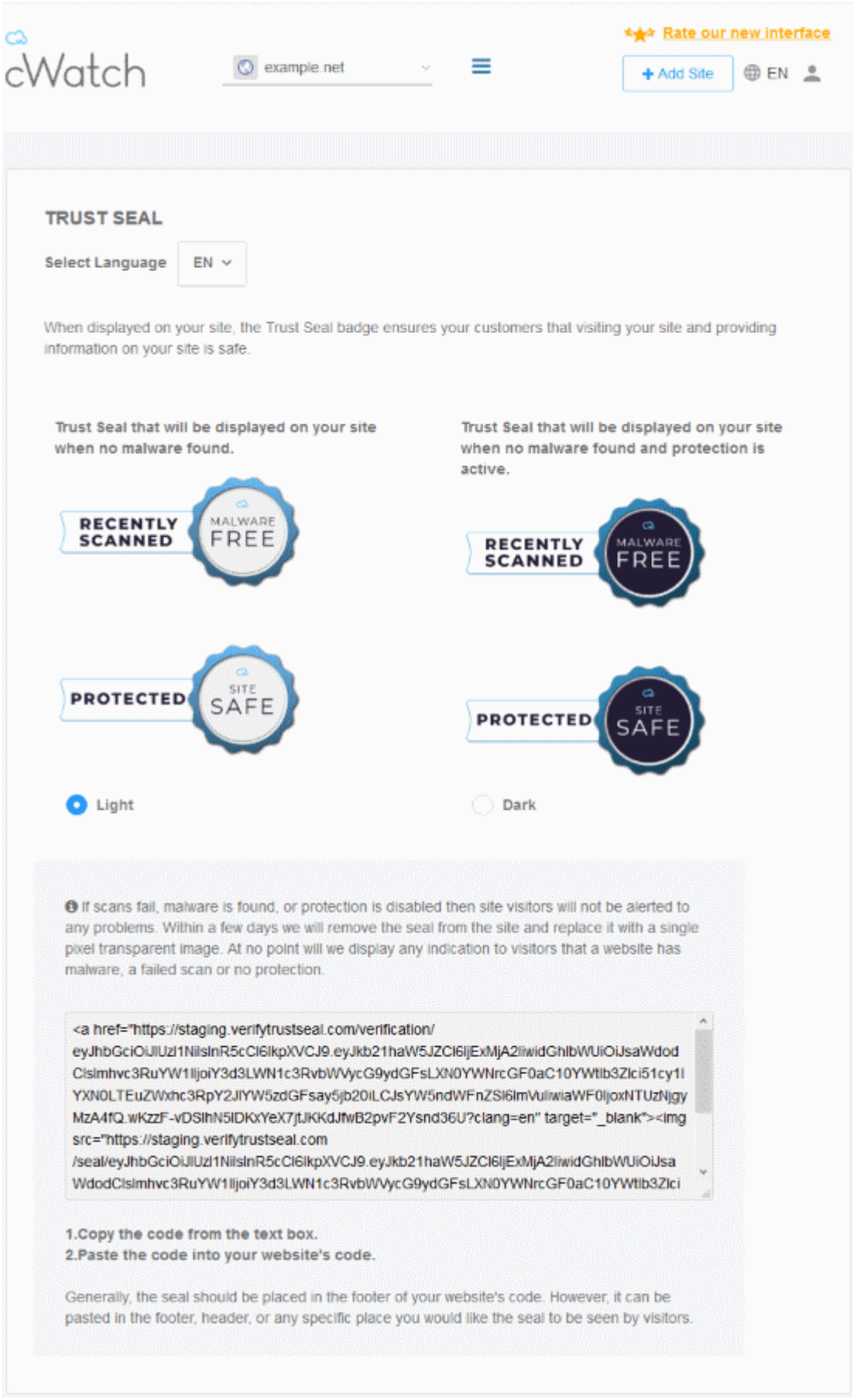


4.9 Add Trust Seal to your Websites

- Select a website from the drop-down at top-left and choose 'Trust Seal'
- The trust seal proves to your visitors that your site is malware free and enjoys 24/7 protection by one of the leaders in online security.
- This helps build the trust you so often need to convert website visitors into paying customers.
- The site seal is available in multiple languages.

Add the trust seal to your website

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



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

- '**Malware Free**' - Displays if your site is not blacklisted and has no malware.
- '**Protected**' - Displays if your site is not blacklisted, has no malware, and both 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

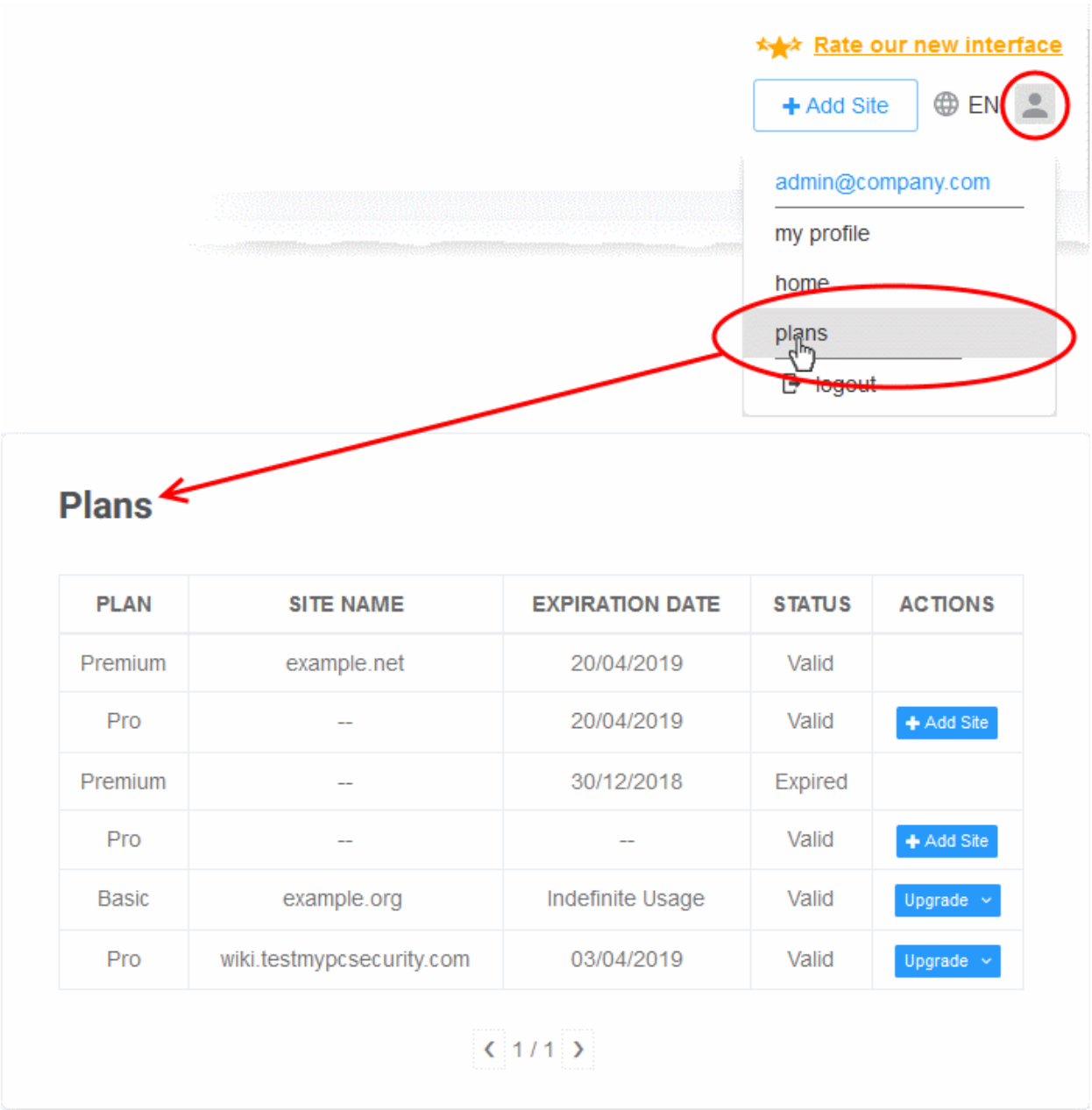
- No negative messaging is shown if your site fails a scan/appears on a blacklist. After a grace period, the seal will simply disappear, replaced by a transparent single-pixel image. The seal will reappear when the issues are fixed.
- Select the language which should be used in the trust seal
- Follow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

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 on the top-left
- Select 'Plans' from the drop-down



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: • **Associate a domain with a unused license** • **Upgrade license for a domain**

From this interface you can:

- **Upgrade license for a domain**
- **Add a new domain to a unused license**

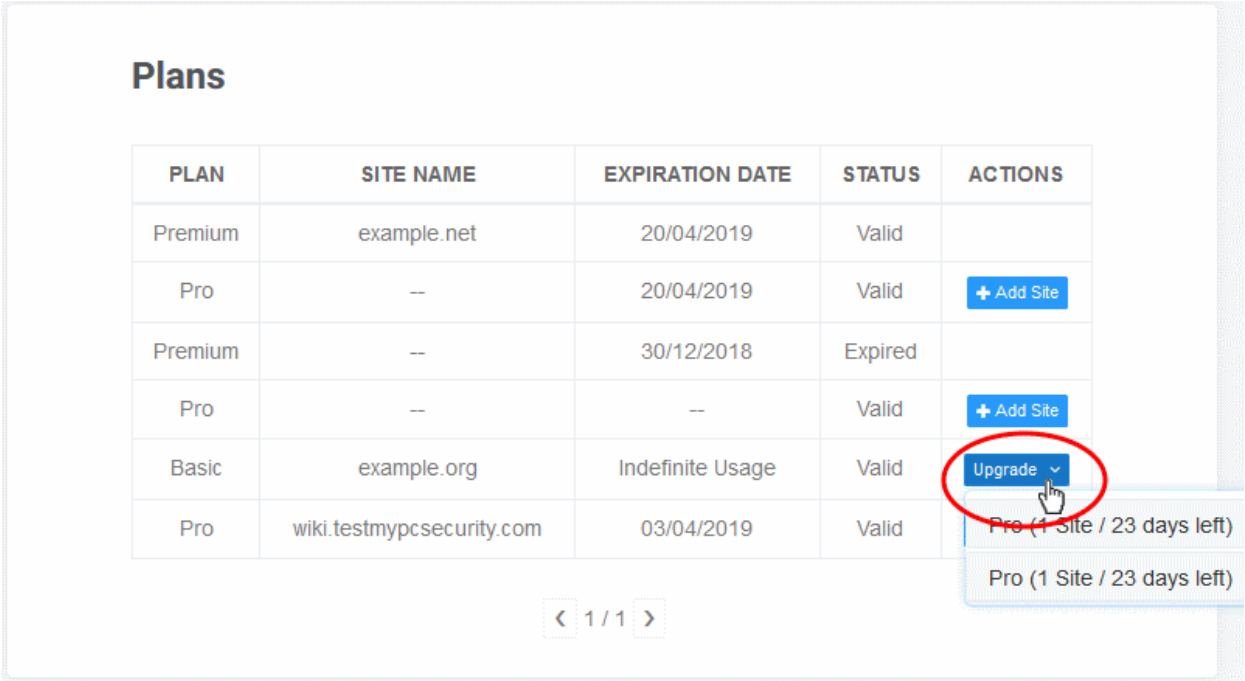
Upgrade license for a domain

You may want to upgrade your cWatch license if:

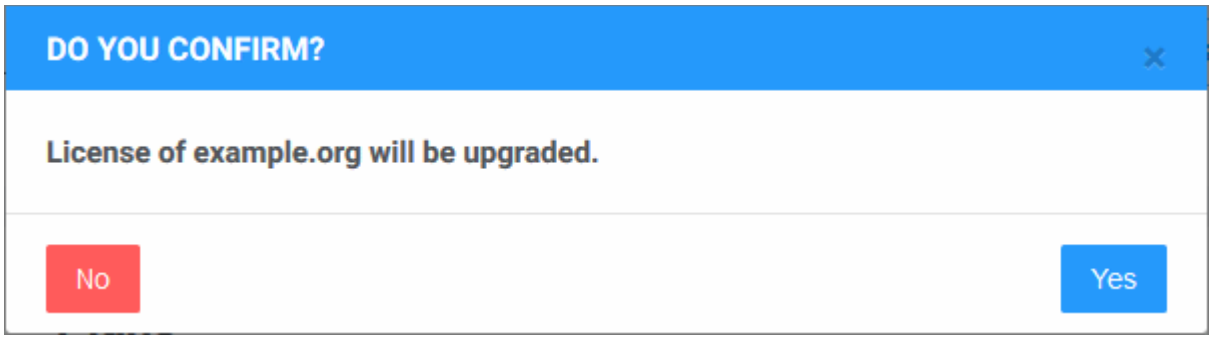
- You wish to enable the superior protection features afforded by a Pro or Premium license
- You want to add sub-domains for a website

Upgrade license

- Click the user icon on the top-left
- Select 'Plans' from the drop-down



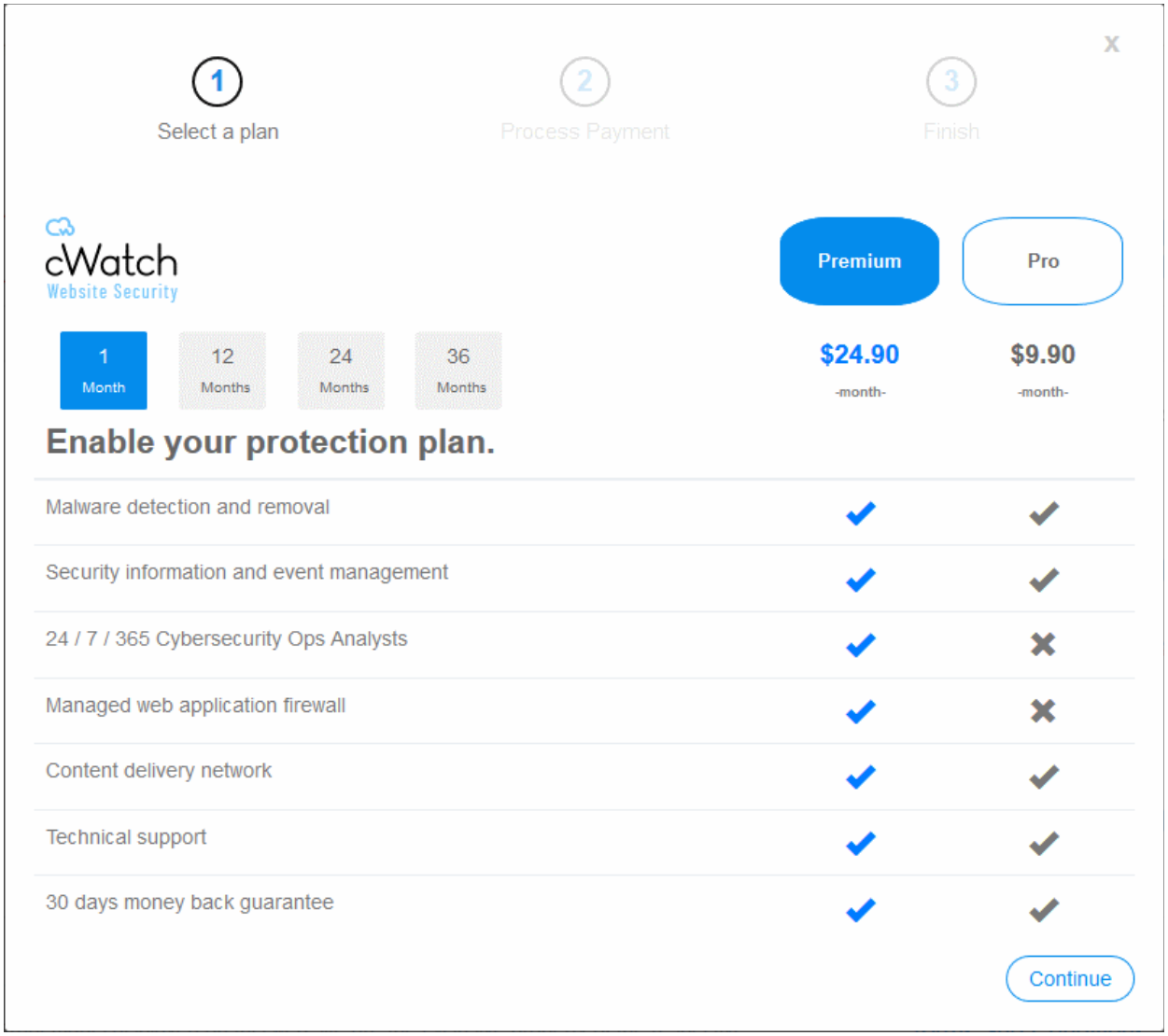
- If you have any unused licenses, a list of available license is shown.
- Select the license you want to associate to the domain



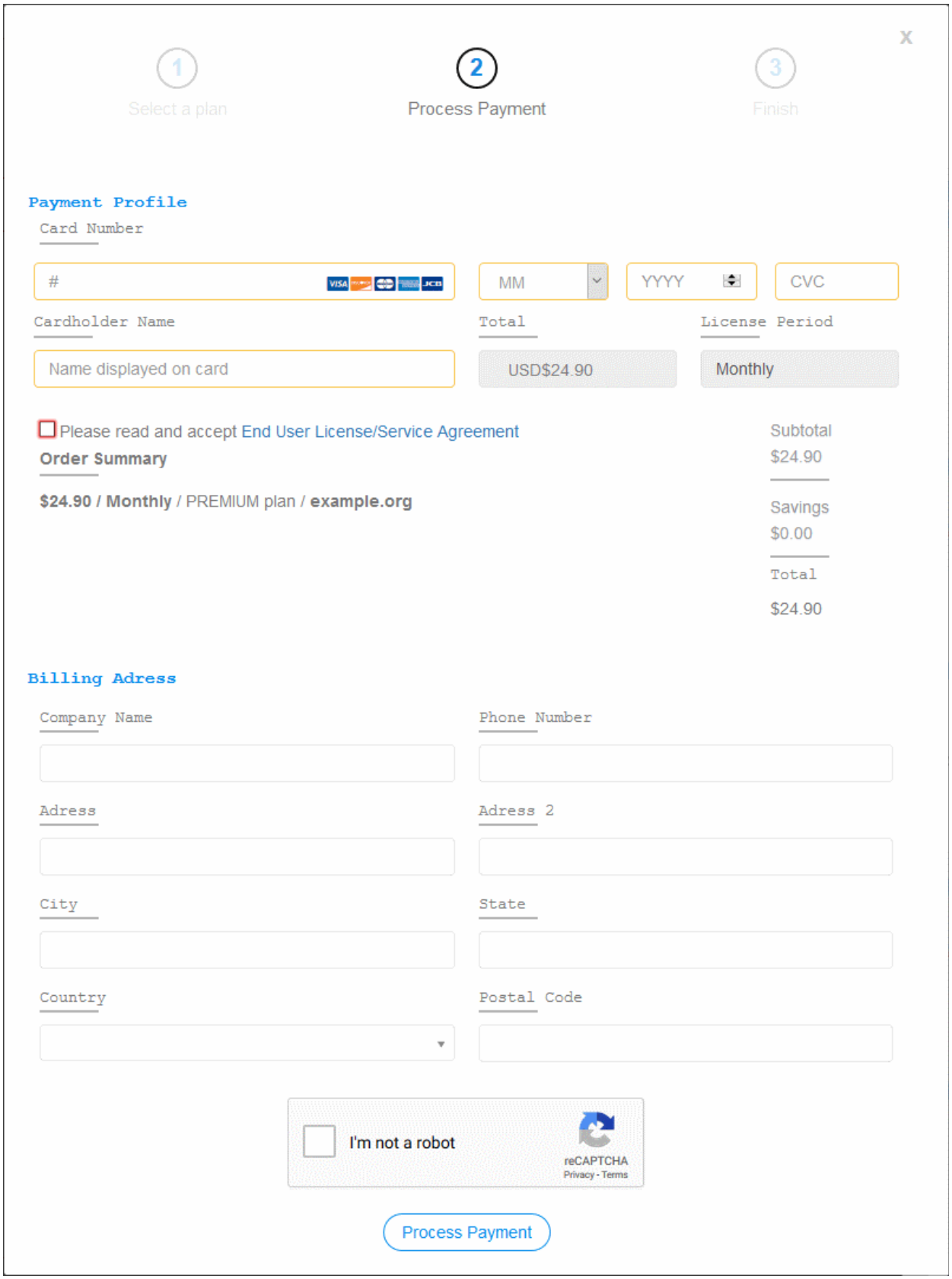
- Click 'Yes' to apply the upgrade.

The domain will be associated with the selected license.

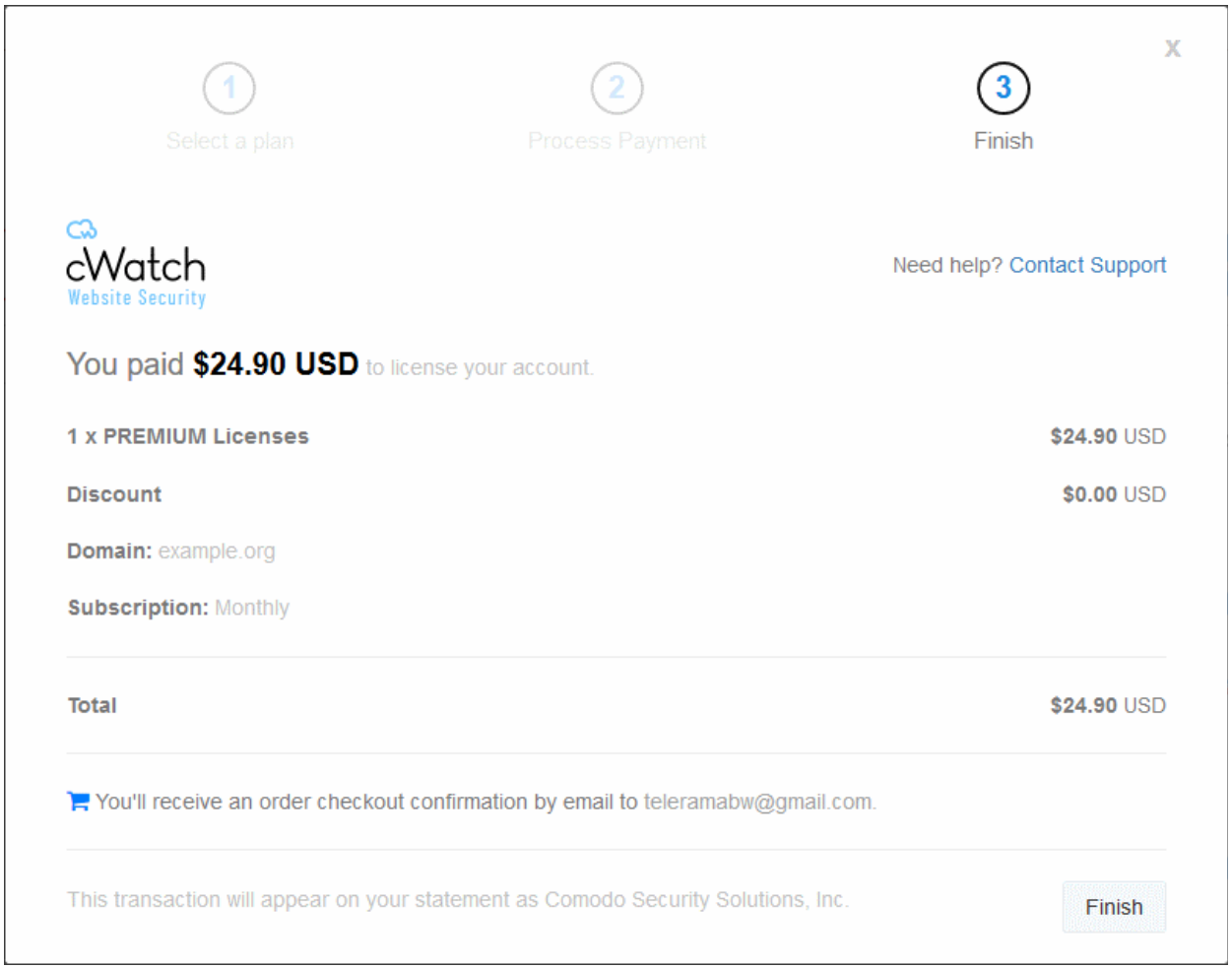
- If you do not have any licenses available then you will be taken to the license purchase page:



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



- 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'

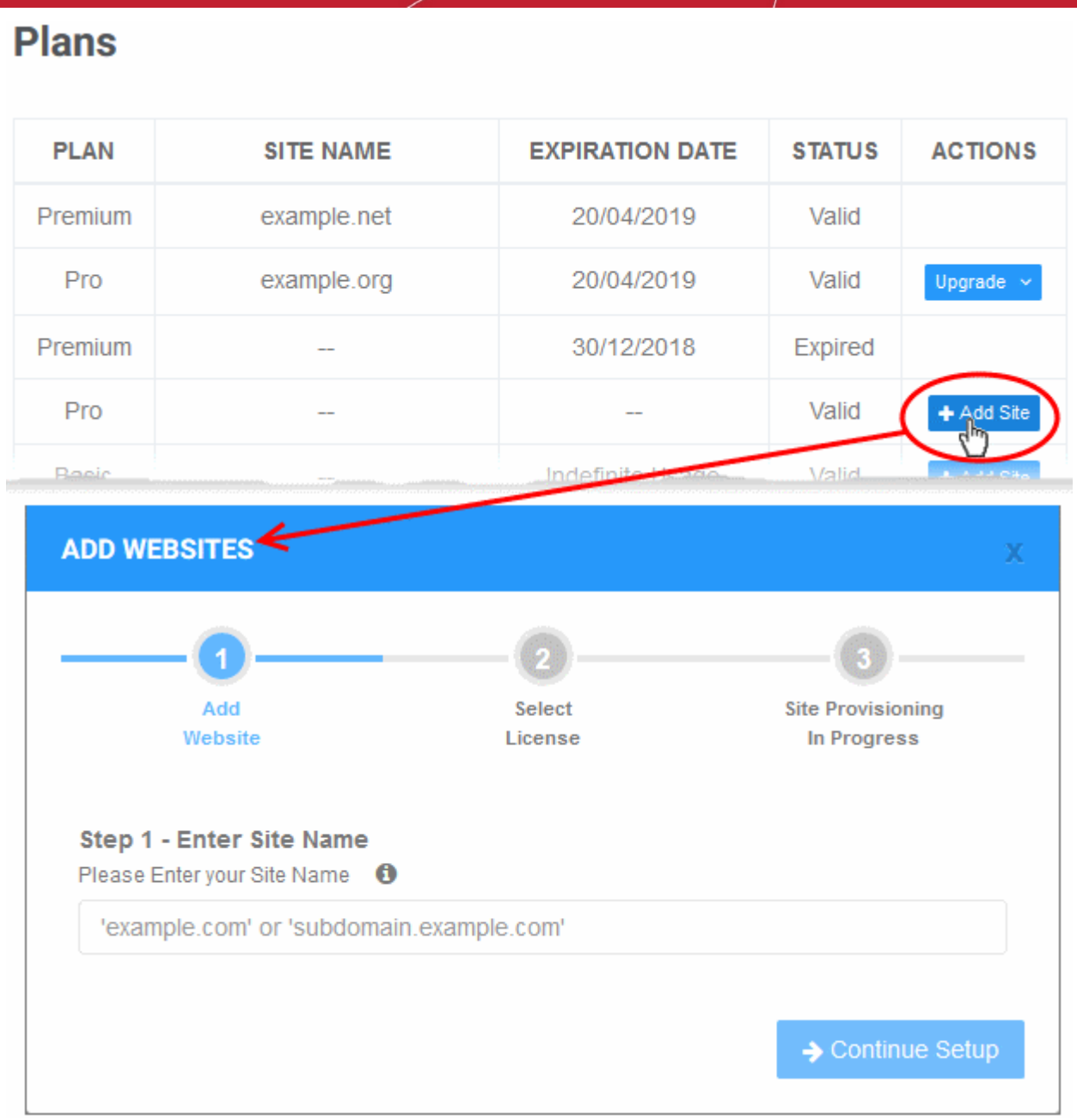


- The new license is added to your account and can be applied to a site in cWatch.
- Restart the process to upgrade the license for the domain.

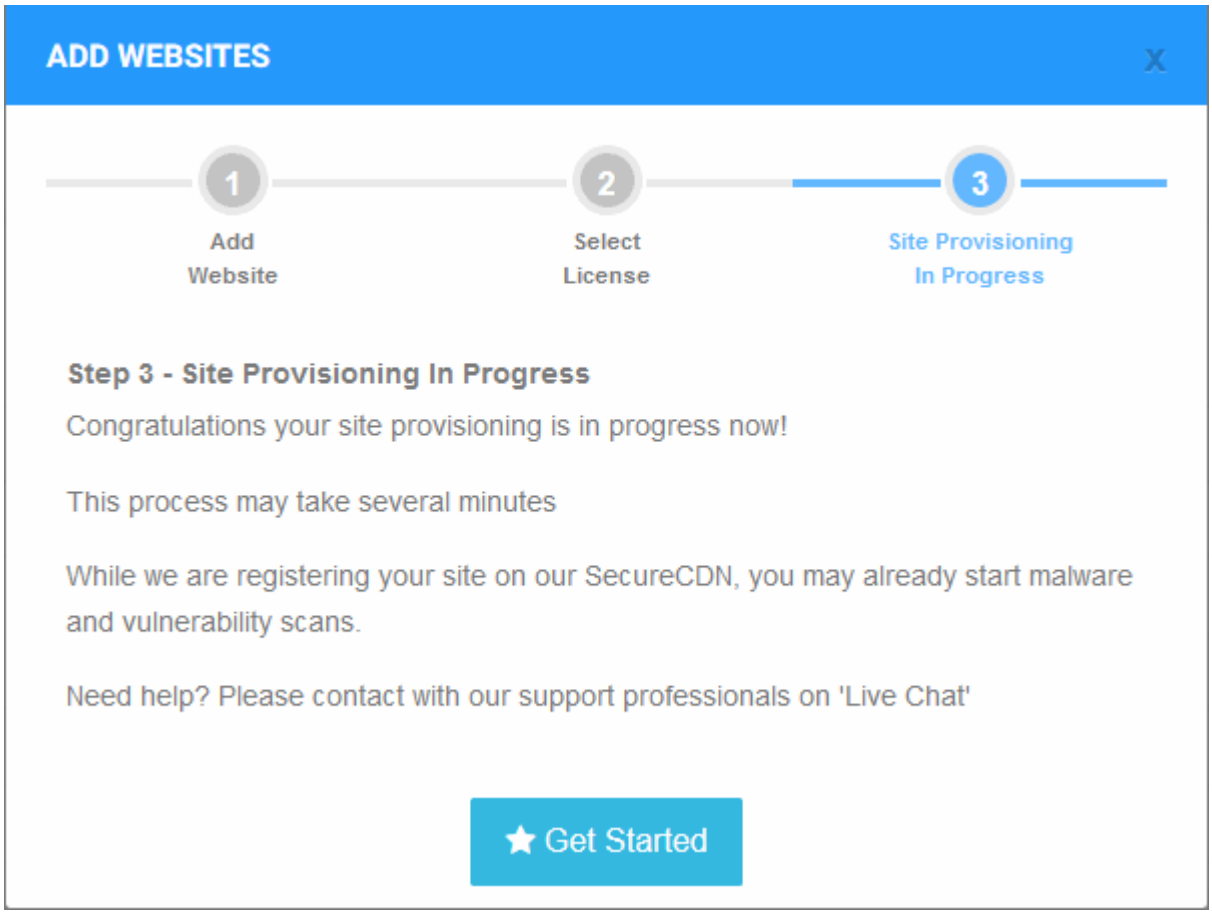
Add a new domain to a unused license

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:



- 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'



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

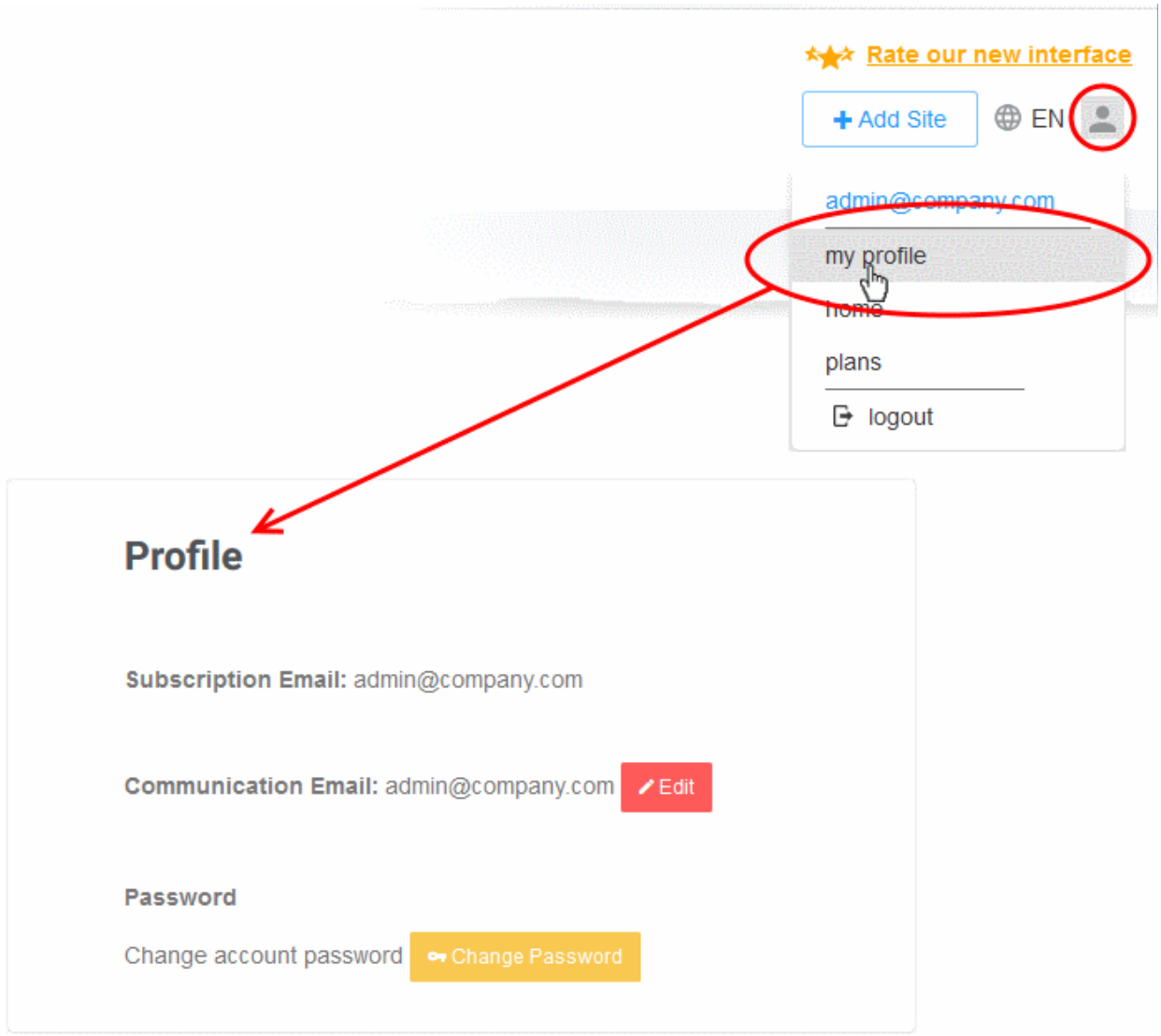
- Next up is to enable cWatch protection on the site.
- Click 'Get Started' to open the 'Overview' page for the site
- The overview page lets you configure malware and vulnerability scans, firewall rules, CDN settings, and more.
- This is covered in more detail in the **Website Overview** section.

6 Manage Your Profile

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

Manage your profile

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

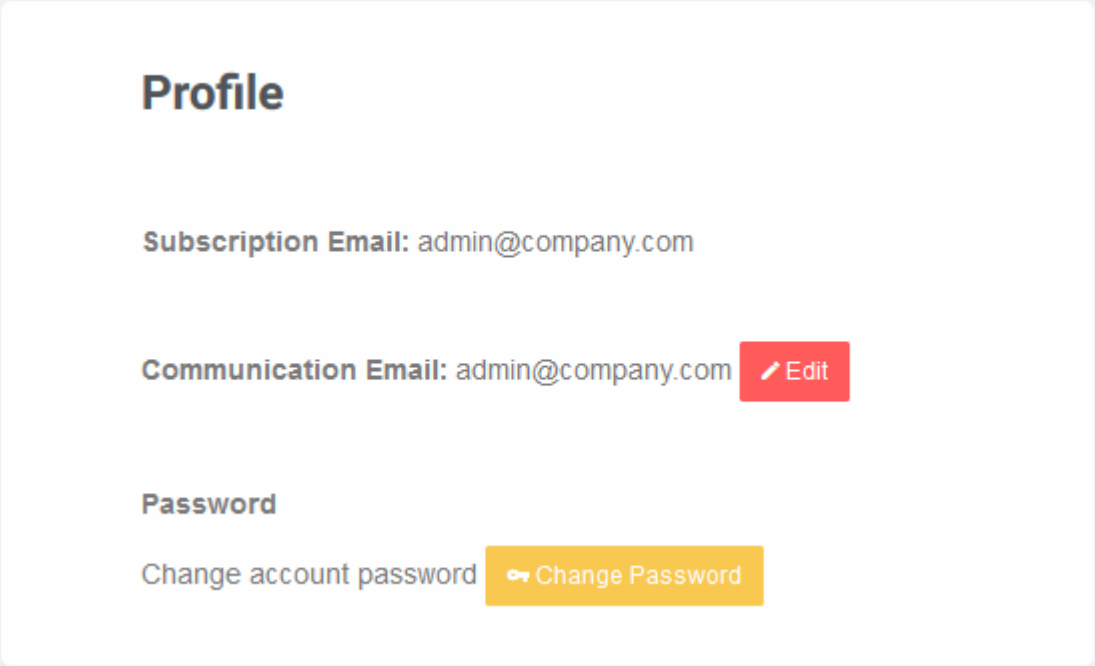


The "Profile interface lets you:

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

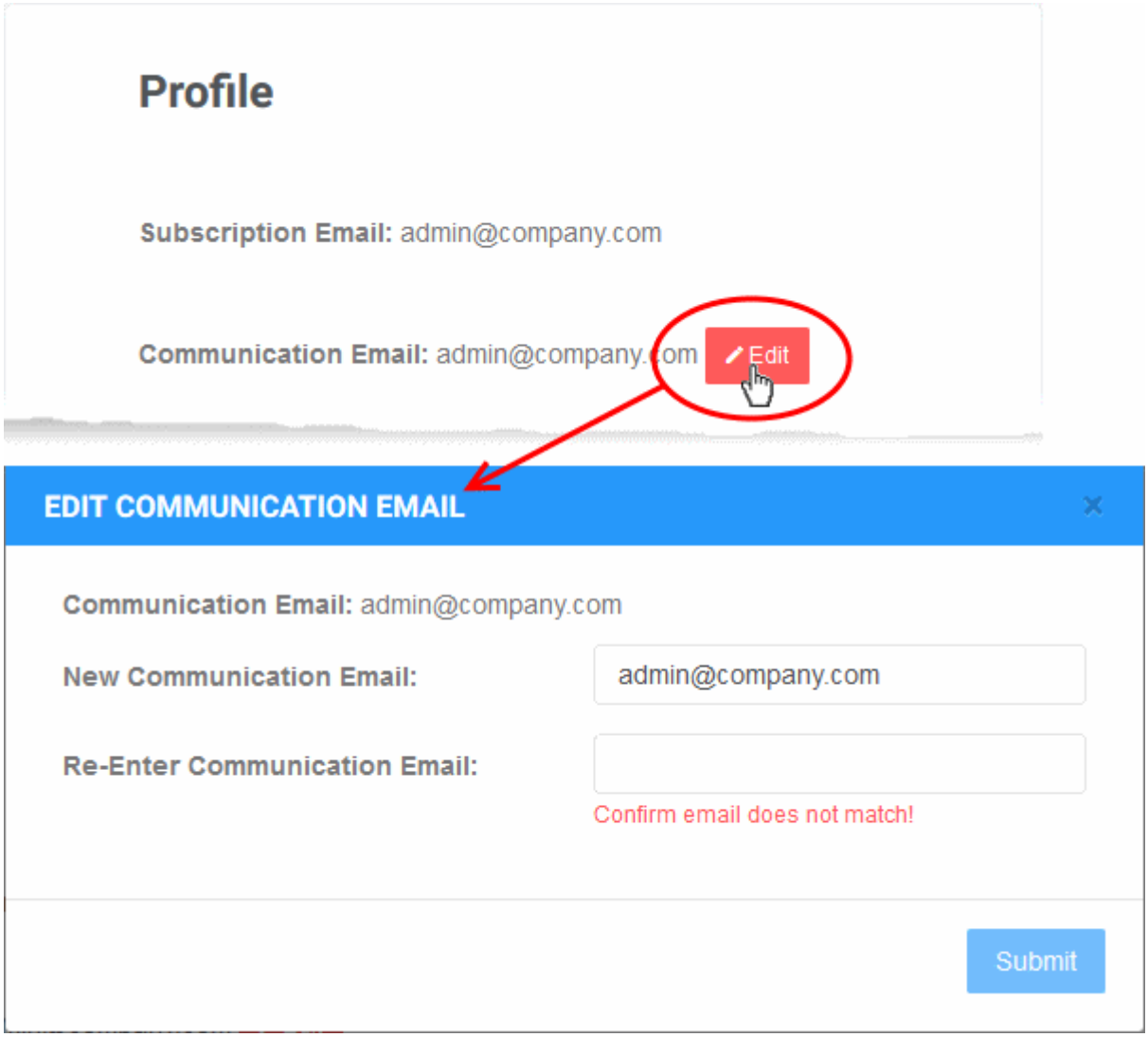
Edit your profile

- Click the user icon on the top-left
- Select 'My Profile' from the drop-down



- **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.

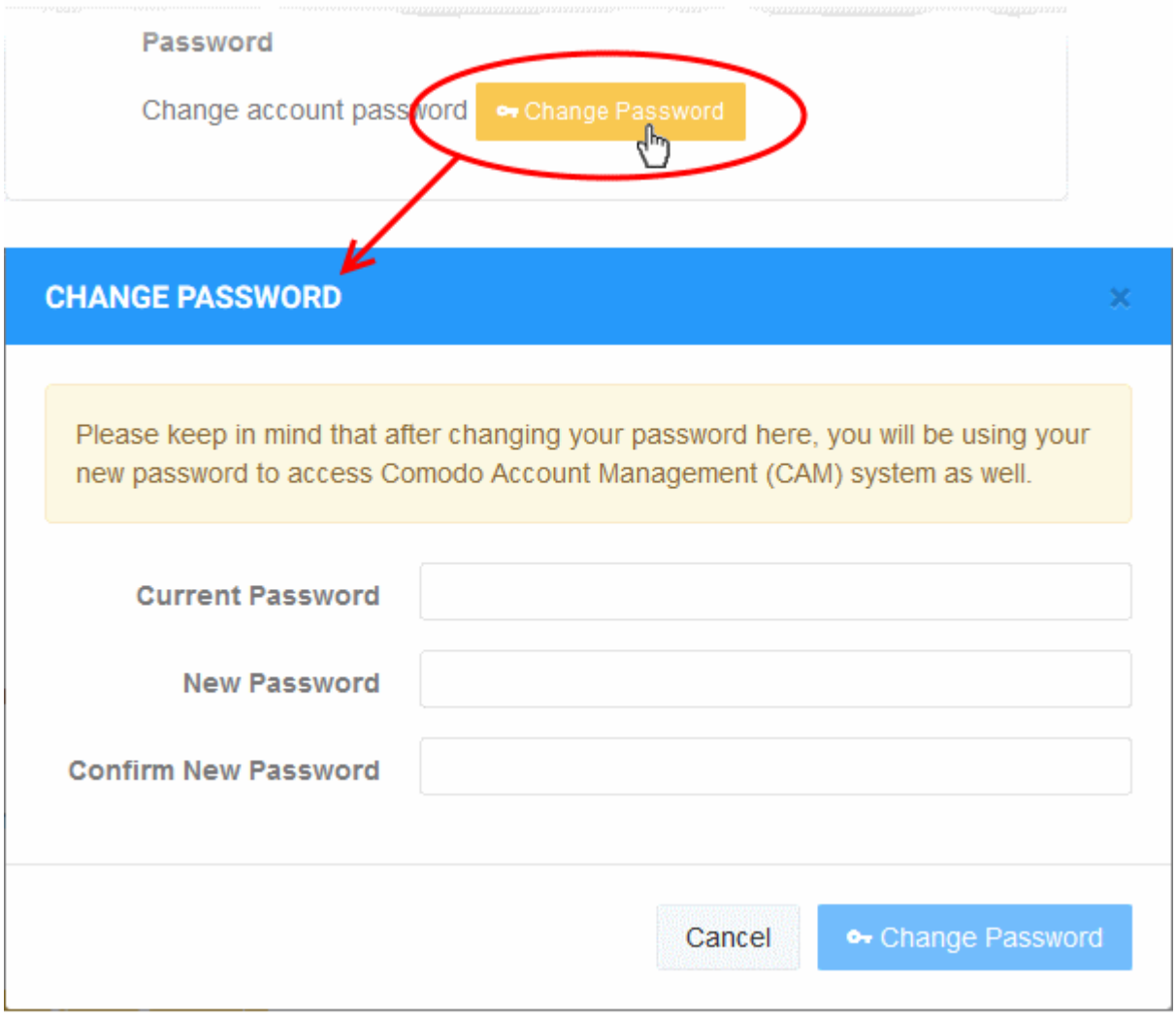
    You will get system emails for the following:
    - Account Creation
    - Purchase cWatch Web
    - Malware Found
    - When license is expired
    - When a license is distributed for the first time
    - When a license is distributed by partner
    - When license is expired
    - When a license is 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'



- 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



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

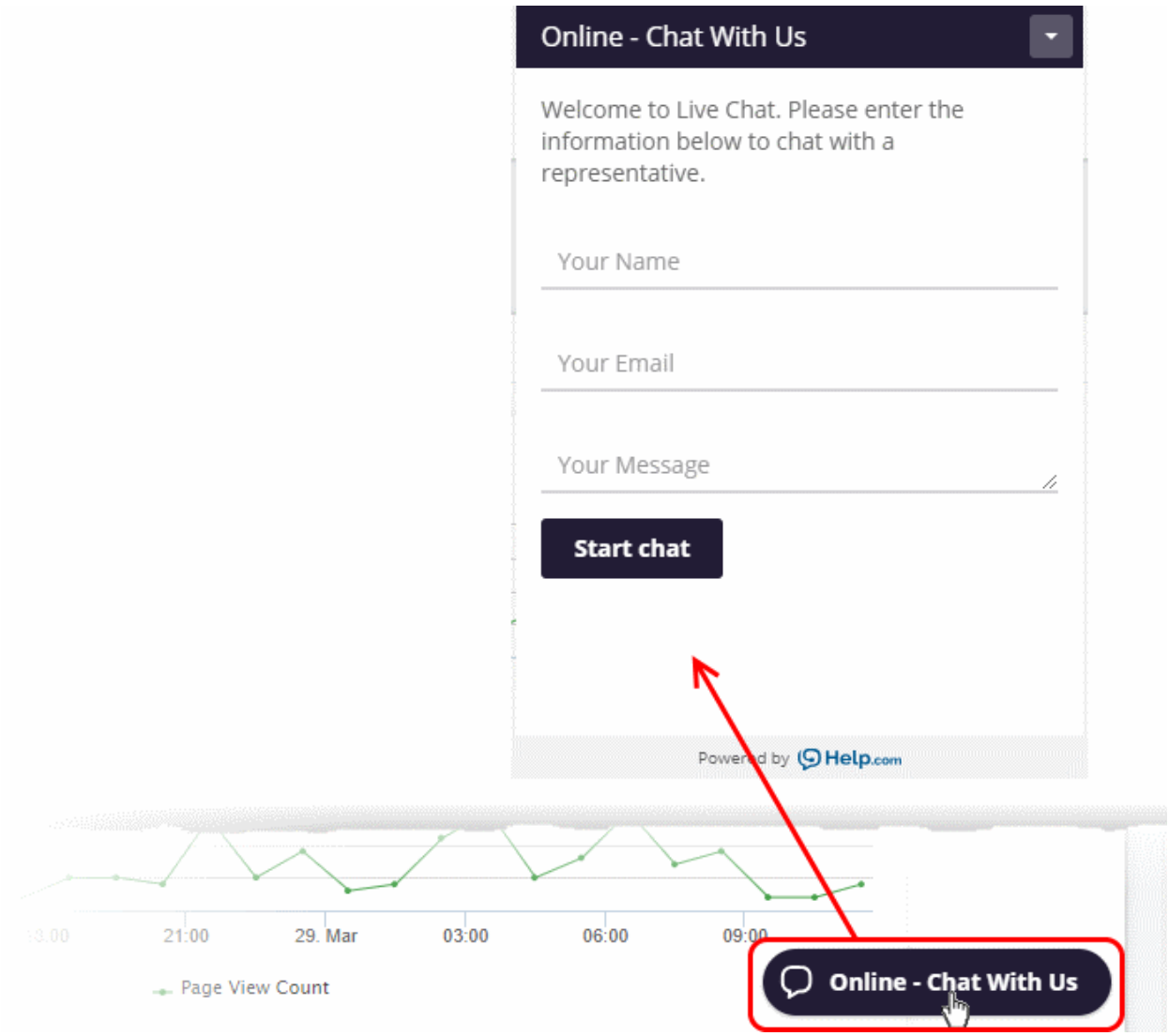
You can use the new password to login to both cWatch and **Comodo Accounts Manager**.

7 Get Support

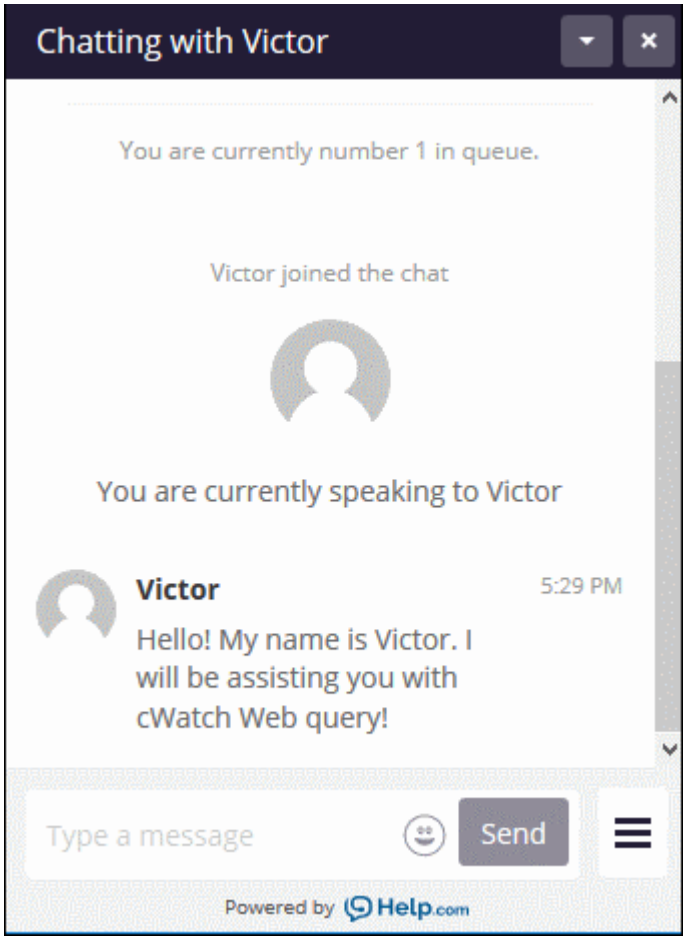
- The live chat service is the fastest way to get help with cWatch.
- Support chat is included with all cWatch license types, including the free 'Basic' license.
- Click 'Online - Chat with us' at the bottom-right of the interface to chat with a Comodo support technician.

Launch a chat session

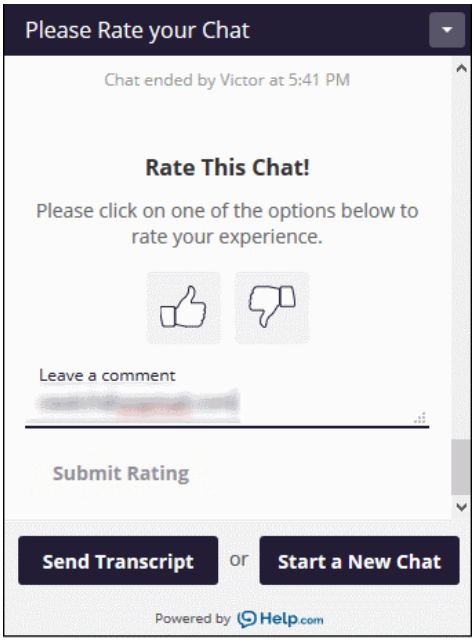
- Click the 'Chat with us button' at the bottom right of the cWatch interface.
- Enter your name and email address in the respective fields
- Type your message
- Click 'Start chat':



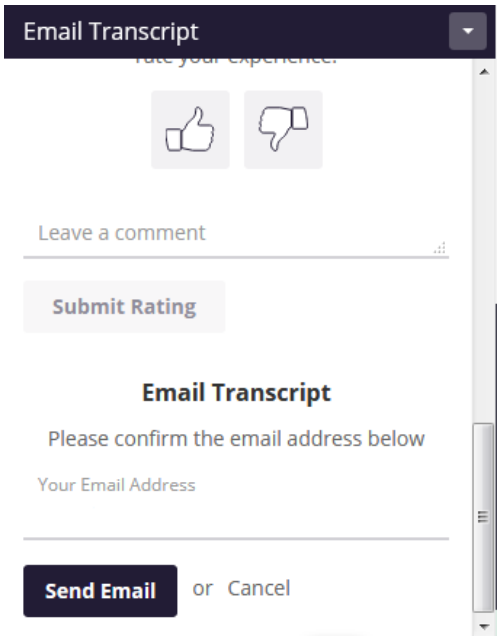
Within seconds, a Comodo technician will respond and ask you to describe the problem:



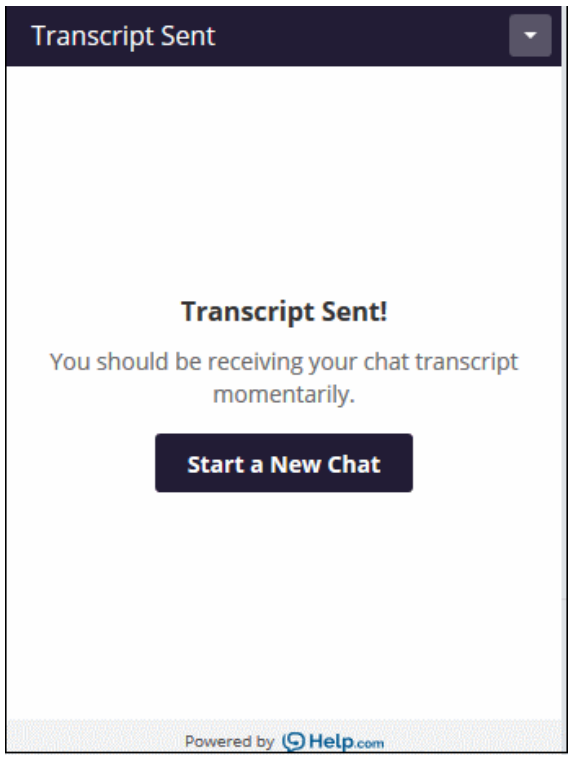
- Start chatting! Use the chat window to explain any problems you are having. The technician will offer advice accordingly.
- End the chat - click the hamburger icon at bottom-right and choose 'End Chat'
- You are given the option to save the chat for future reference.
    - Click 'Send Transcript':



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



- Click 'Send Email'



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

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com 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**