Comodo

cWatch Web Security

Software Version 5.8

Website Administrator Guide

Guide Version 5.8.010820

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo cWatch Web Security....4
1.1 Purchase a License....5
1.2 License Types....20
1.3 Login to the Admin Console....20
1.4 Add Websites....24
2 The Main Interface....29
3 The Dashboard....32
4 Website Data and Settings....33
4.1 Website Overview....35
4.2 Security Scans....40
4.2.1 Website Scans....41
4.2.2 Website Files Security Scans....45
4.2.2.1 Configure Malware Scan Settings....46
4.2.2.1.1 Automatic Configuration....47
4.2.2.1.2 Manual Configuration....49
4.2.2.2 Run a Malware Scan and View Results....50
4.2.2.3 Configure Notifications, Automatic Malware Removal and Schedule Website Scan....62
4.2.3 Vulnerability Scans....64
4.2.3.1 CMS Vulnerability Scans....65
4.2.3.2 OWASP Top 10 Vulnerability Scans....70
4.3 Content Delivery Network....76
4.3.1 Activate CDN for a Website....77
4.3.2 CDN Settings....81
4.3.3 View CDN Metrics....85
4.4 Firewall....90
4.4.1 WAF Statistics....90
4.4.2 WAF Events....92
4.4.3 Configure WAF Policies....93
4.4.4 Manage Custom Firewall Rules....97
4.5 SSL Configuration....100
4.6 DNS Configuration....110
4.7 Add Trust Seal to your Websites....121
4.8 Back up your Website....123
4.8.1 Purchase a Backup License....125
4.8.2 Configure Backup Settings....127
4.8.3 On-Demand Backup....135
4.8.4 View Backup Records and File Statistics....136
4.8.5 Restore and Download Website Files....139
5 View and Upgrade Licenses for Domains....147
6 Manage Your Profile....153
7 Get Support....158

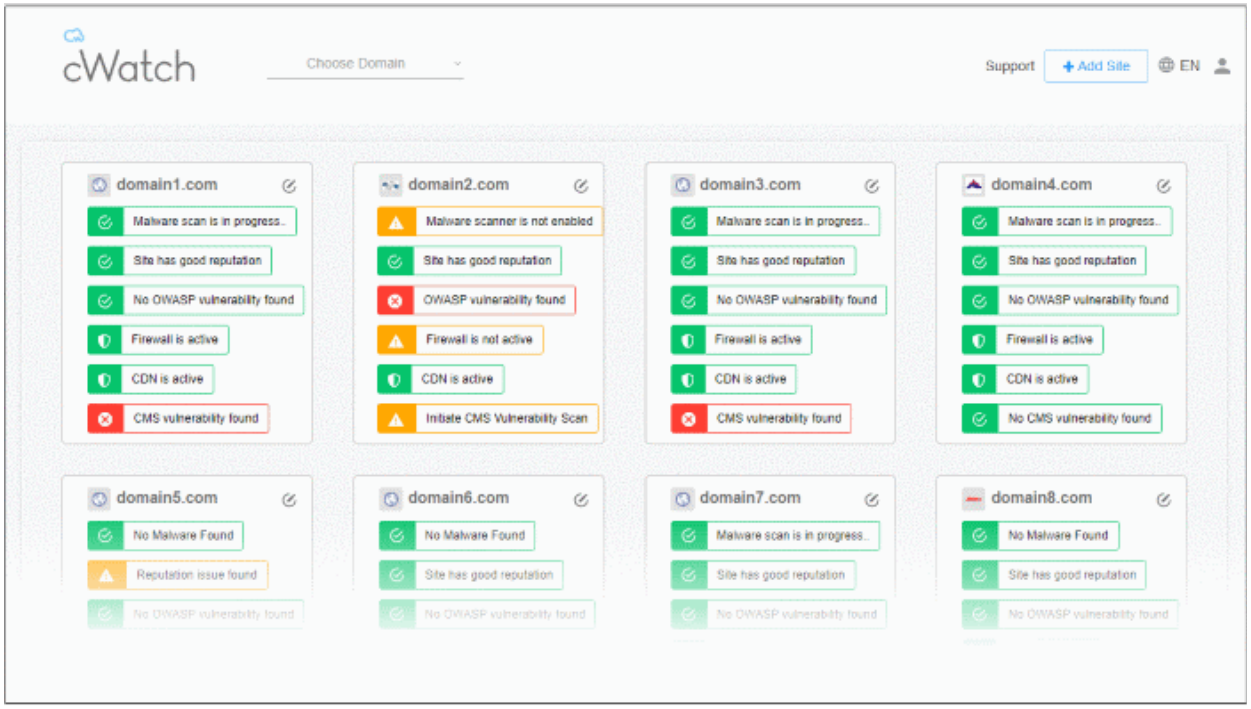
About Comodo Security Solutions.....162

1 Introduction to Comodo cWatch Web Security

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

- cWatch runs regular malware scans on your domains and automatically removes any malware. The content delivery network (CDN) accelerates site performance by delivering your web content from data centers near your visitors.
- The service constantly logs events on your domains to identify new attack vectors. These logs allow the Comodo cyber-security team (CSOC) to create new firewall rules to combat the latest threats.
- The console dashboard instantly tells you about the health of your sites, including any attacks and security related incidents. You can have threat notifications sent to your email.
- The web application firewall provides military grade defense against hacker, SQL injections, bot traffic and more. You can also create your own custom firewall rules.
- You can run regular scans for the top 10 OWASP threats and known CMS vulnerabilities. The 'Website Scan' gives you an immediate heads-up on errors on your front-end pages.
- You can backup your entire website and database, or just specific files to our highly secure servers. An essential disaster-recovery service, cWatch Backup lets you restore your site in a single click.

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



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

Guide Structure:

- **Introduction to Comodo cWatch Web Security**
  - **Purchase a License**
  - **License Types**

- Log-in to the Administrative Console
- Add Websites
- The Main Interface
- The Dashboard
- Website Data and Settings
  - Website Overview
  - Security Scans
    - Website Scans
    - Website Files Security Scans
      - Configure Malware Scan Settings
      - Run a Malware Scan and View Results
      - Configure Notifications, Automatic Malware Removal and Schedule Website Scan
    - Vulnerability Scans
      - CMS Vulnerability Scans
      - OWASP Top 10 Vulnerability Scans
  - Content Delivery Network
    - Activate CDN for a Website
    - CDN Settings
    - View CDN Metrics
  - Firewall
    - WAF Statistics
    - WAF Events
    - Configure WAF Policies
    - Manage Custom Firewall Rules
  - SSL Configuration
  - DNS Configuration
  - Add Trust Seal to your Websites
  - Back up your Website
    - Purchase a Backup License
    - Configure Backup Settings
    - On-Demand Backup
    - View Backup Records and File Statistics
    - Restore and Download Website Files
- View and Upgrade Licenses for Domains
- Manage Your Profile
- Get Support

1.1 Purchase a License

Three types of cWatch license are available:

- Basic
- Pro
- Premium

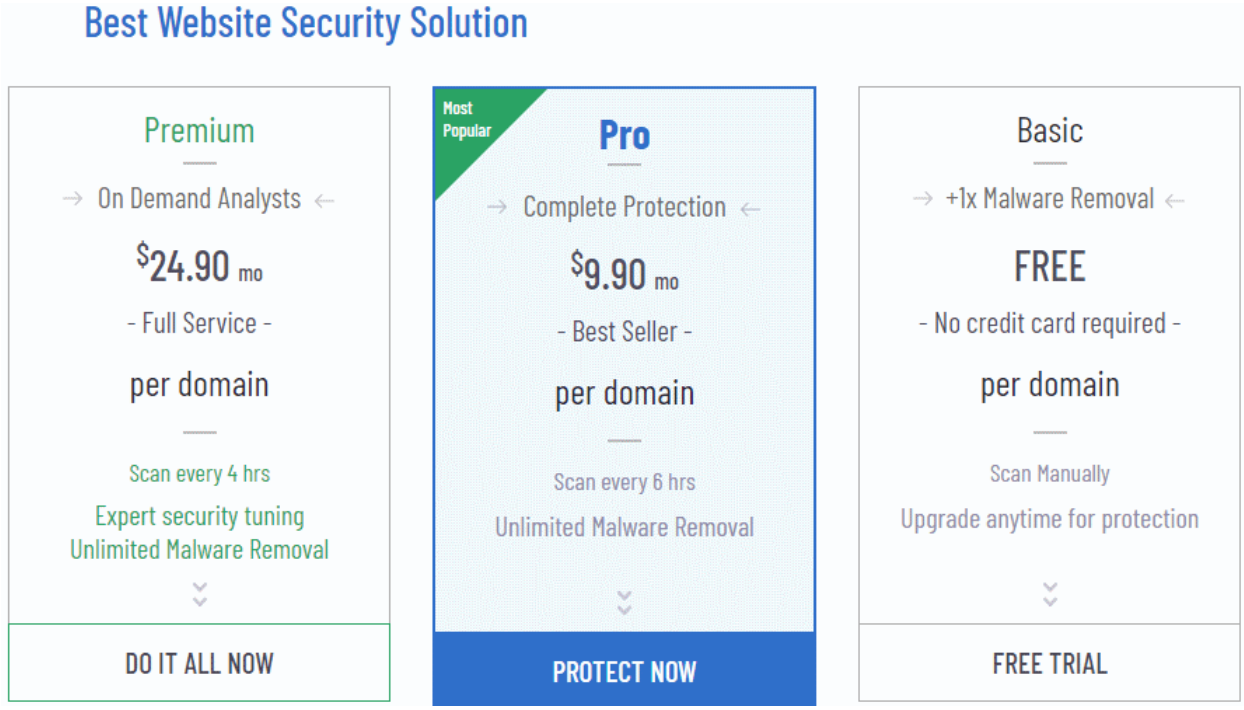
See **License Types** for details on the differences between licenses.

General notes

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

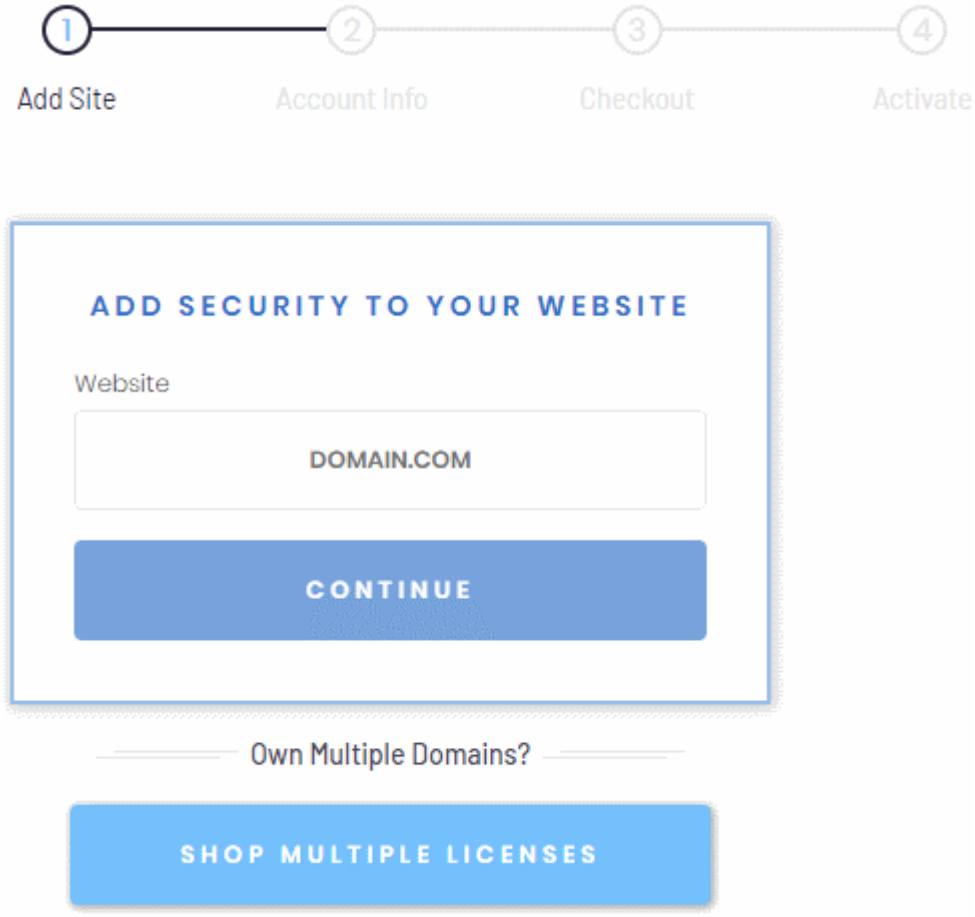
Purchase a license

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



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

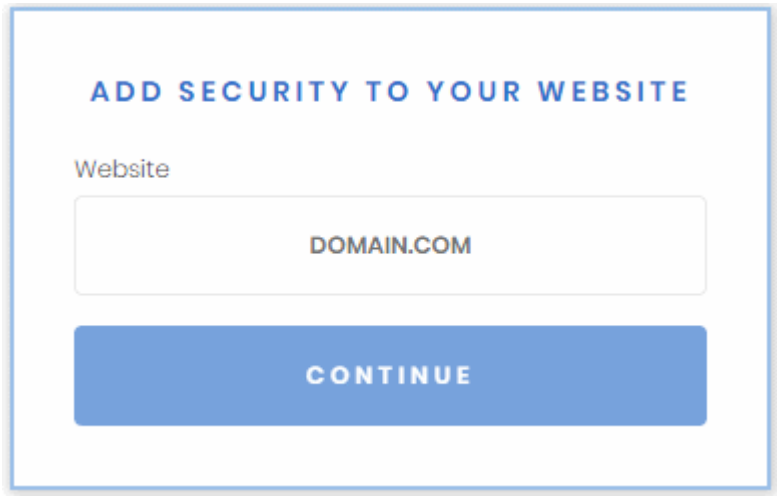
You will be taken to license configuration page:



- 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.

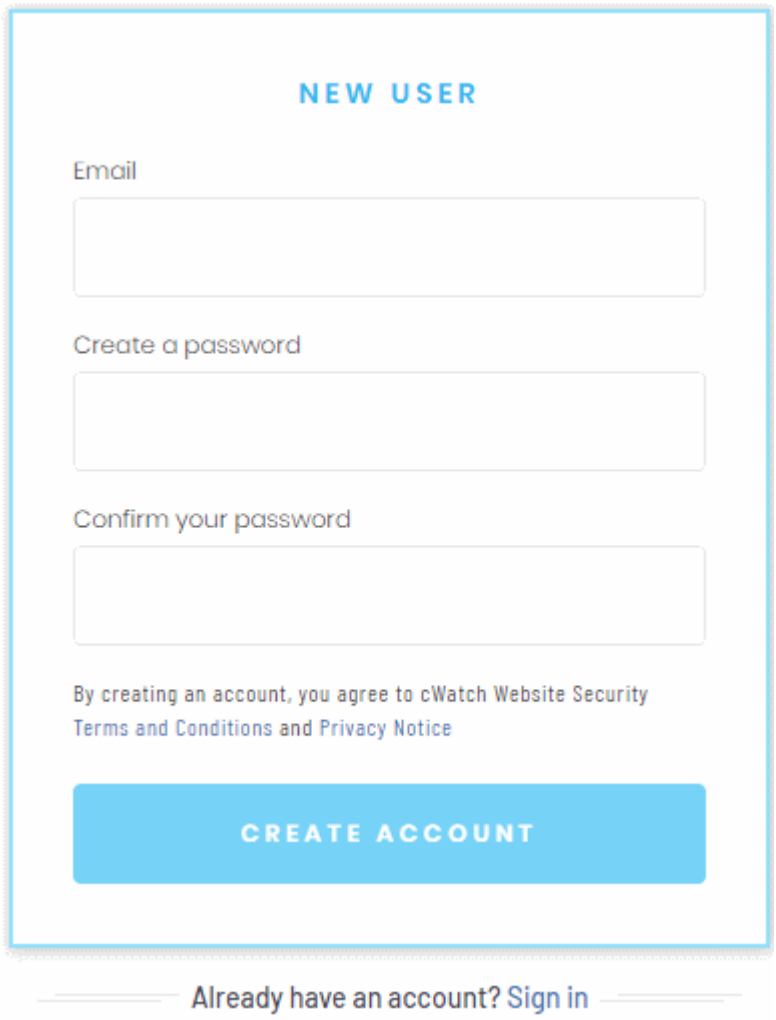
Purchase single domain license

Step 1 - Enter your domain name

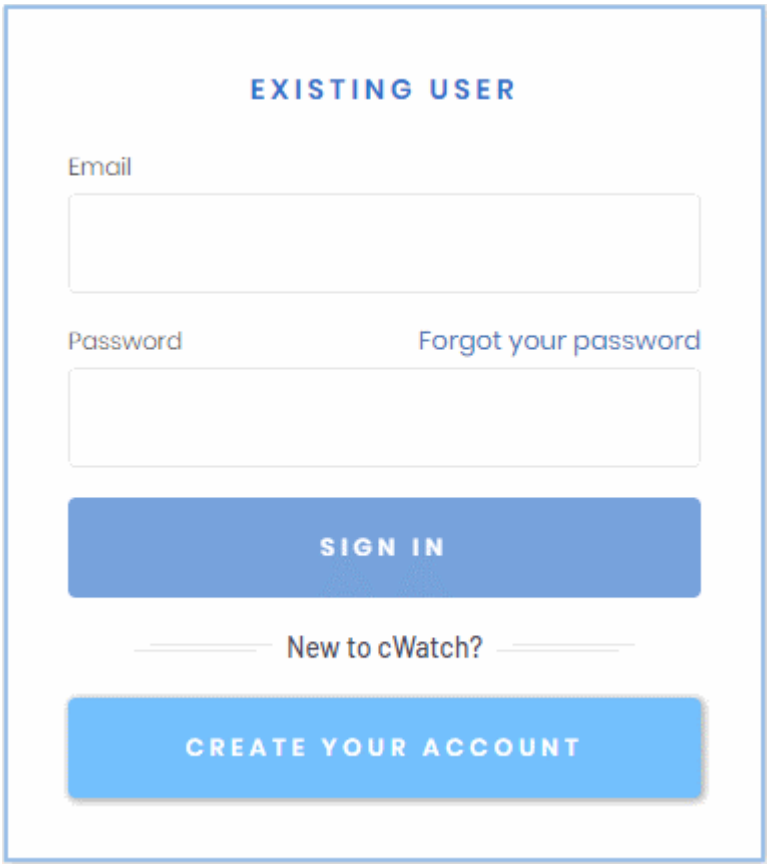


- Type your website (without 'www.') in the Website field and click continue

Step 2 - Enter your Comodo account Information

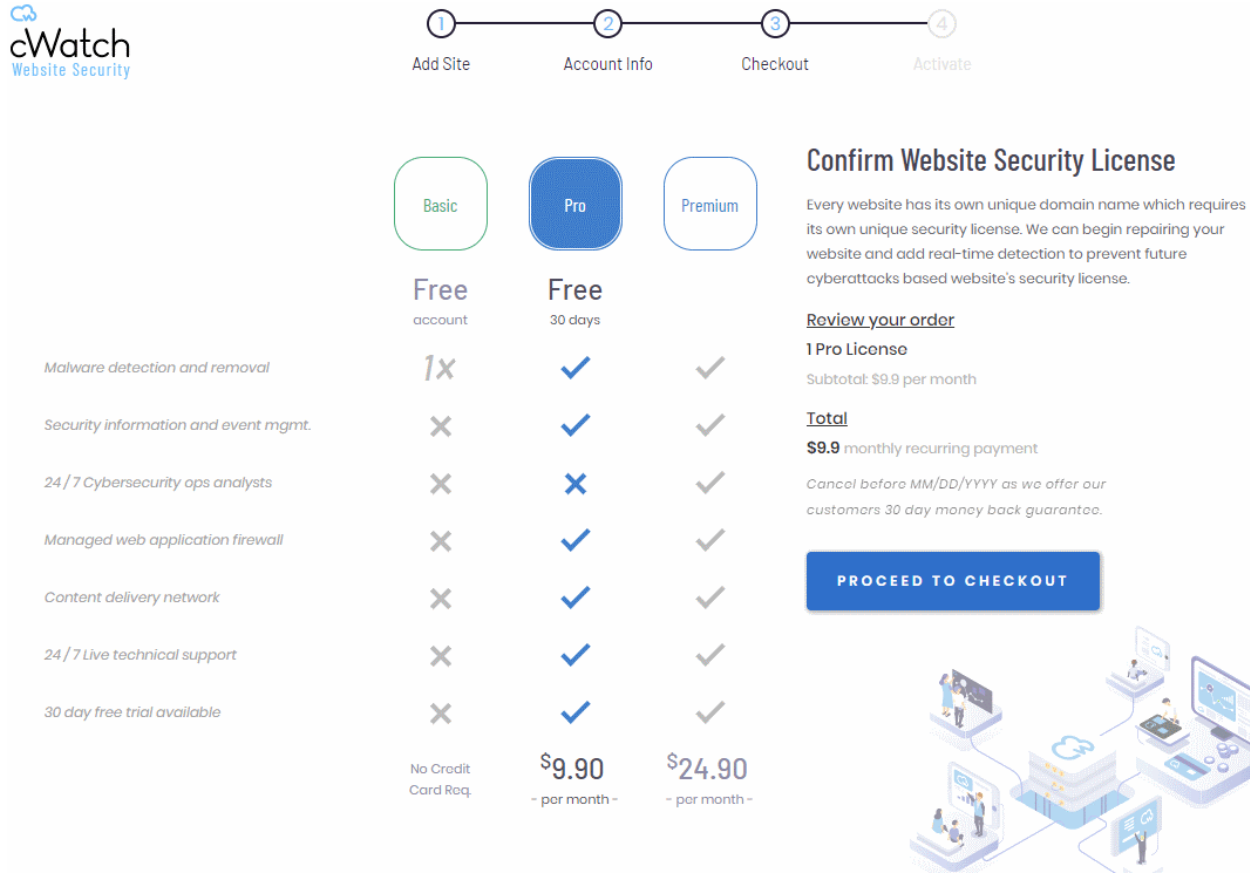


- If you don't have a Comodo account, enter your email address and a password to create a new account
- If you already have a Comodo account, click 'Sign in'



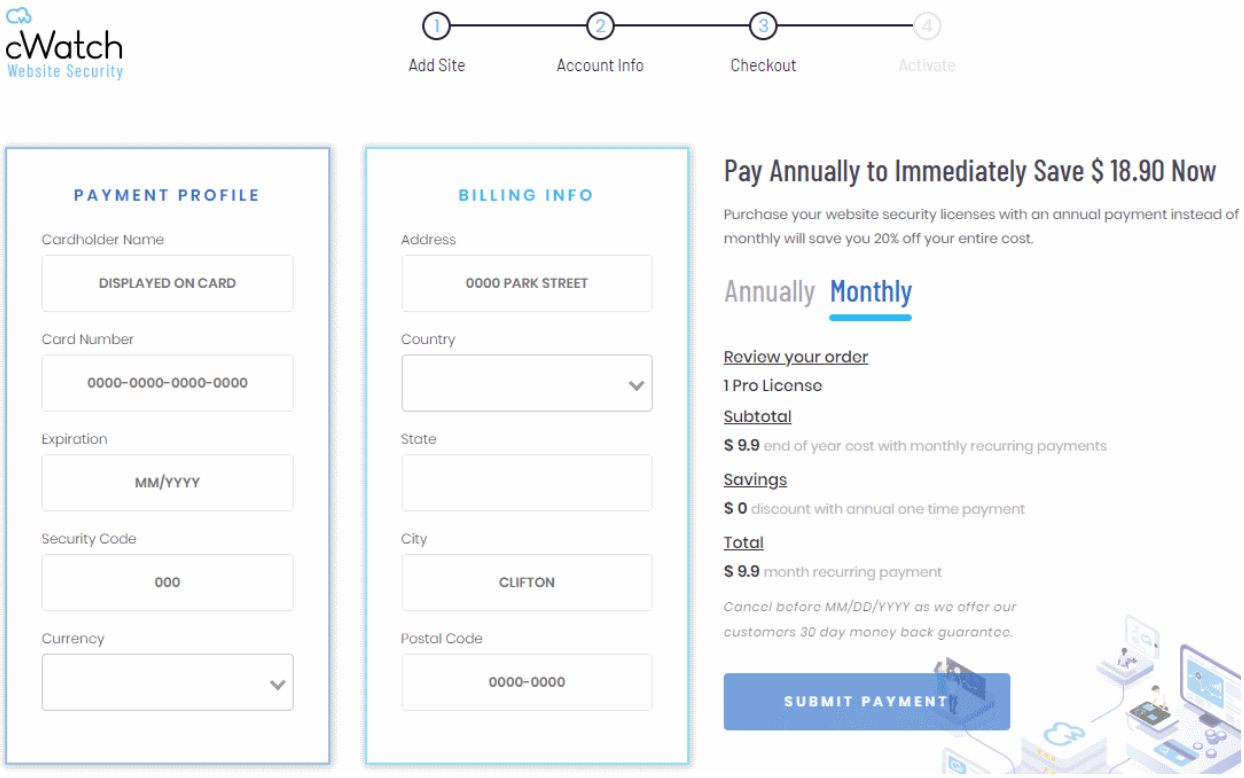
- Enter your username and password and click 'Sign-in'

Step 3 - Select License Type



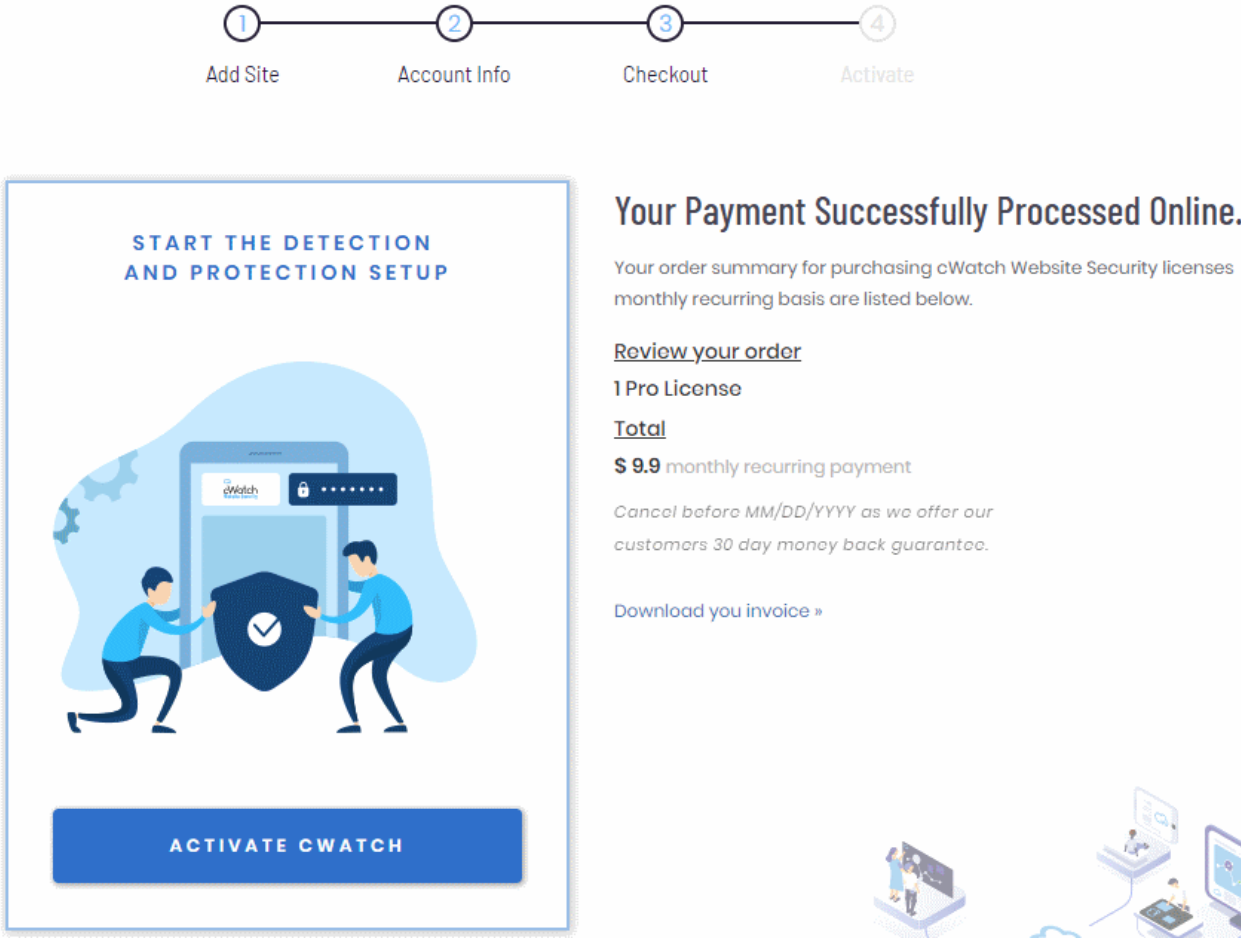
- Select the license type for the domain. See **License Types** for more details about the features of each license.
- Click 'Proceed to Checkout'

Step 4 - Enter Payment Details

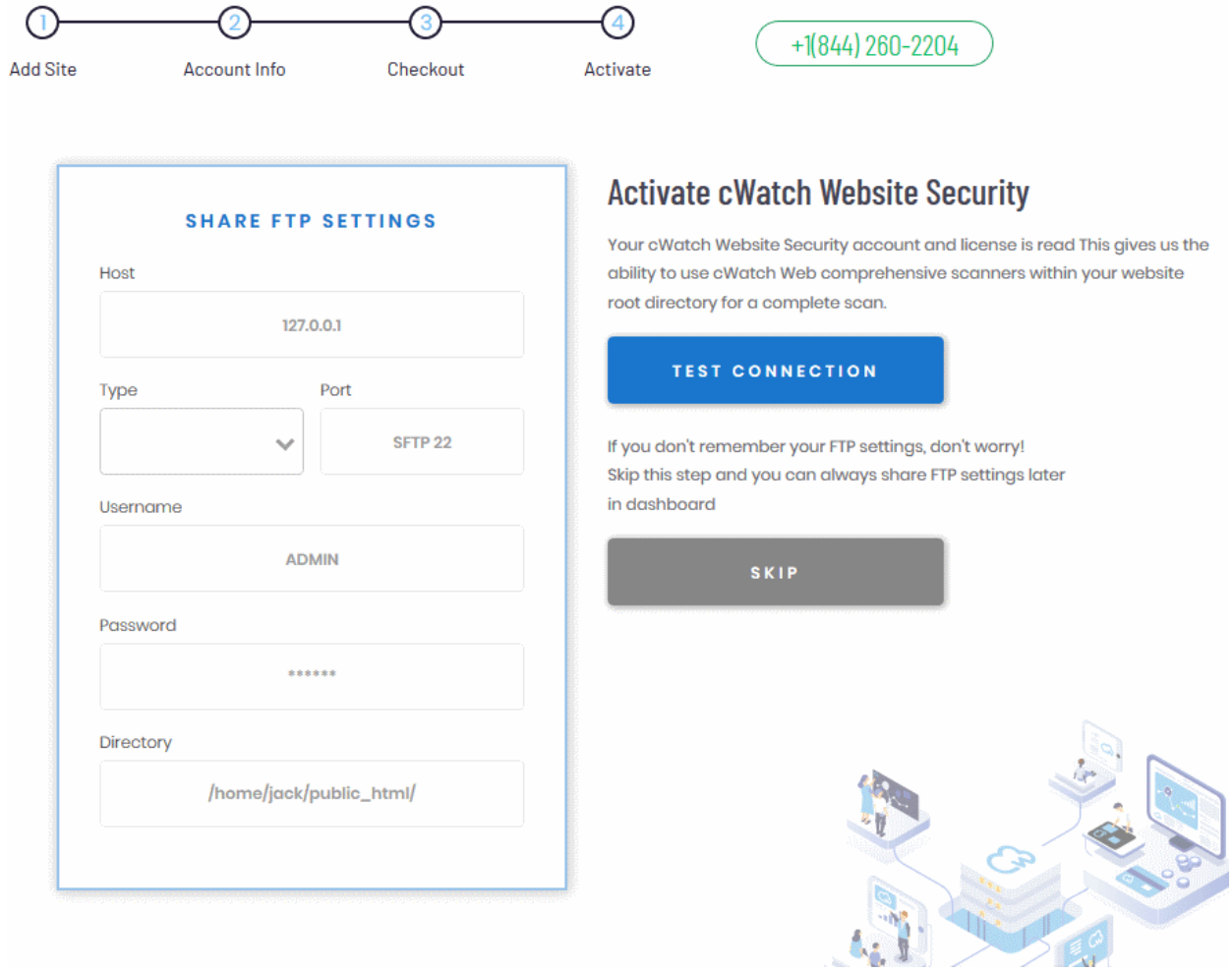


- Payment Profile - Enter your card details for recurring payments for auto-renewal of license.
- Billing Info - Enter your billing address
- Choose the period of license. The available options are 'Annually' or 'Monthly'.
- Click 'Submit Payment'

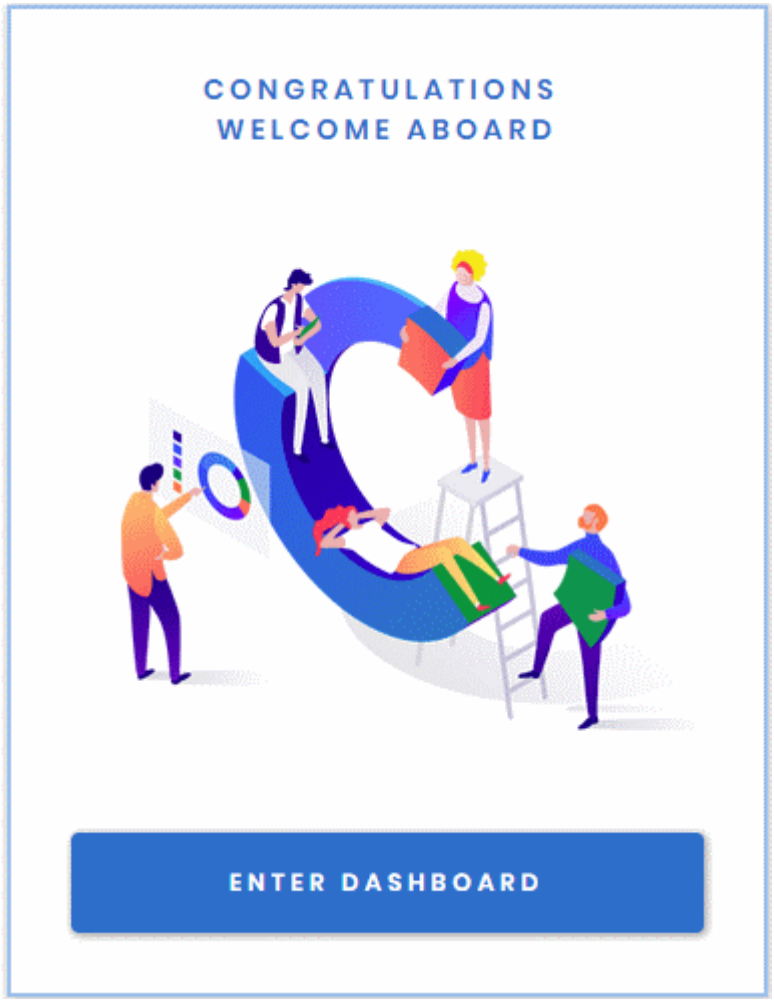
Step 5 - Activate License



- 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.

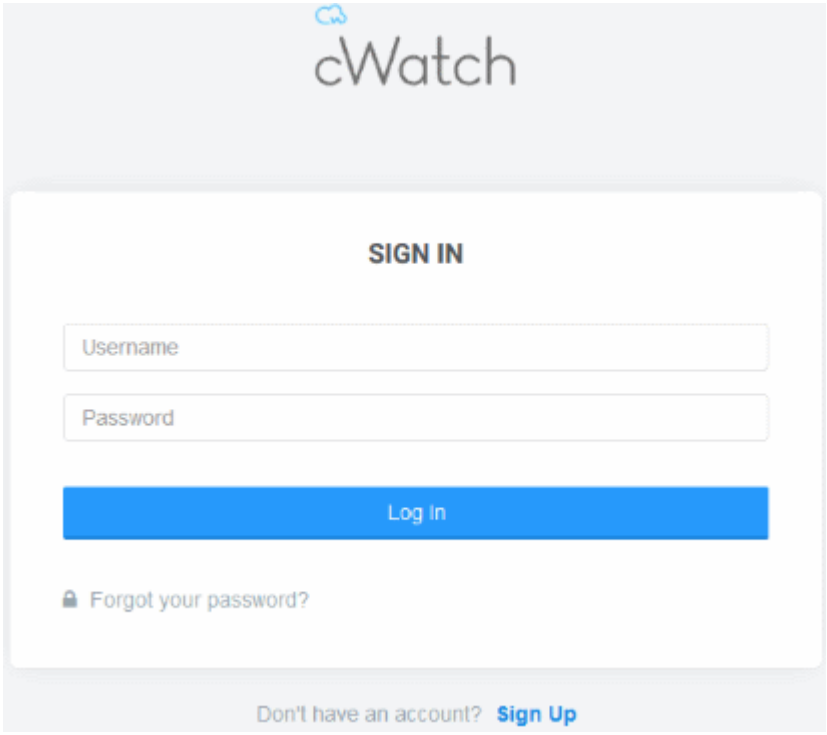


- Enter the hostname, login details and upload directory. The location must be publicly accessible.
- Click 'Test Connection' for cWatch to check whether it can reach the location.
  - Note. Our technicians will also use these settings to access your site IF you request them to remove malware.
- Click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

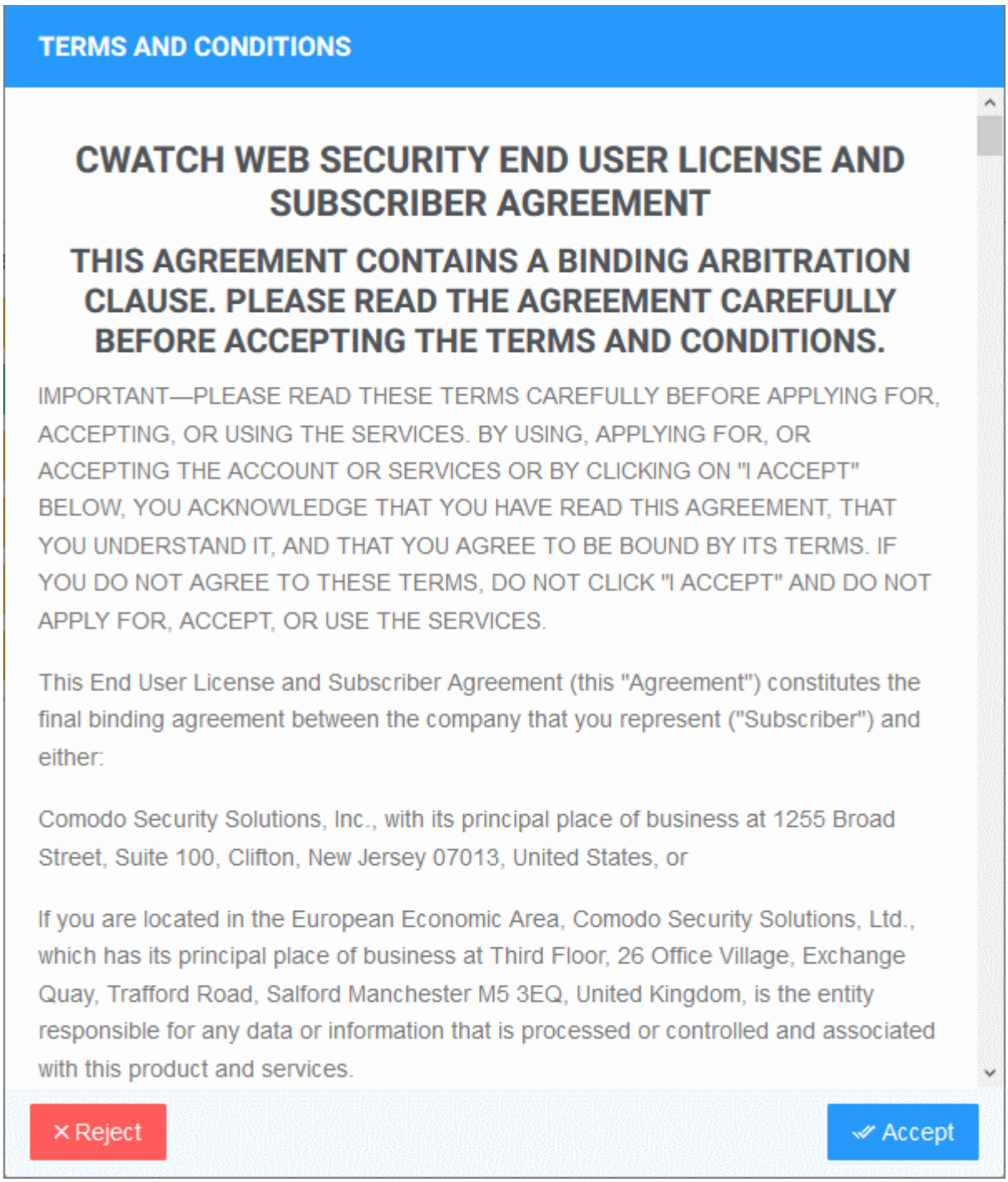


Your license is now activated.

- Click 'Enter Dashboard' to login to cWatch



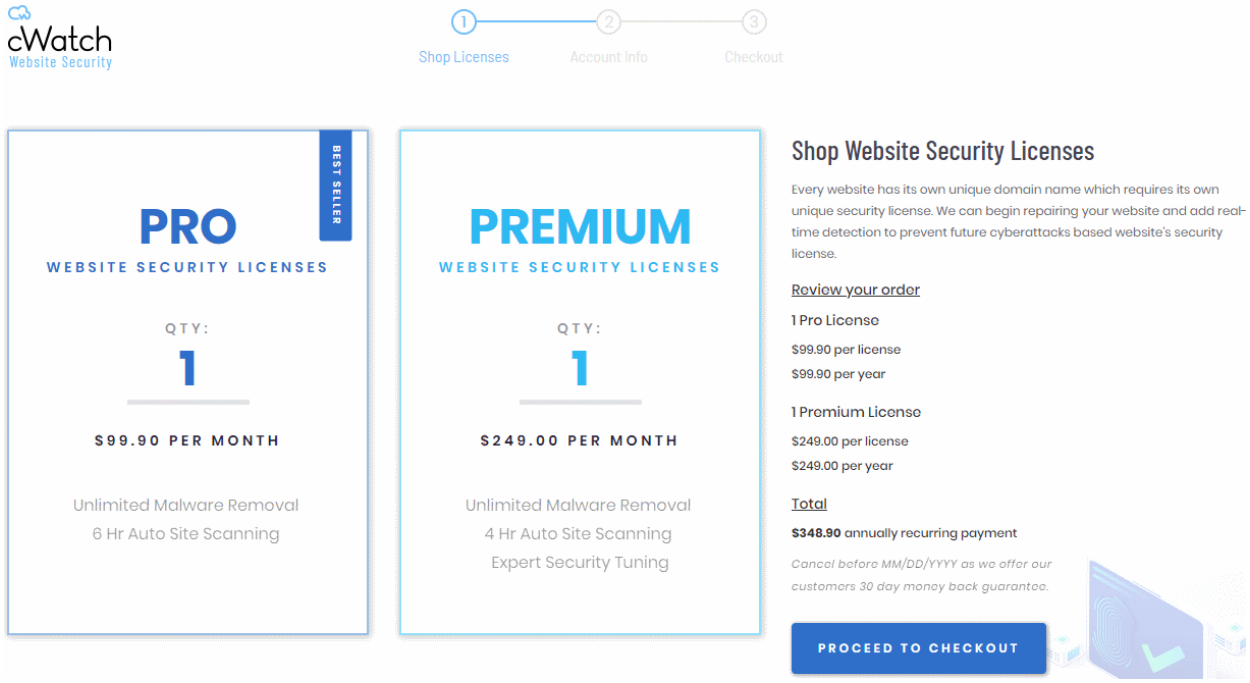
- Use your Comodo username and password to login to cWatch.
- You have to read and accept to the 'Terms and Conditions' on your first login.



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

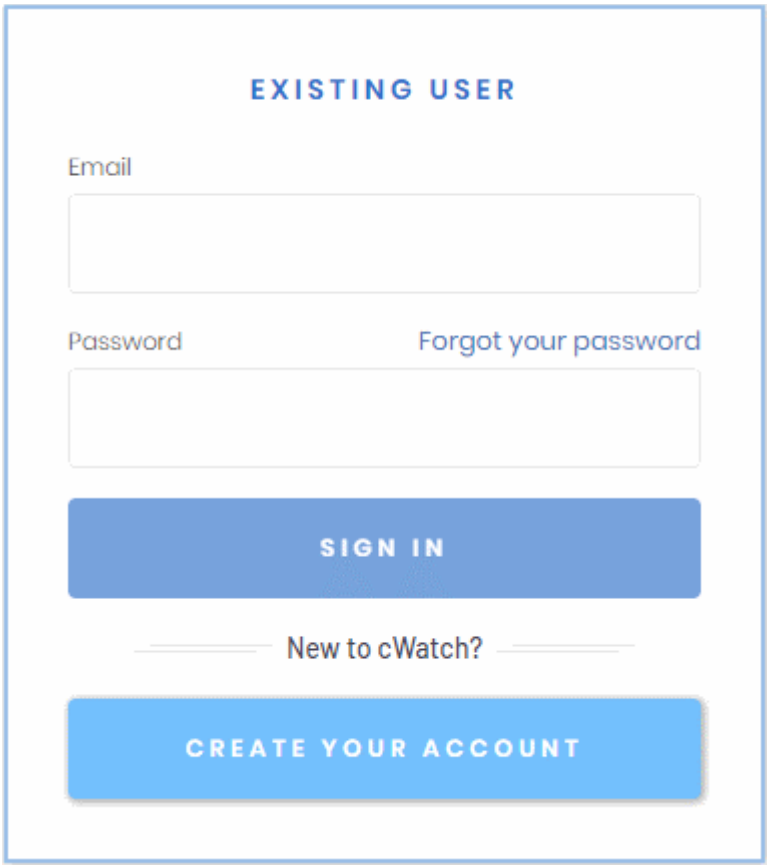
Purchase multi-domain license

Step 1 - Select Licenses

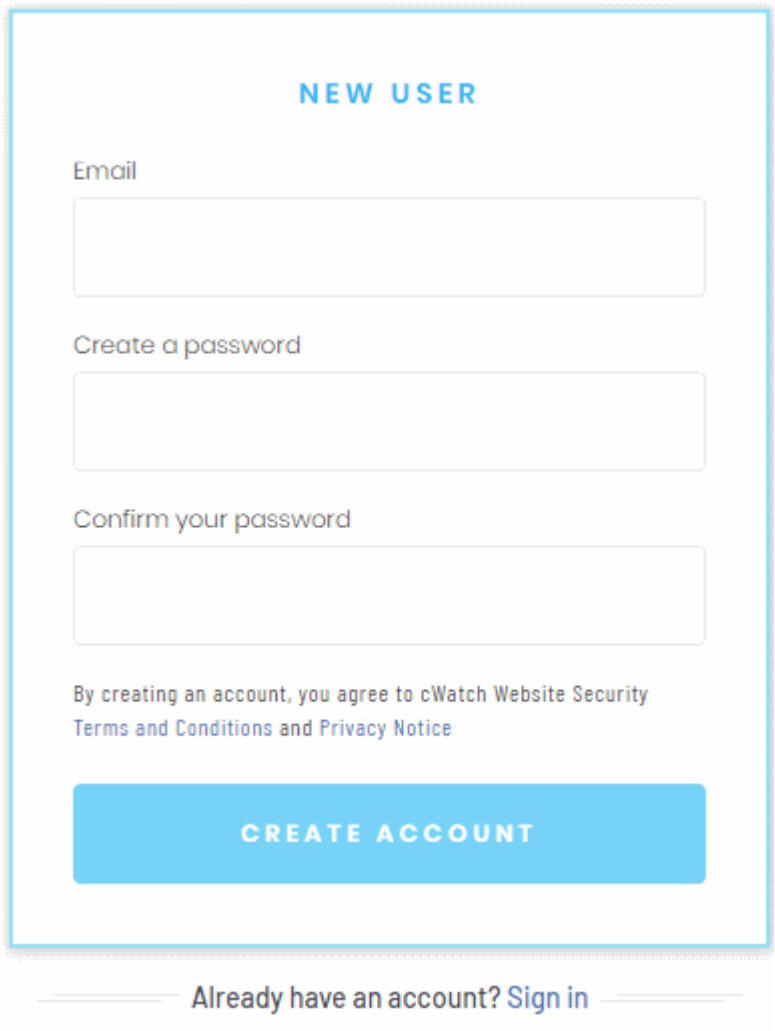


- Enter the number of licenses you want in the 'Pro' and/or 'Premium' boxes.
- Each license covers one domain or sub-domain
- Click 'Proceed to Checkout'

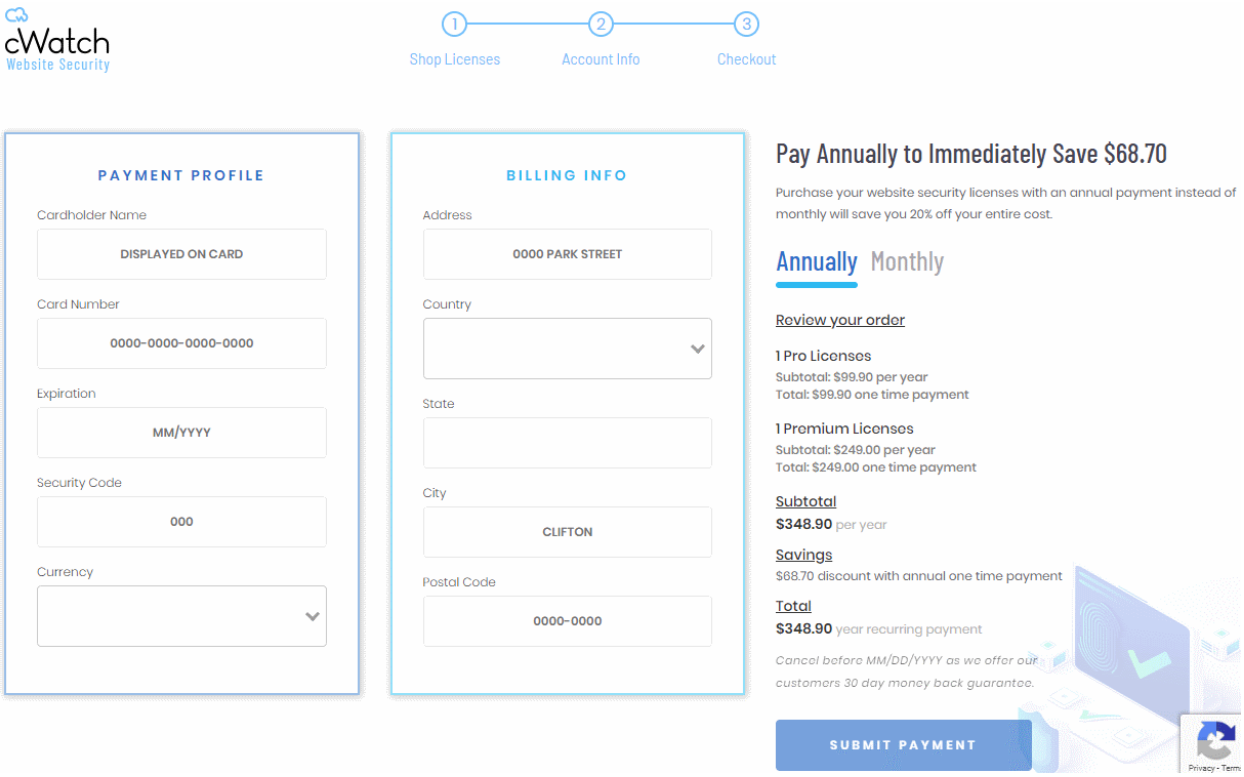
Step 2 - Enter your Comodo account Information



- 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

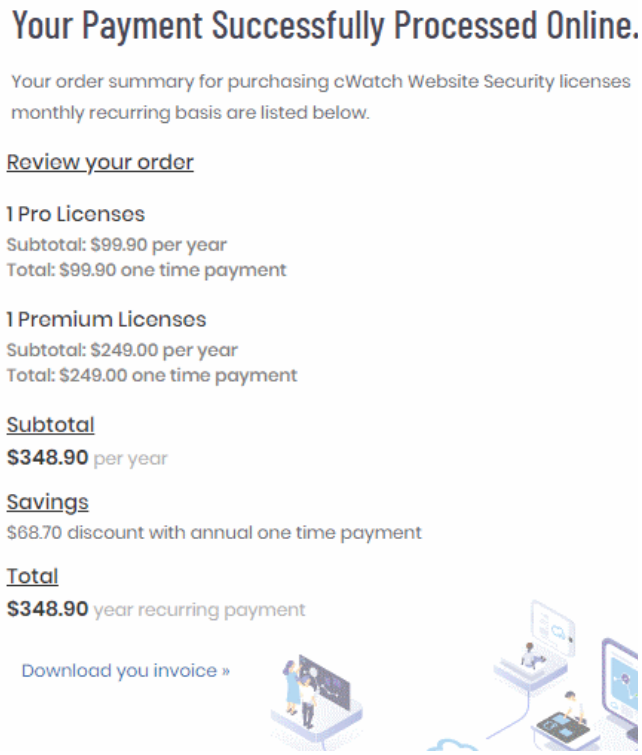


Step 3 - Enter Payment Details

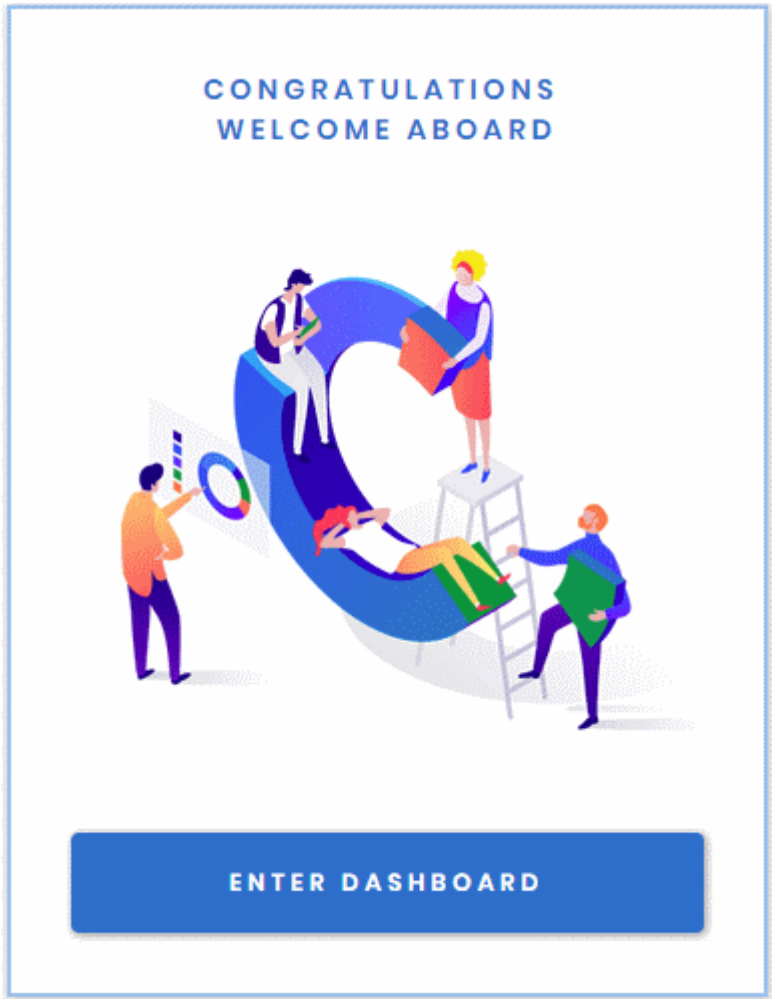


- Payment Profile - Enter your card details for recurring payments for auto-renewal of licenses.
- Billing Info - Enter your billing address
- Choose the period of license. The available options are 'Annually' or 'Monthly'.
- Click 'Submit Payment'

Step 4 - Activate License

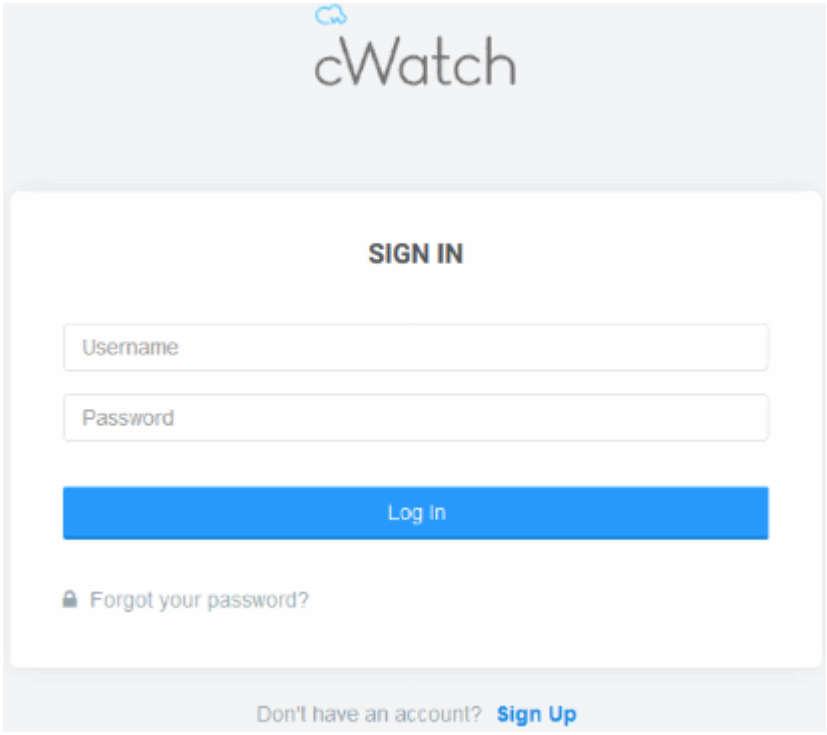


- Click 'Activate cWatch' to start protecting your website

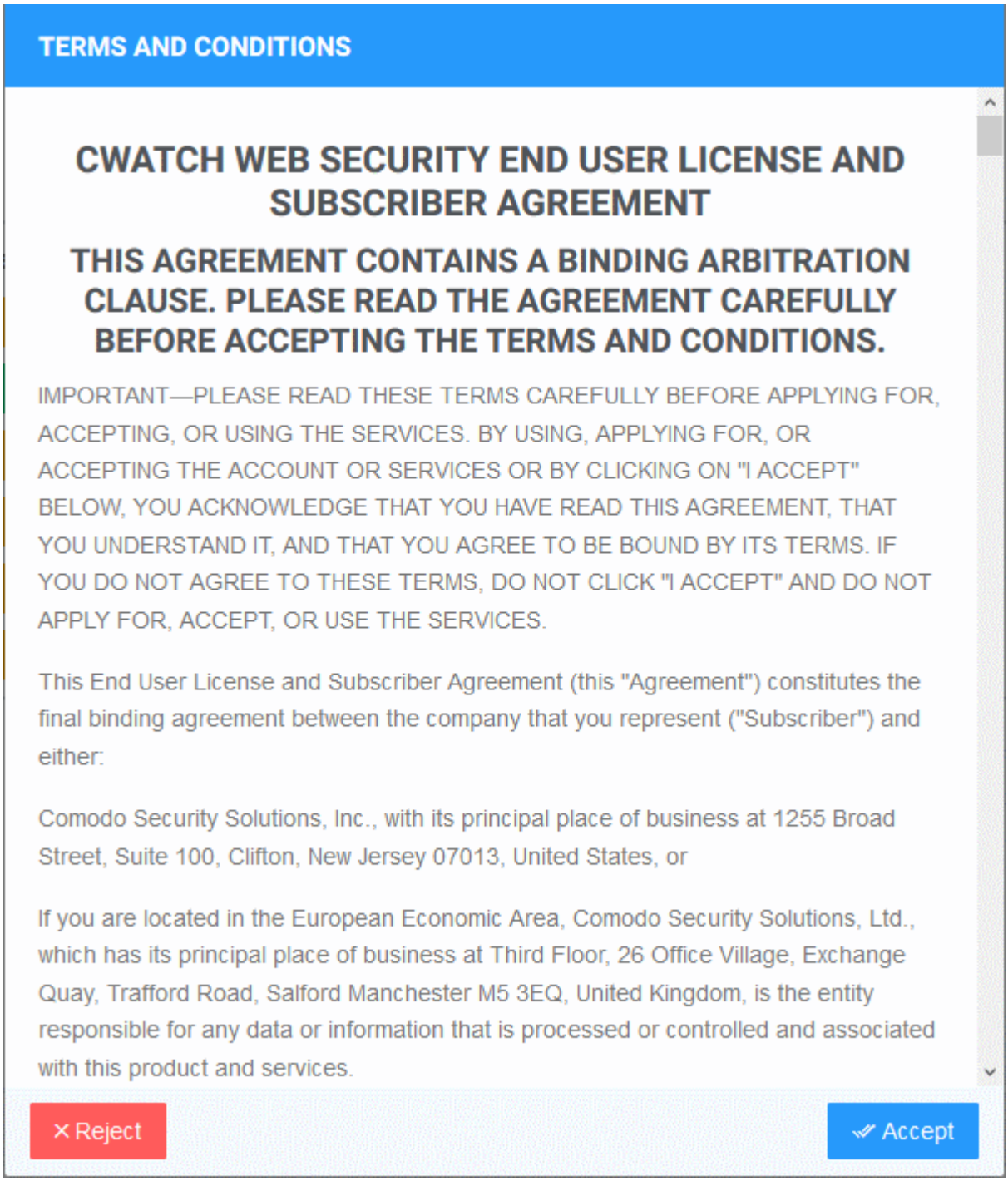


Your license is now active.

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

The three license types are:

- Basic
- Pro
- Premium

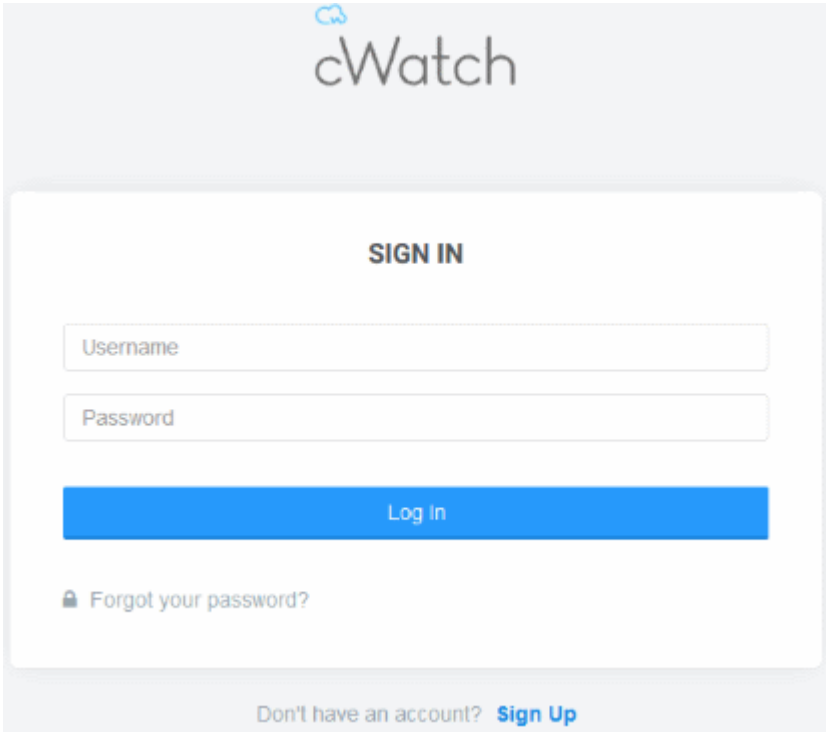
The following table shows the features available with each license type:

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

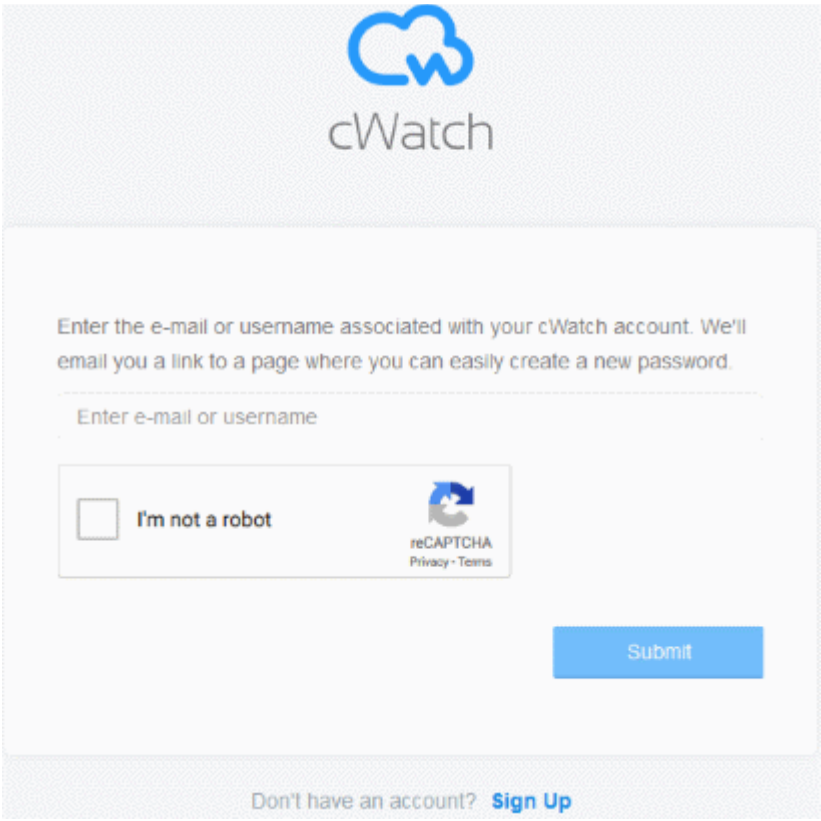


First time login

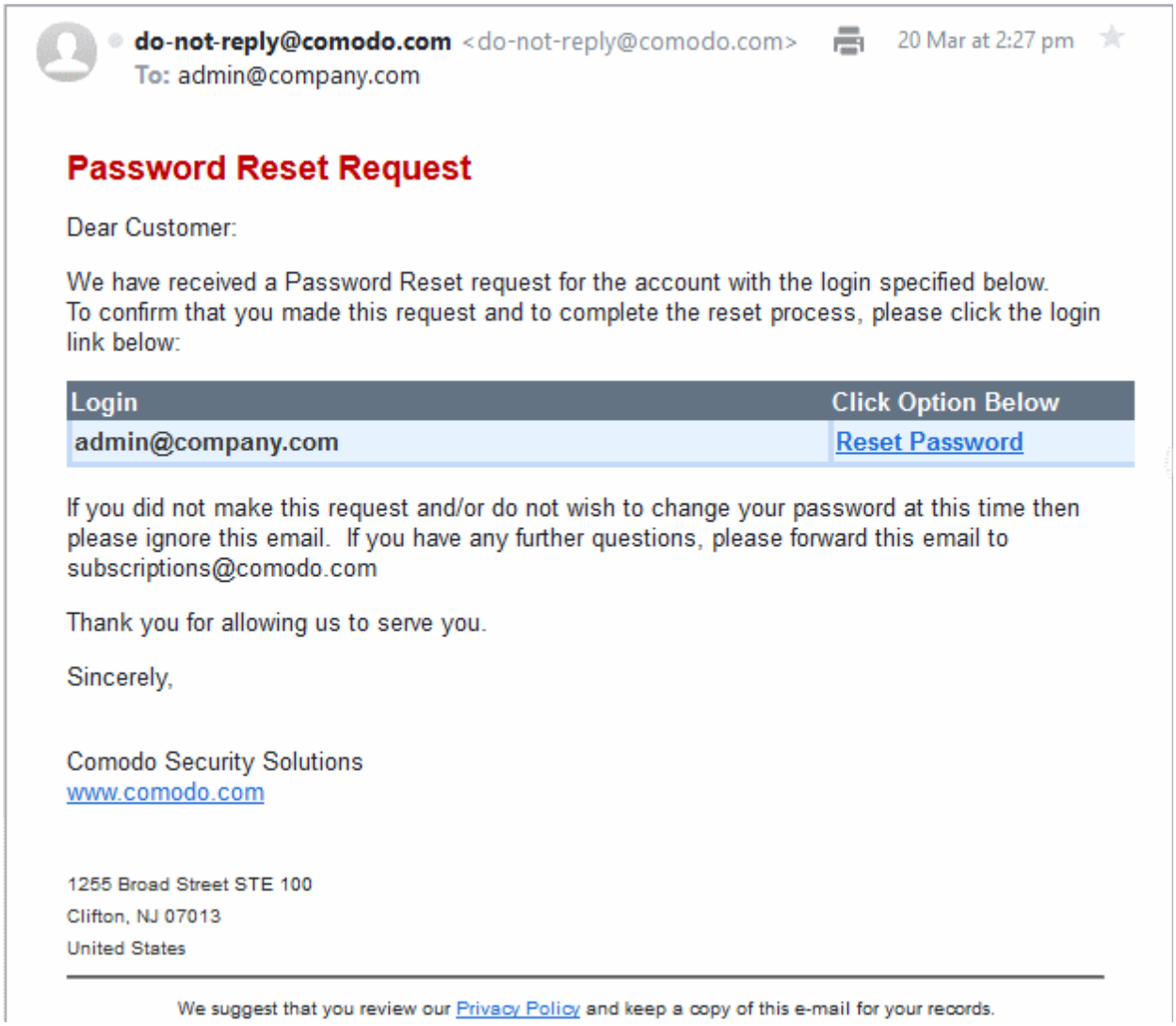
- Get your username and password from the cWatch confirmation email.
- After logging in, we strongly recommend you change your password for security reasons.

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.

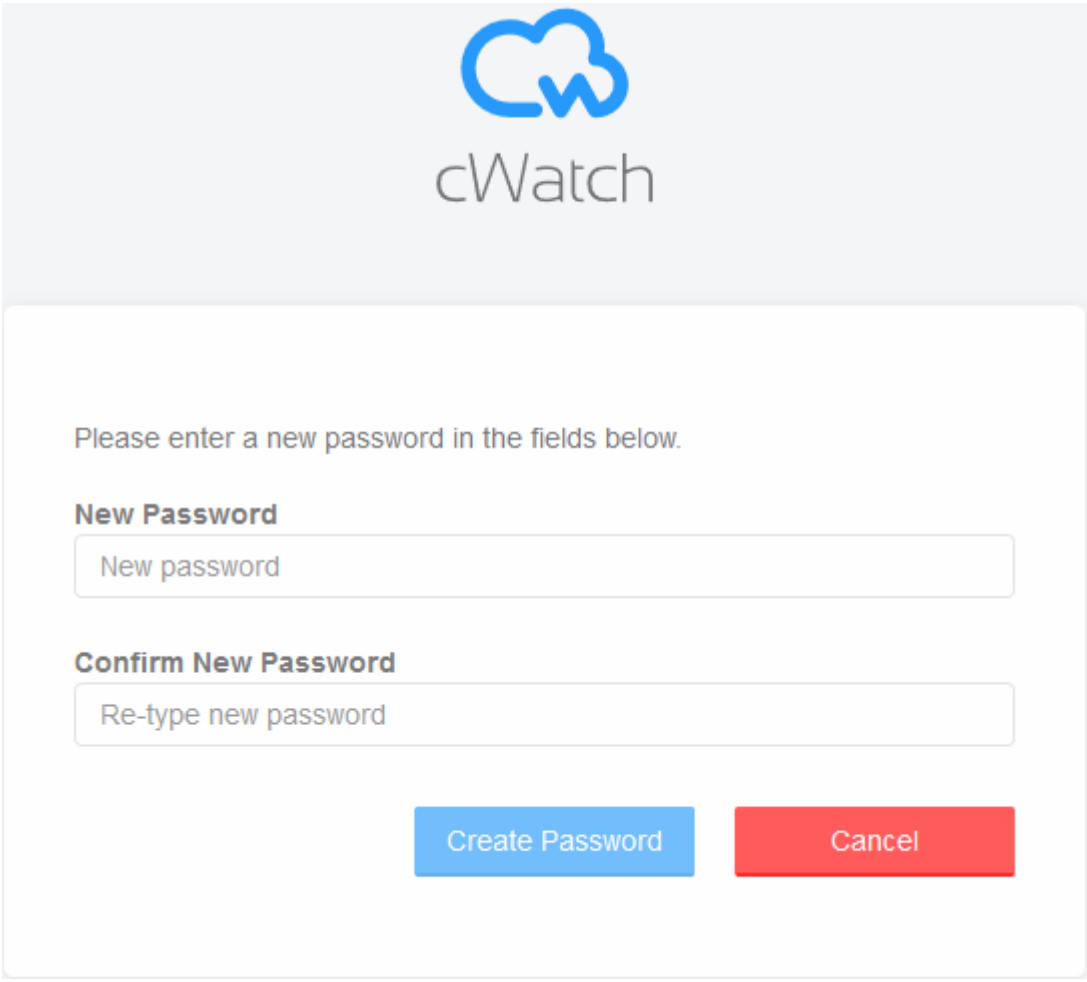
Sincerely,

Comodo Security Solutions
www.comodo.com

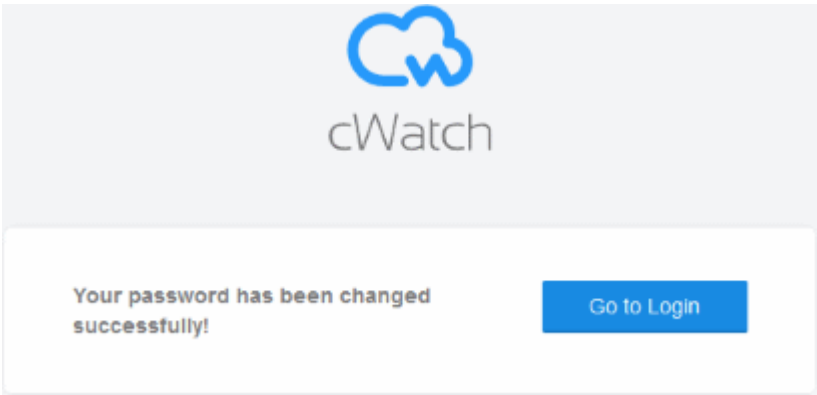
1255 Broad Street STE 100
Clifton, NJ 07013
United States

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

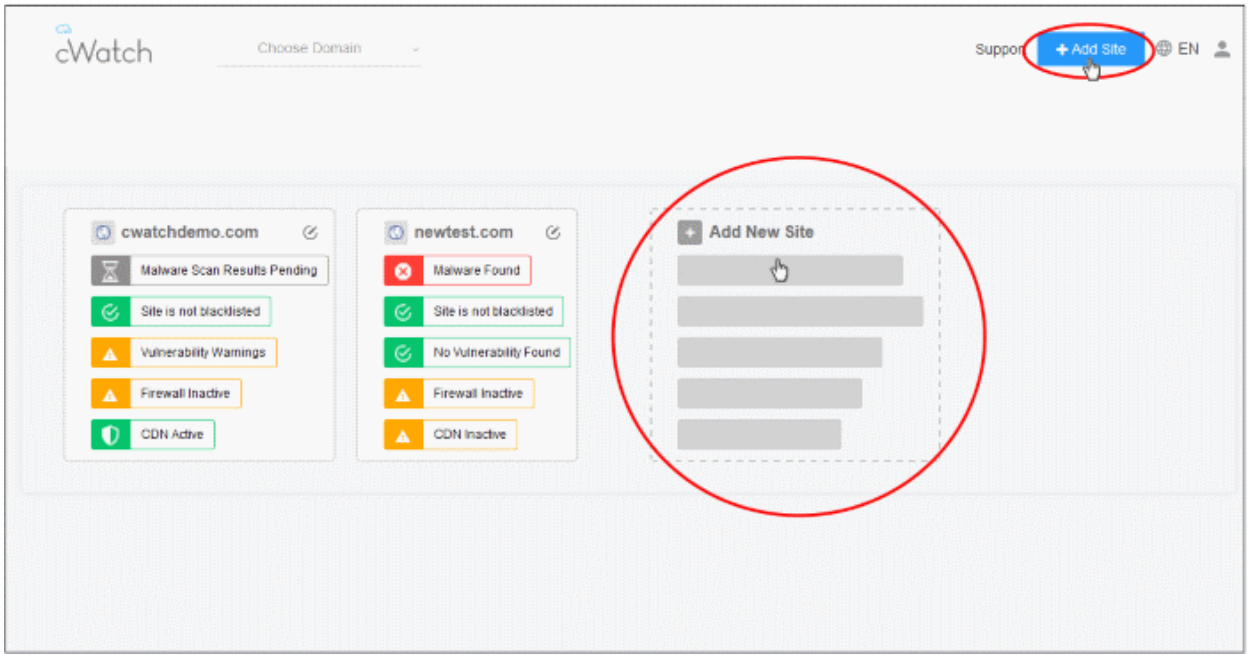
- You need to add websites to cWatch to enable protection and to use the content delivery network (CDN).
- The number of sites you can add depends on your license. See **License Types** more info.
- Once added, you can configure threat monitoring and CDN settings for each site.

Add a new domain

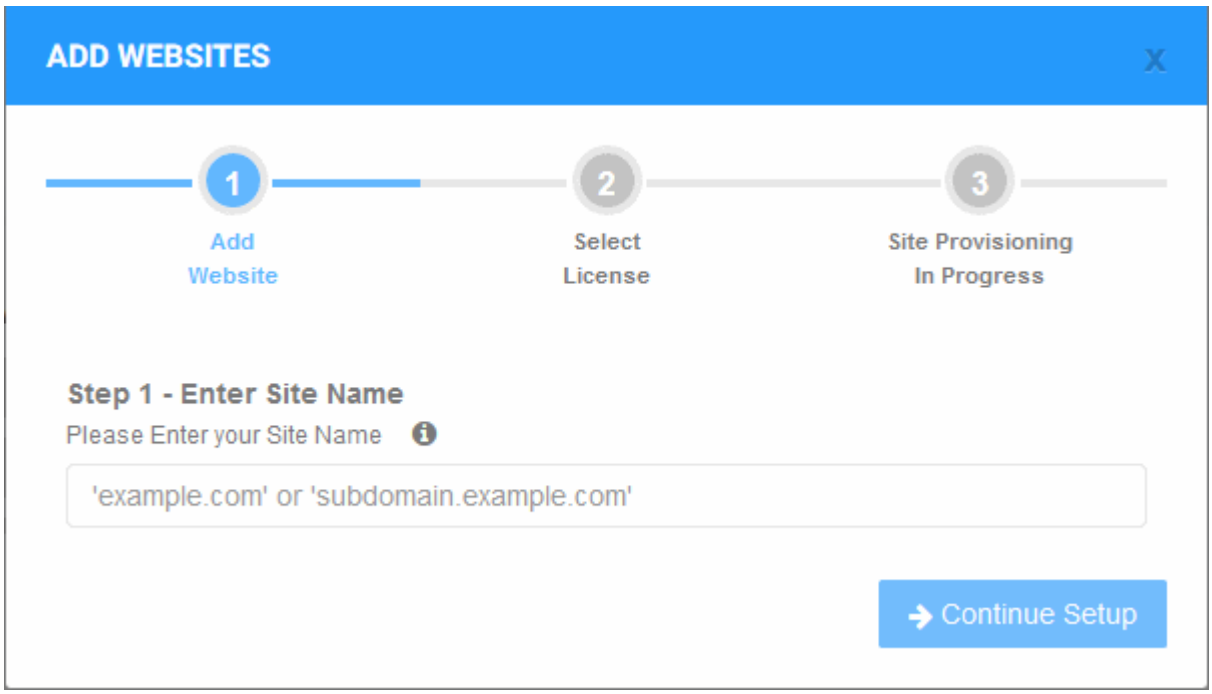
- Login to cWatch at **https://login.cwatch.comodo.com/login** with your username and password.

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

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



The 'Add Websites' wizard starts:

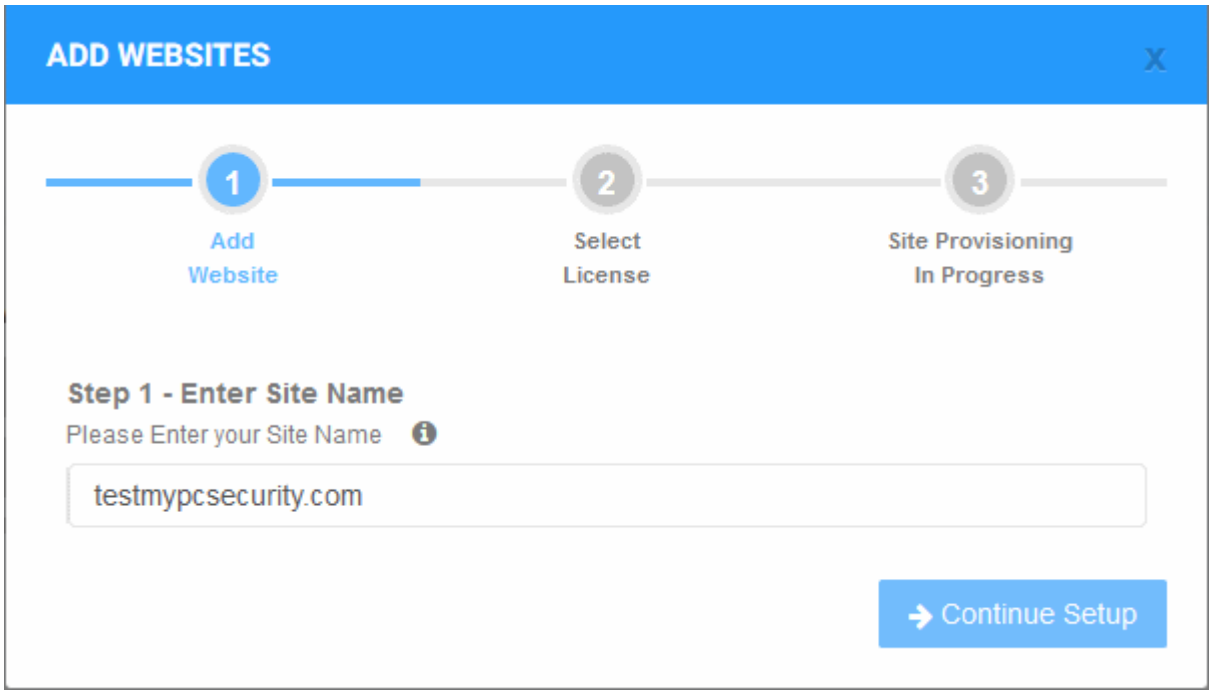


The wizard has three steps:

- **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.

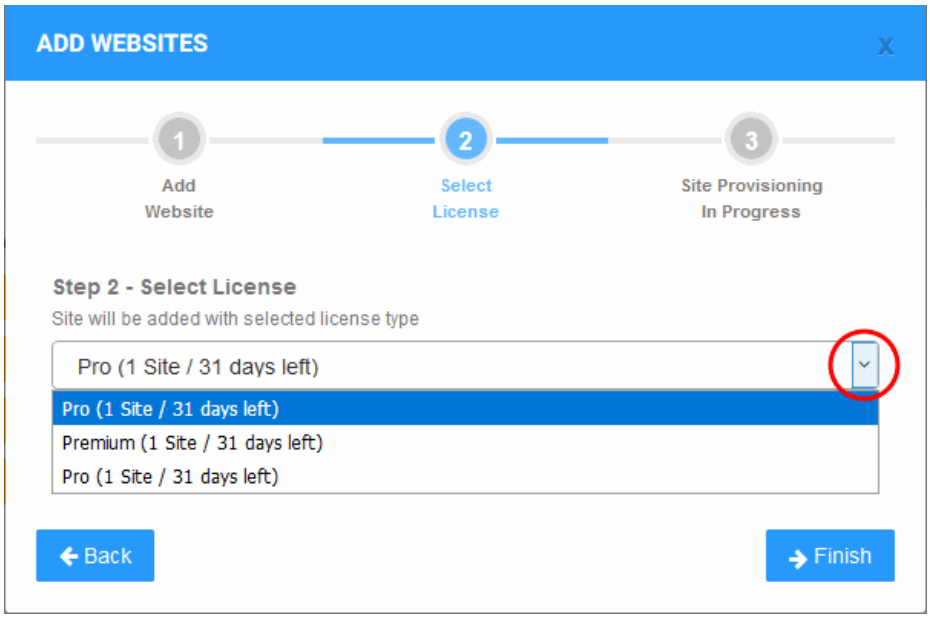


- Click 'Continue Setup' to move to the next step.

Step 2 - Select License

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

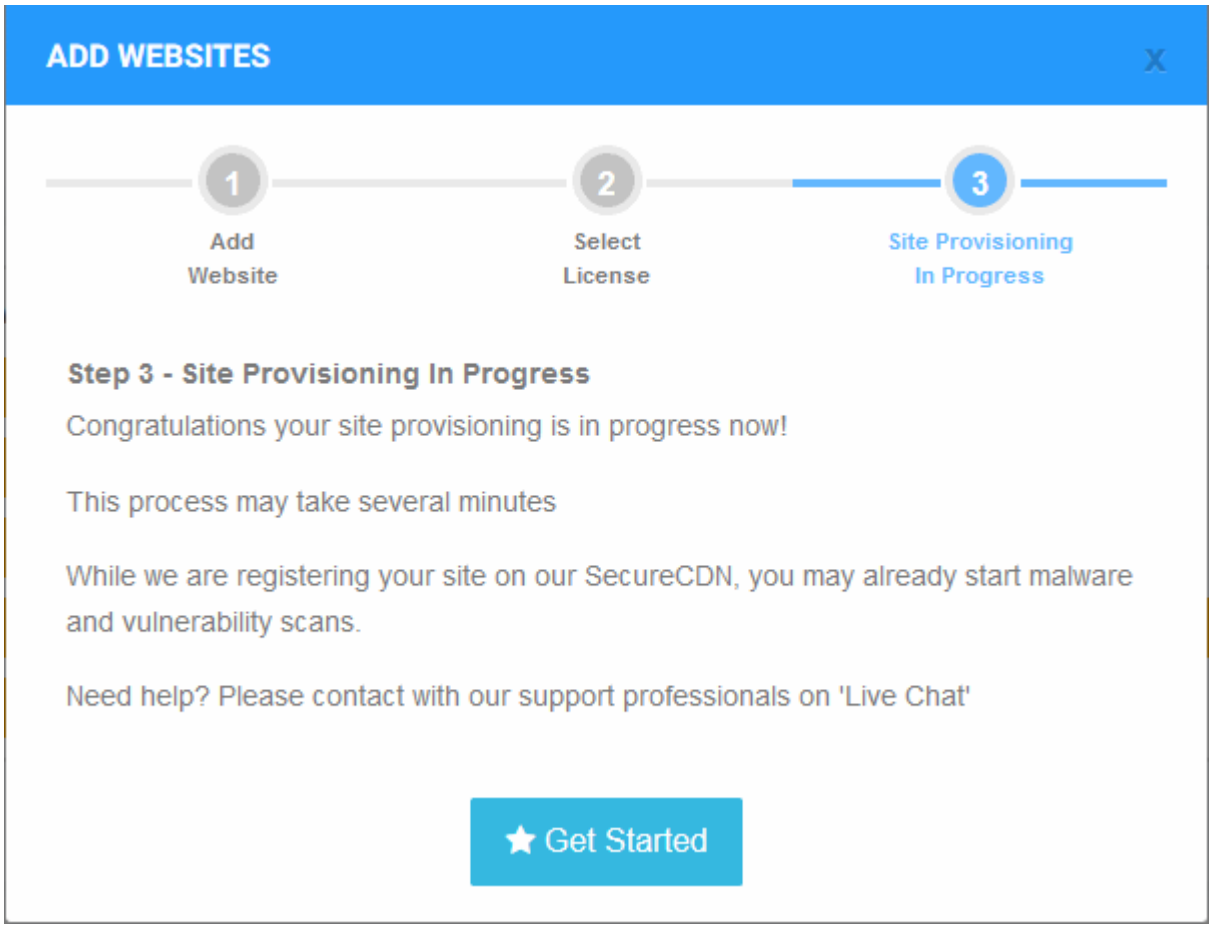
- cWatch features vary according to license type. See **License Types** for more details.
- The drop-down menu lets you select from all licenses you have purchased.
- Choose the type of license you wish to associate with the domain:



- 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**.

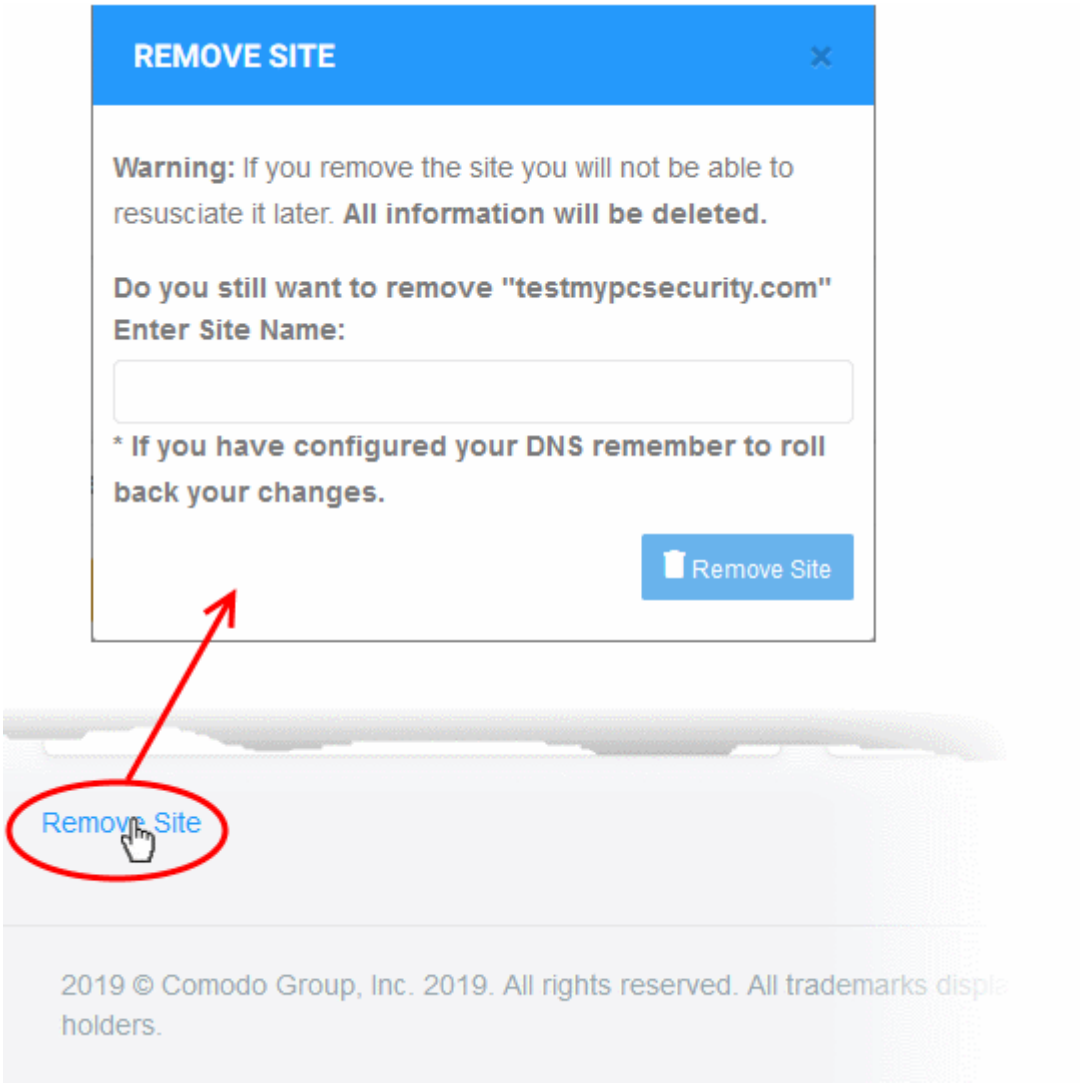
Tip: You can skip this step for now and add the CNAME to DNS later. See **DNS Configuration** for help with this.

- 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

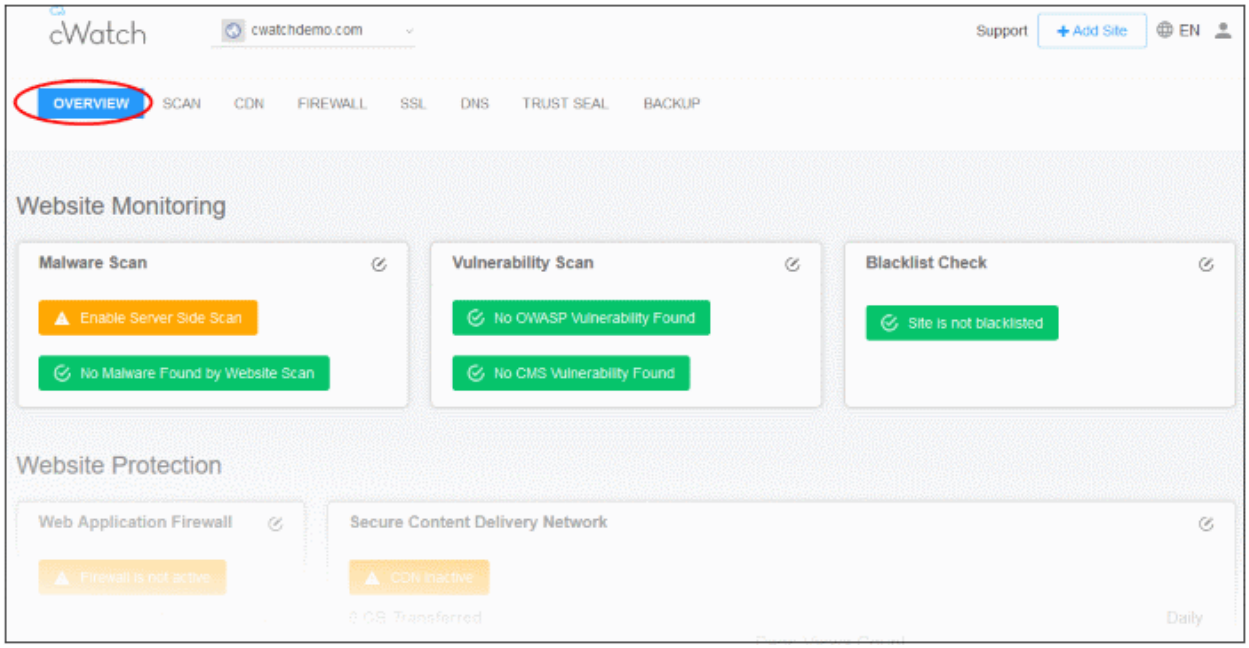
- The cWatch dashboard shows the security status of all protected domains.
- Click the 'cWatch' logo in the top-left corner to return to the dashboard at any time
- The drop-down to the right of the logo lets you change to a different site. Use the links in the top-menu to access each major area of cWatch.

- **Overview** – Shows security and performance data from each cWatch module. Click on a specific site tile to open its statistics and configuration pages. See **Website Overview** for more details.
- **Scan** – cWatch offers thee types of security scans:
  1) **Website Scans** - A first-level scan that checks front-end files for threats, blacklist status, missing headers, SSL errors, and more. The website scan runs automatically straight after you add a site to cWatch. No configuration required. See '**Website Scan**' if you need help with this.
  2) **Website Files Security Scans**– A full, deep-scan of your website's front-end and back-end files for all known threats. You can schedule malware scans to run at a time that suits you, and you can also configure automatic removal of discovered threats. You need to upload our .php file to the server to enable malware scans. See **Website Files Security Scans** for more details.
  3) **Vulnerability** – contains two types of scan:
     - **CMS vulnerability scans** - Identifies weaknesses in your content management system (CMS). You can enable weekly automatic scans on each protected site, and can also run on-demand scans at any time.

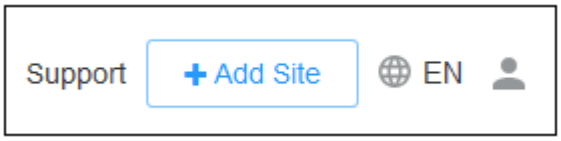
       The scanner supports the following CMS types:
       - WordPress
       - Joomla
       - Drupal
       - ModX
       - Typo3
     - **OWASP top-ten threats** – Scans for the top-10 threats identified by the Open Web Application Security Project (OWASP). You can schedule weekly automatic scans on each protected site, and on-demand scans at any time.

       See **Vulnerability Scans** for more details.
- **CDN** - Configure the cWatch content delivery network and view traffic for your site. This includes total data usage, status/error-code distribution, and the geographic locations from which your site was accessed. See **Content Delivery Network Metrics**
- **Firewall** - Configure Web Application Firewall (WAF) policies for the domain and create your own custom firewall rules. View attack and threat statistics on your domains. See **Firewall** for more information.
- **SSL** – Secure the traffic between the CDN edge servers and your website visitors. You can get a complimentary SSL certificate from Comodo. Alternatively, you can upload an existing certificate. See **SSL Configuration** for more details.

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

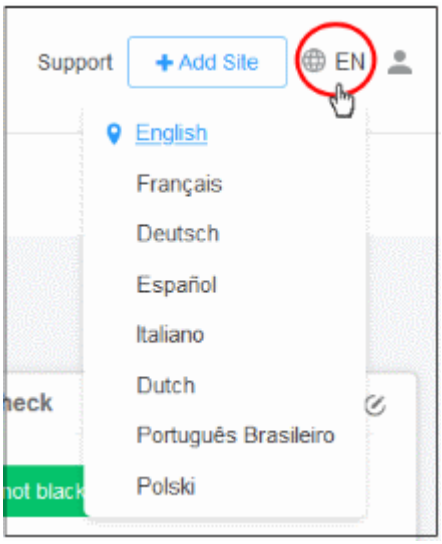


- The options on the top right let you to add a new website, select your language, manage your profile, view your subscriptions, submit a support ticket and logout:

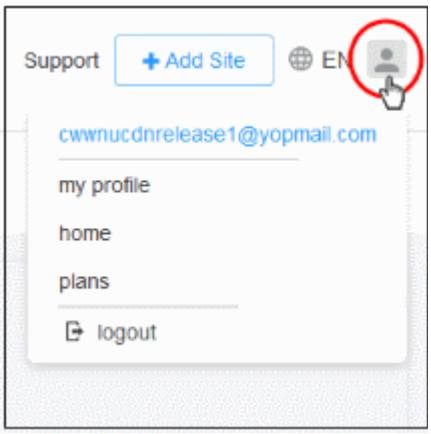


- Starts the site enrollment wizard. See **Add Websites** for more details.

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



- Click to manage your profile and view your subscriptions.



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

- Help and support:

Support

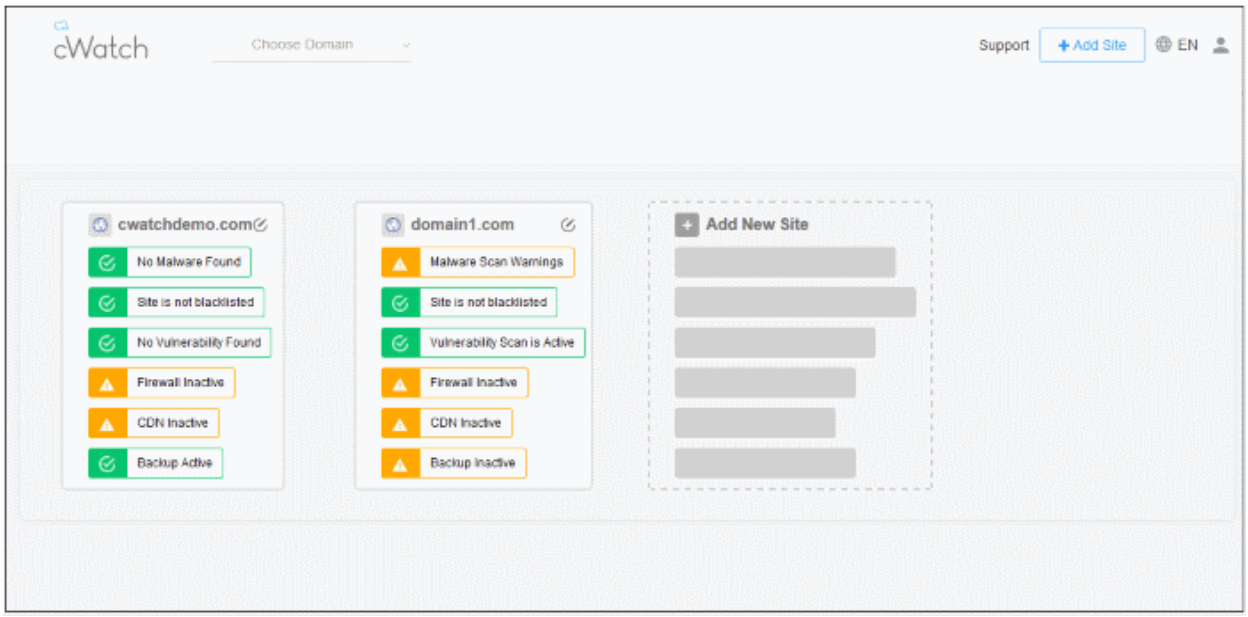
- Click the 'Support' link to submit tickets. See '**Get Support**'

The footer contains copyright information, terms and conditions:

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

3 The Dashboard

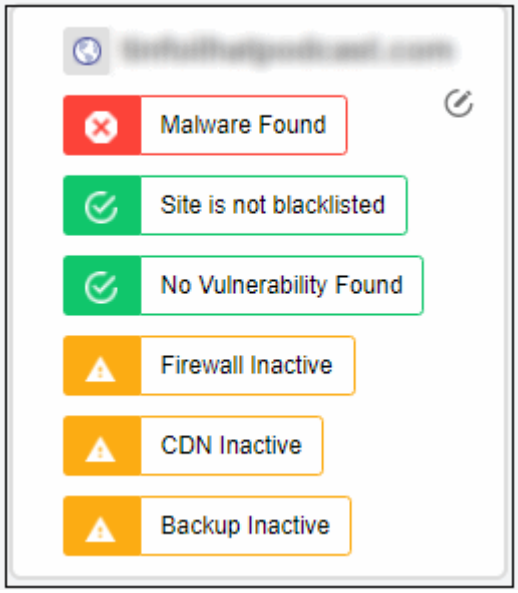
- Click the cWatch logo at top-left to open the dashboard.
- The condensed view shows a security summary for each site on your account:



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

Condensed view

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



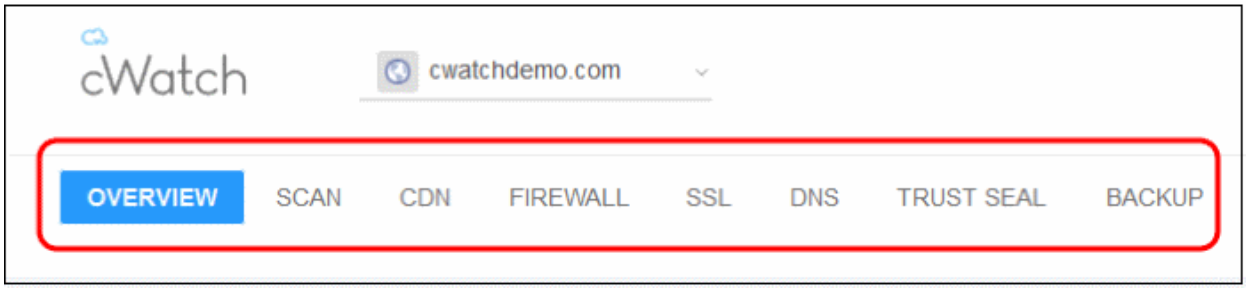
  - Green - No threats found in the category
  - Yellow - Requires action. For example, activate the firewall or run a malware scan.
  - Red - Threats found in this category
- Click the ✎ at the top left corner of a tile to go to the domain overview page. See **Website Overview** for more details.
- Click a row to go to the respective configuration or results page

Examples:

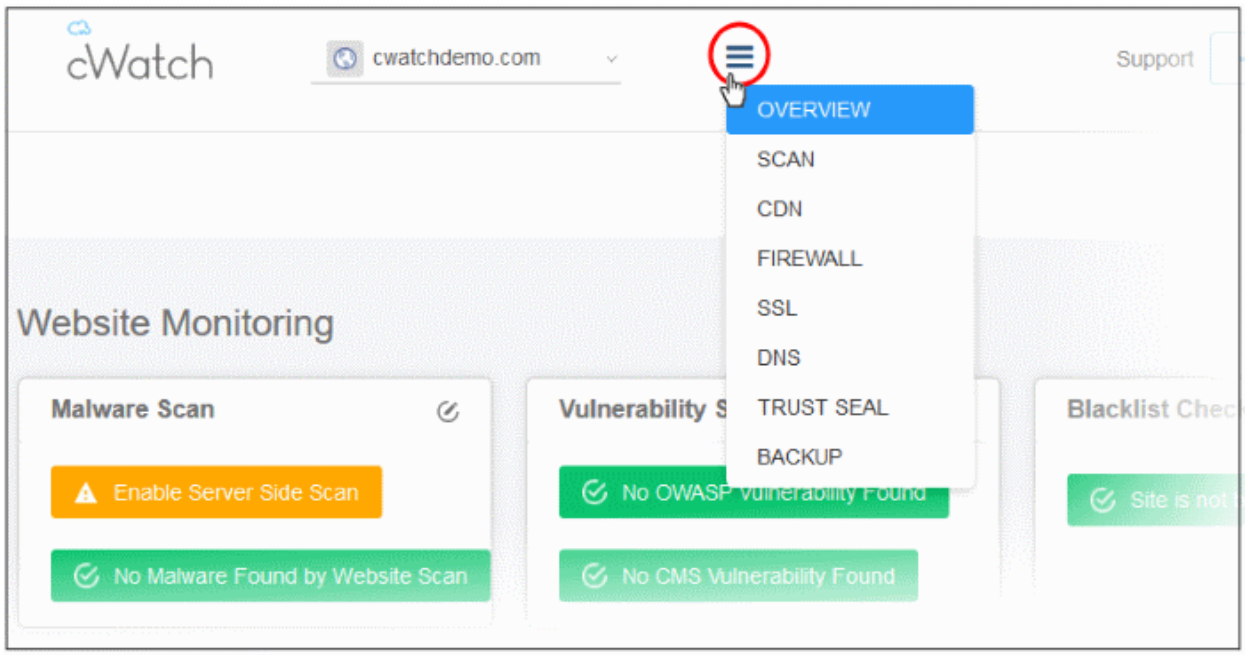
- Firewall Inactive - Opens the web application firewall settings page. See **Configure WAF Policies**.
- CMS vulnerability found - Opens the vulnerability scan results page. You can review the results and take further actions. See **CMS Vulnerability Scans** for more details.

4 Website Data and Settings

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



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



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

     You need to upload our .php file to the server to enable malware scans. See **Configure Website Files Malware Scan Settings**
  3. **Vulnerability** – two types:
     - **CMS scans** - Identify weaknesses in your content management system (CMS). You can enable weekly automatic scans on each protected site, and can also run on-demand scans at any time.

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

    - Typo3
  - **OWASP top-ten threats** – Scans for the top-10 threats as identified by the Open Web Application Security Project (OWASP). You can enable weekly automatic scans on each protected site, and can also run on-demand scans at any time.

  See **Vulnerability Scans** for more details.

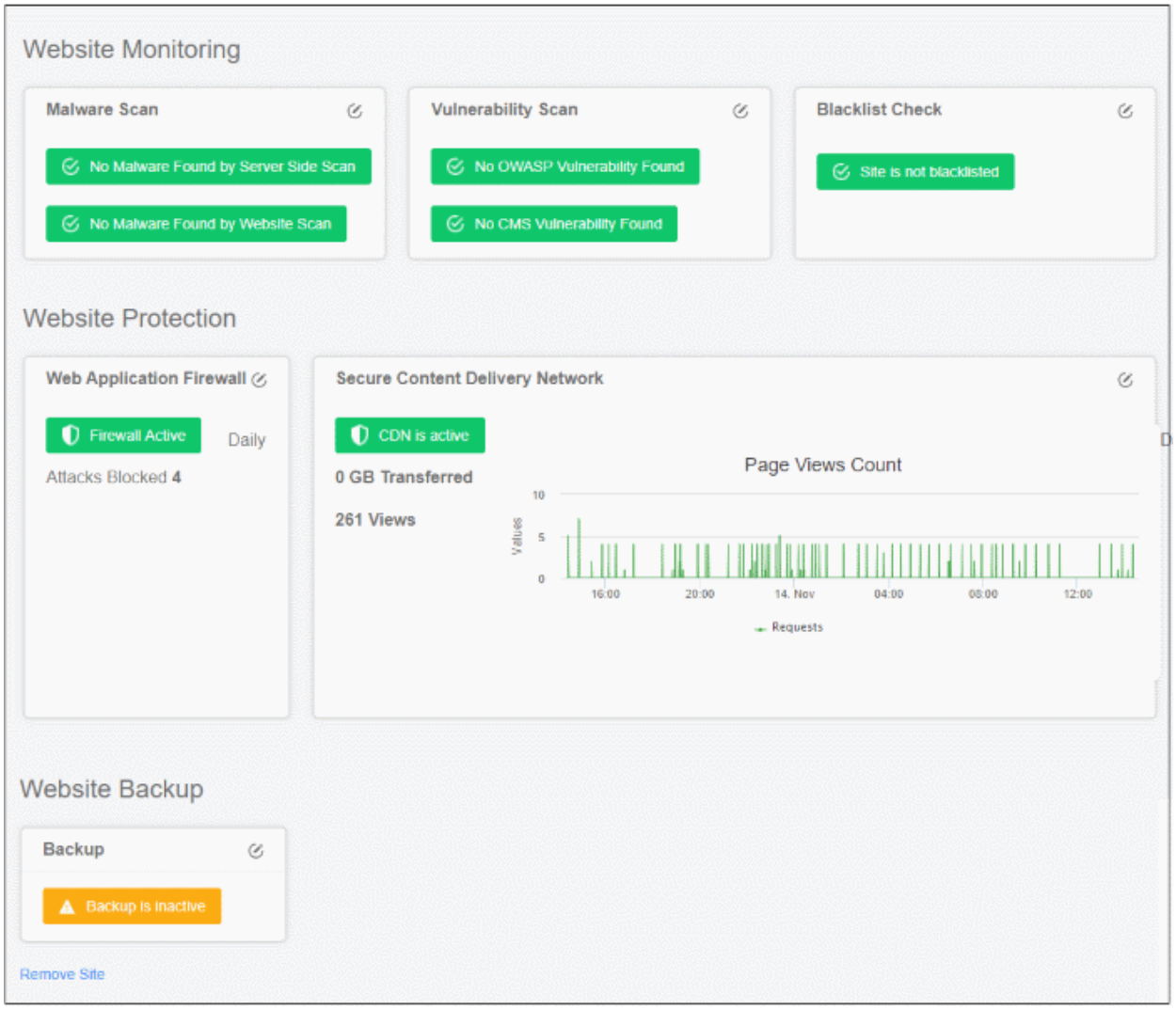
- **CDN** - Configure the cWatch content delivery network and view traffic for your site. This includes total data usage, status/error-code distribution, and the geographic locations from which your site was accessed. See **Content Delivery Network Metrics**
- **Firewall** - Configure Web Application Firewall (WAF) policies for the domain and create your own custom firewall rules. View attack and threat statistics on your domains. See **Firewall** for more information.
- **SSL** - Secure traffic between the CDN edge servers and your website visitors. You can get a complimentary SSL certificate from Comodo. Alternatively, you can upload an existing certificate. See **SSL Configuration** for more details.
- **DNS** - Configure DNS and nameservers in order to enable cWatch protection. See **DNS Configuration** for more information.
- **Trust Seal** - Add a cWatch site seal on managed websites. There are two types of seals: 'Malware Free' and 'Protected'. See **Add Trust Seal to your Websites** for more details.
- **Backup** – Backup your entire website and databases to our highly secure cWatch servers. Restore your website with a single click. See '**Back up your Website**' for more information.

4.1 Website Overview

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

Open the overview page

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



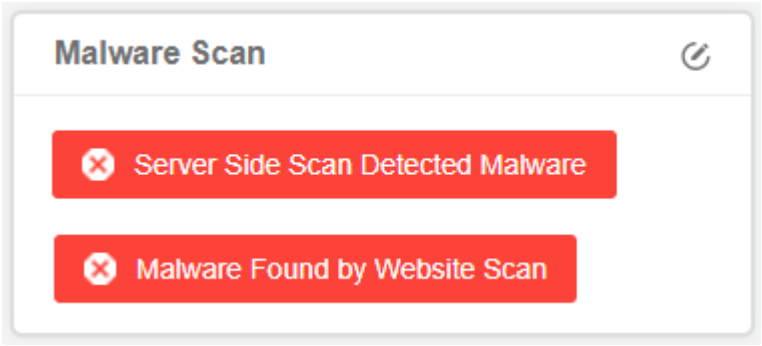
- Tiles are broken down into three categories:
  - **Website Monitoring**
  - **Website Protection**
  - **Website Backup**
- Each tile shows data from a different cWatch module. Threat information is color-coded as follows:
  - Green - No threats found / The module is running OK
    - Click the stripe 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 **Website Files Security Scans** for more details.

Website Monitoring

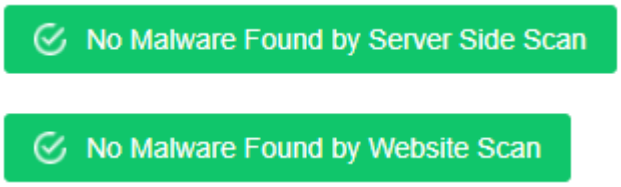
- Shows key information from cWatch scans. This includes malware scan results, vulnerability scan results, and site reputation checks.

Malware Scan:

The result of the most recent manual or scheduled scan on the website and site files.



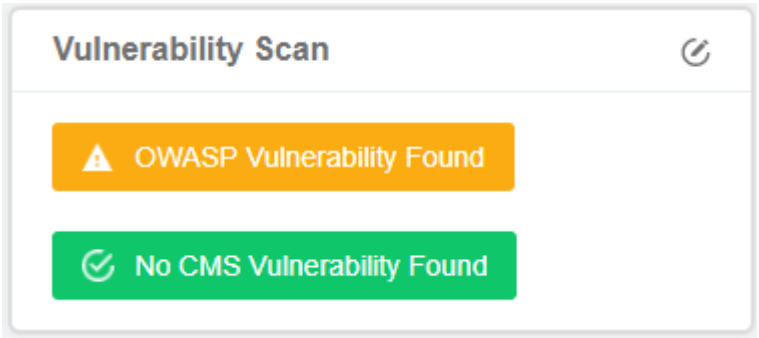
- Click a stripe to see full malware details and read threat remediation advice.
- If no threats are found, the following message is shown on the tile:



You need to upload the cWatch agent to your site to enable scans on website files. An alert message is shown if not enabled:

- Click the stripe to enable the 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.

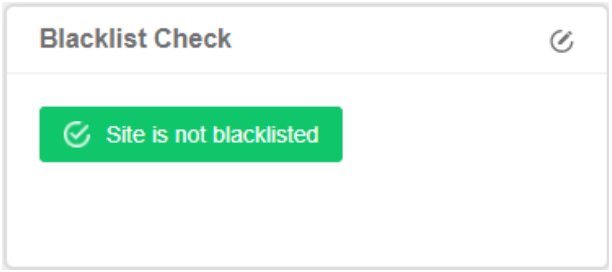
  - Note - cWatch automatically blocks any OWASP threats it finds.
- Click the stripe to go to the 'Vulnerabilities' page.
  - Click 'View full report' under OWASP
  - Then click on a vulnerability category to view all files affected by that attack type.
  - The file list page also has instructions to 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

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.

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



Blacklist Check - The result of the most recent automatic or manual website scan.

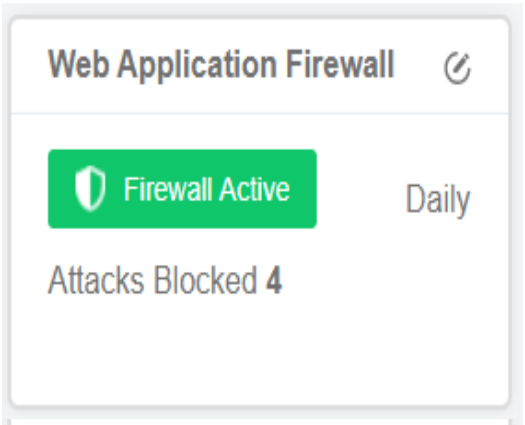
- **Site is blacklisted / Site is not blacklisted** – States whether or not your site is listed as harmful on one of the major website blacklists.

Click the stripe to open the website scan page.

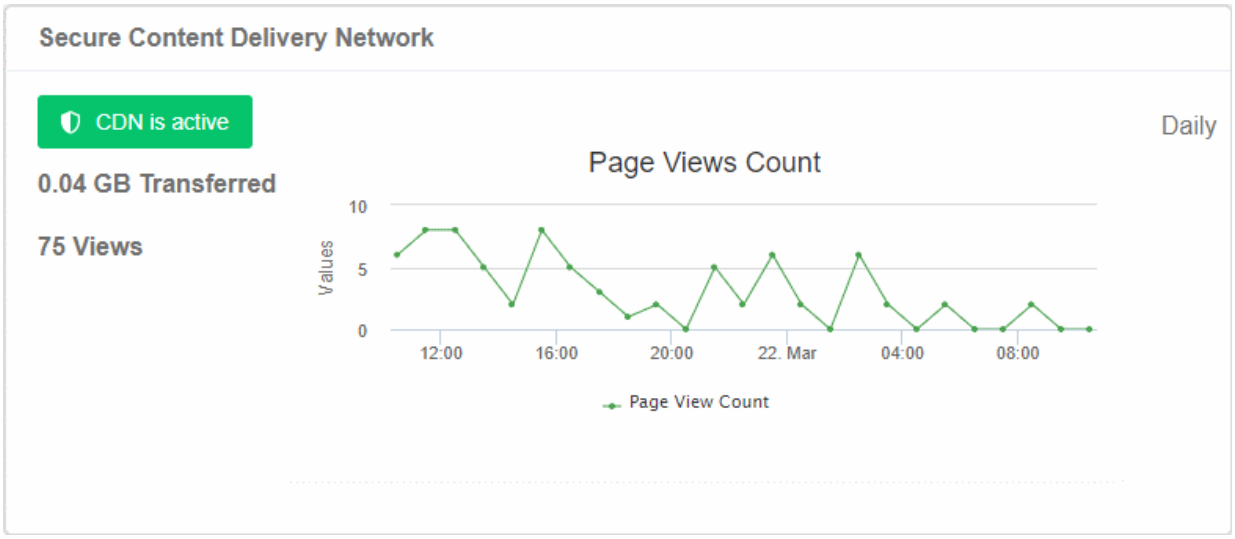
See '**Website Scans**' for more information.

Website Protection

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



- **Web Application Firewall** - Number of incidents detected by the firewall, and the number of attacks prevented. You can configure these items in your web application firewall rules.
  - Click the stripe to configure the WAF policies and create custom firewall rules for the domain.
  - The period covered by the report is shown at the right of the stripe
- **Attacks Blocked** - Number of incidents identified as potential intrusion attempts and blocked



Secure Content Delivery Network

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

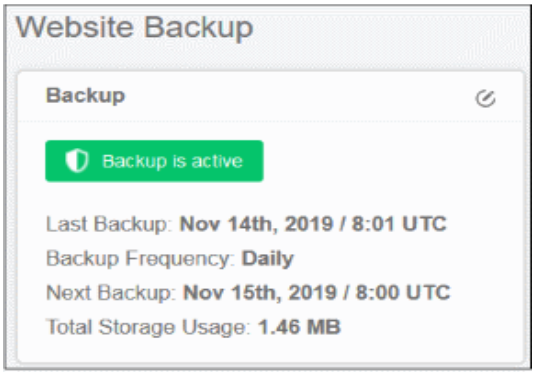
Note: The CDN statistics are shown only for websites configured to use the CDN service.

- You need to add a CNAME to your site's DNS record to use the CDN. This record is auto-generated by cWatch.
- Click 'Settings' > 'CDN' > 'Settings' > 'Activation' to view the CNAME record for your site.
- If you haven't configured the CNAME then no data is shown here.
- Click 

to start the configuration process.
- See **Content Delivery Network Metrics** for more details about CDN statistics.

Website Backup

You can backup your website files and databases to remote servers. The backup tiles shows whether backup is active or inactive and other details. You should have purchased a backup license and configured backup settings. **Click here** for more information.



Backup – Shows whether backup is active or not.

- Last Backup – The most recent backup of website files and database.
- Backup Frequency – How often the files are backed up.
- Next Backup – Upcoming scheduled backup date and time.
- Total Storage Usage – Backup storage size used

Click the stripe to open the backup section.

'Backup is inactive' message is shown if:

- You have not purchased a backup license

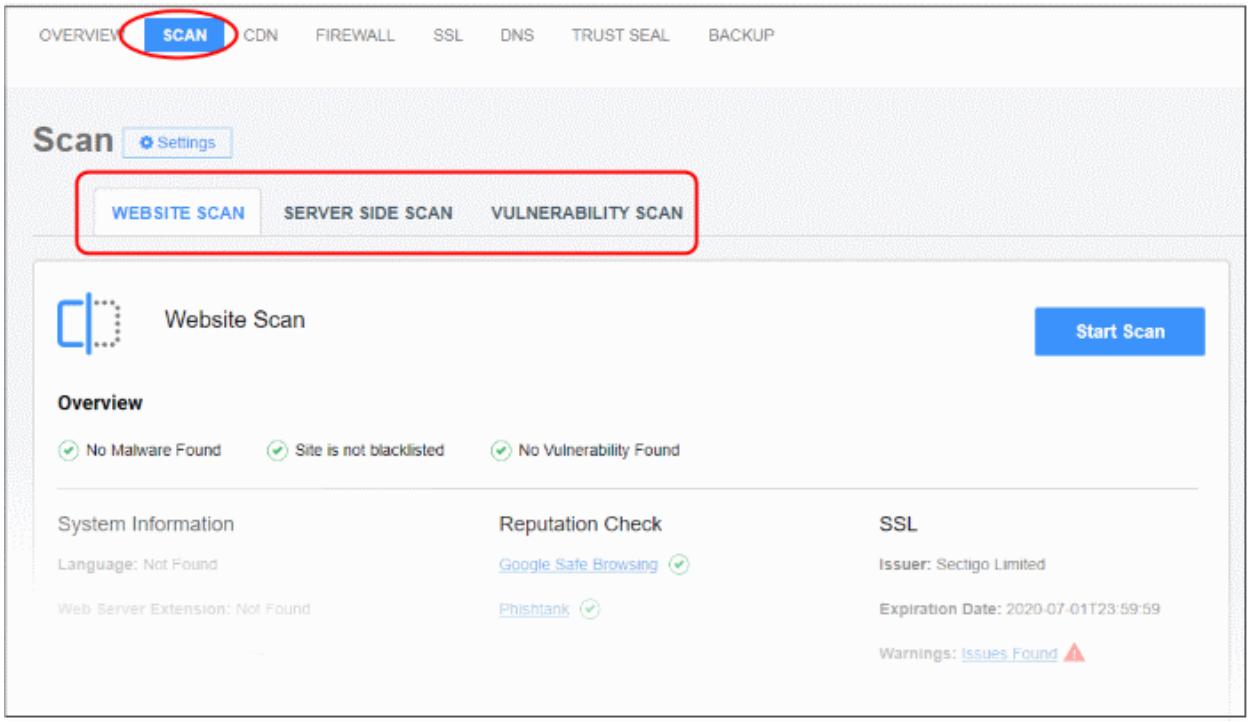
- Backup option is disabled

4.2 Security Scans

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

- **Website Scan** – An automatic scan that runs immediately after you add a site to cWatch. Website scans require no configuration are a fast and convenient way to identify threats.
- The scan searches front-end pages for threats, missing security headers, SSL errors, and checks the site's blacklist status. You can run website scans on-demand at any time.
- **Website Files Security Scan** – An in-depth scan of files on the webserver for known malware and viruses. The scan checks both front-end and back-end files, including perl, php, asp.net and SQL.
  You can schedule regular scans to run at times of your choice, and have any discovered malware automatically removed. You need to upload the cWatch agent to your server to enable this type of scan.
- **Vulnerability Scan** – A scan for content management system (CMS) vulnerabilities and for top ten vulnerabilities published by the Open Web Application Security Project (OWASP).

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



Click the following for more information about each scan:

- **Website Scans**
- **Website Files Security Scans**
- **Vulnerability Scans**

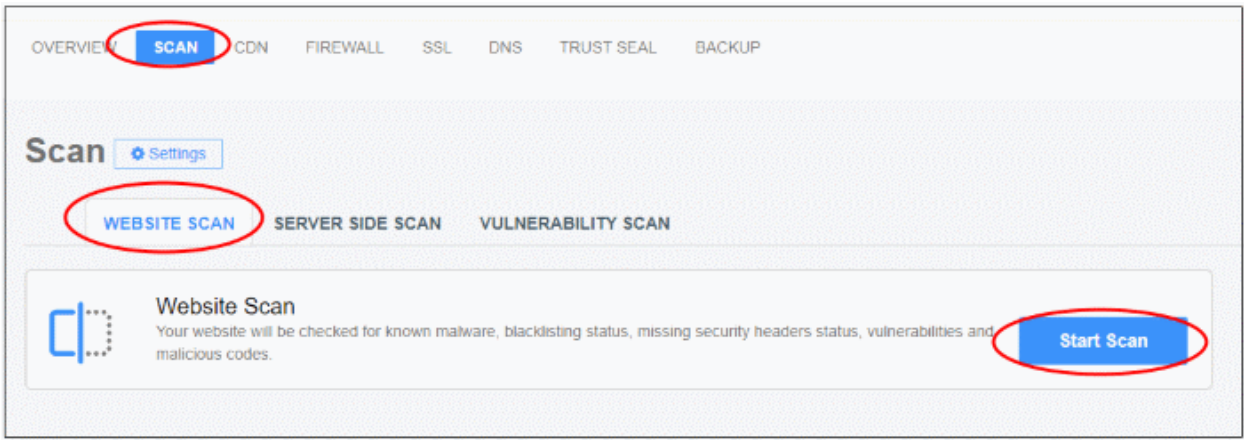
4.2.1 Website Scans

- The website scan checks your front-end web-pages for vulnerabilities, errors and known malware. It is a good, 'first-level' check of threats on your site, but you should enable the full malware scanner for long-term protection.
- The website scan checks the following items:
  - Javascripts, iframes and malicious links
  - Safe browsing status (blacklist status)
  - SSL certificate errors
  - Content Management (CMS) errors
  - HTTP errors and missing security headers
- The website scan starts automatically right after you add a website

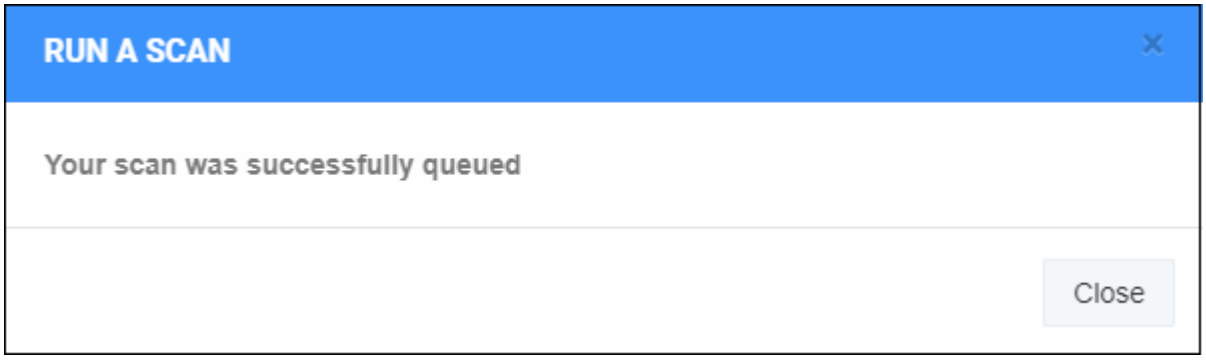
Run Website Scans and View Results

You can run a manual website scan every two hours. You can also **schedule a website scan**.

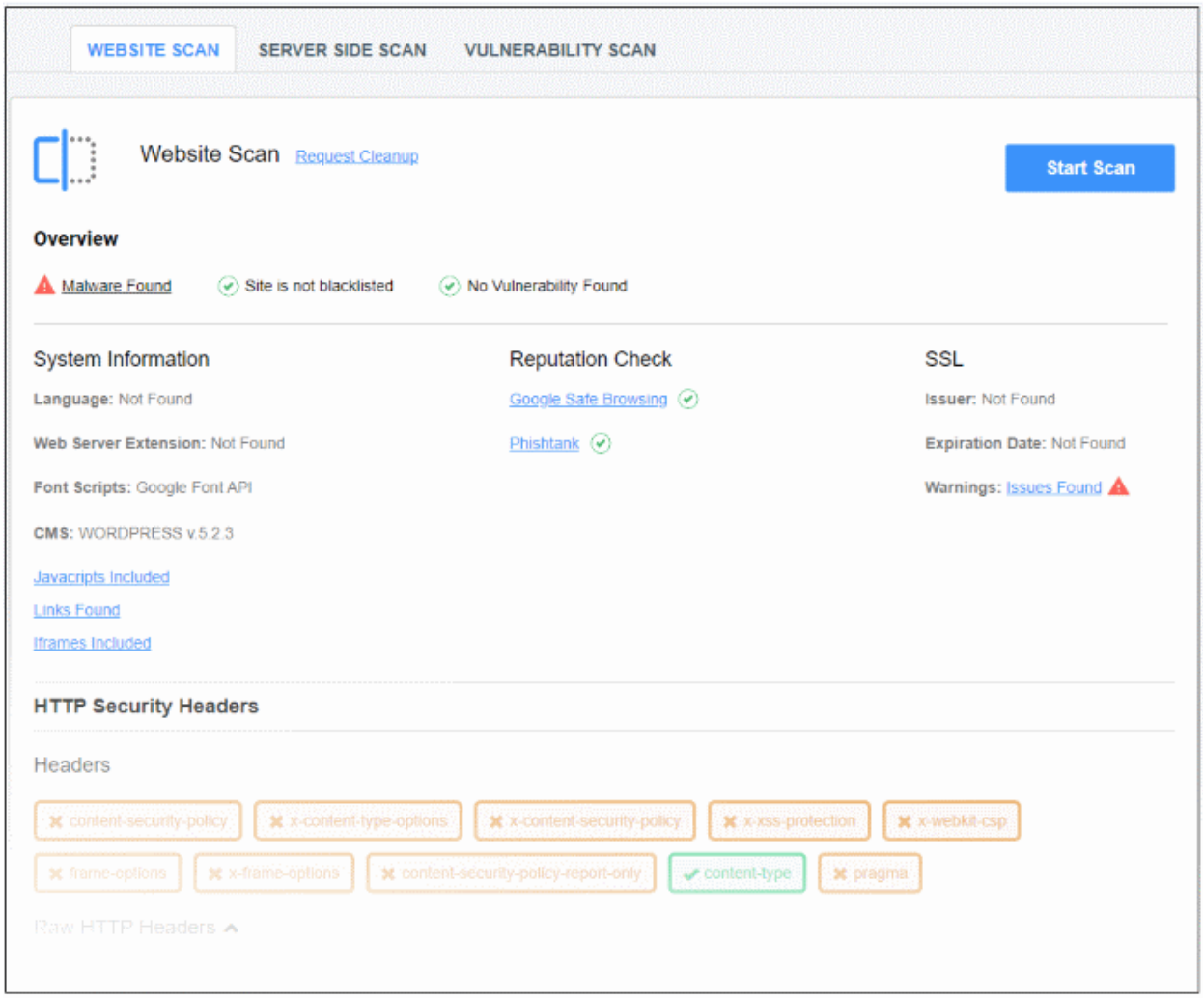
- Select a website at top-left then choose 'Scan'
- Open the Website Scan' tab
- Click 'Start Scan':



- The scan is added to tasks and may take a few minutes to complete:



- All vulnerabilities are shown at the end of the scan. The results show missing headers, SSL errors and blacklists on which your site appears:



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

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

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

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

System Information

- **Language** – The programming language used in the site. For example, PHP, Python and so on.
- **Web Server Extension** – Optional module used in the website. For example, OpenSSL, mod_ssl, Google PageSpeed and so on.
- **Font Scripts** – Shows fonts used on your web pages.

- **CMS** – The content management system (CMS) tool used on the site.
- **JavaScripts Included** – Click the link to view details of JavaScripts used on site pages.
- **Links Found** - Click the link to view internal and external hyperlinks used on site pages.
- **Iframes Included** - Click the link to view internal and external inline frames (iframes) used in site pages. Iframes can be vulnerable to attack.

Reputation Check

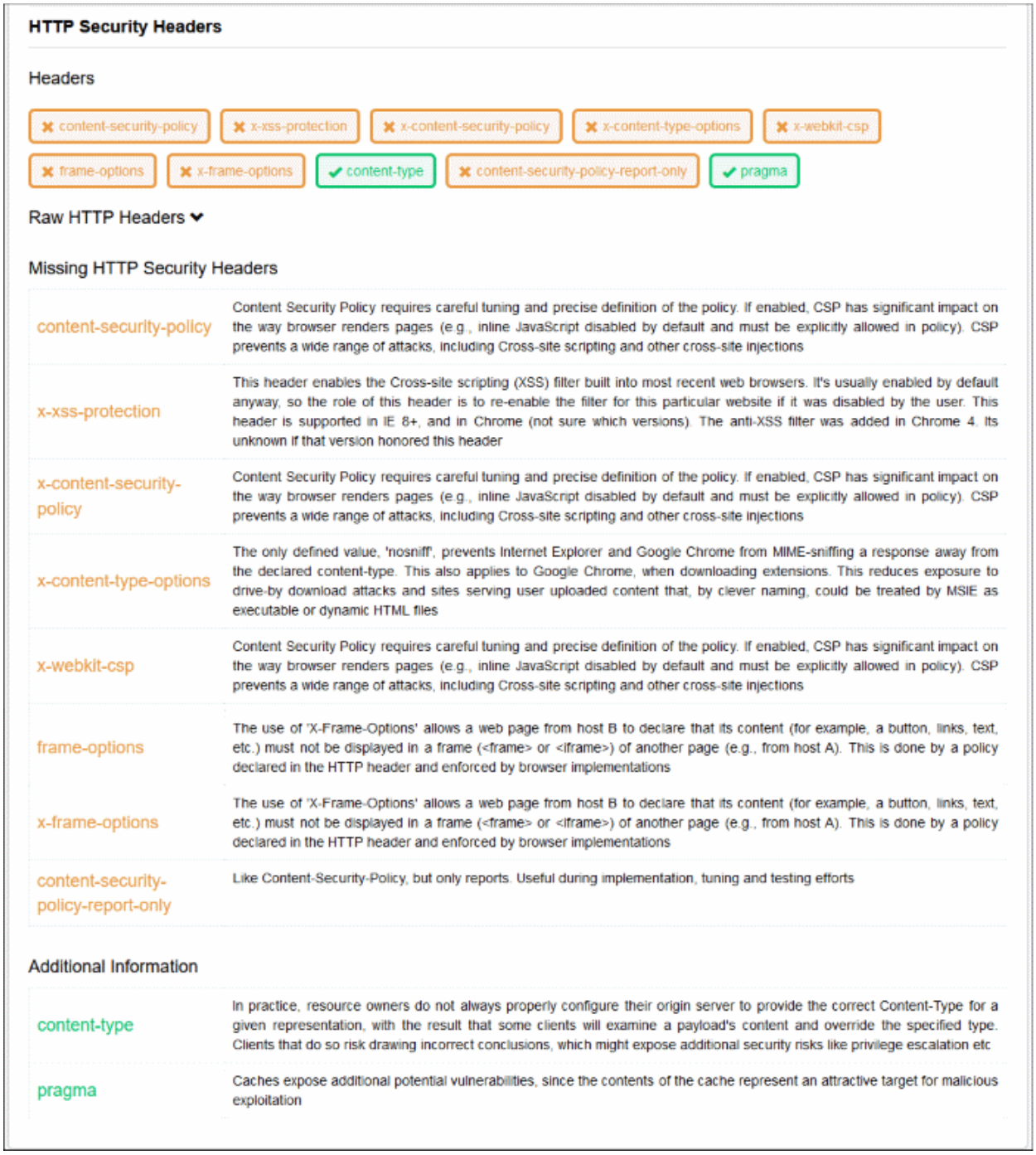
- **Google Safe Browsing** – Opens **https://transparencyreport.google.com/safe-browsing/**. Use this site to check whether any of your sites have been flagged as harmful.
- **Phishtank** – Opens the PhishTank website at **https://www.phishtank.com/**. Use this site to run to see if any of your sites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

SSL

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

HTTP Security Headers

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


HTTP Security Headers
Headers
content-security-policy
x-xss-protection
x-content-security-policy
x-content-type-options
x-webkit-csp
frame-options
x-frame-options
content-type
content-security-policy-report-only
pragma
Raw HTTP Headers
Missing HTTP Security Headers
content-security-policy
Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
x-xss-protection
This header enables the Cross-site scripting (XSS) filter built into most recent web browsers. It's usually enabled by default anyway, so the role of this header is to re-enable the filter for this particular website if it was disabled by the user. This header is supported in IE 8+, and in Chrome (not sure which versions). The anti-XSS filter was added in Chrome 4. Its unknown if that version honored this header
x-content-security-policy
Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
x-content-type-options
The only defined value, 'nosniff', prevents Internet Explorer and Google Chrome from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions. This reduces exposure to drive-by download attacks and sites serving user uploaded content that, by clever naming, could be treated by MSIE as executable or dynamic HTML files
x-webkit-csp
Content Security Policy requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browser renders pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections
frame-options
The use of 'X-Frame-Options' allows a web page from host B to declare that its content (for example, a button, links, text, etc.) must not be displayed in a frame (<frame> or <iframe>) of another page (e.g., from host A). This is done by a policy declared in the HTTP header and enforced by browser implementations
x-frame-options
The use of 'X-Frame-Options' allows a web page from host B to declare that its content (for example, a button, links, text, etc.) must not be displayed in a frame (<frame> or <iframe>) of another page (e.g., from host A). This is done by a policy declared in the HTTP header and enforced by browser implementations
content-security-policy-report-only
Like Content-Security-Policy, but only reports. Useful during implementation, tuning and testing efforts
Additional Information
content-type
In practice, resource owners do not always properly configure their origin server to provide the correct Content-Type for a given representation, with the result that some clients will examine a payload's content and override the specified type. Clients that do so risk drawing incorrect conclusions, which might expose additional security risks like privilege escalation etc
pragma
Caches expose additional potential vulnerabilities, since the contents of the cache represent an attractive target for malicious exploitation

4.2.2 Website Files Security Scans

- **License notes**
- **Upload the scanner agent**
- **Open the 'Server Side Scan' interface**
- **Configure Malware Scan Settings**
  - **Automatic configuration**
  - **Manual Configuration**
- **Run a Malware Scan and View Results**
- **Configure Notifications, Automatic Malware Removal and Schedule Website Scan**

License notes

Malware removal:

- Automatic malware removal is enabled by default for 'Pro' and 'Premium' licenses. You can manage auto-removal in the **malware settings** page.
- Malware removal is not included with basic licenses. You will be prompted to upgrade your license if you enable removal in **malware settings**.

Scan frequency:

The number of scans you can run depends on your license type:

- Basic – One scan per day
- Pro – Two scans per day
- Premium - Four scans per day

Scheduled and manual scans both count towards your scans per day. For example, if you have a premium license and schedule 4 scans, but run two manual scans, then only two scheduled scans will run that day.

Upload the scanner agent

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

There are two ways to do this:

1. **Automatically** - Use the cWatch interface to upload the agent to your site.
   - Click 'Scan' > 'Server Side Scan' > 'Overview'
   - Click 'Enable Scanner'
   - Choose 'Automatic' in the 'Enable Server Side Scanner' tile
   - Enter your web-server FTP details.
   - Click 'Test Connection'
   - Click 'Save' after the connection is established
   - You will see the message – 'Server side scanner is enabled'
     - See **Automatic configuration** for more information.
2. **Manually** - Download the agent and copy it to your site. The agent is a .php file.
   - Click 'Scan' > 'Server Side Scan' > 'Overview'
   - Click 'Enable Scanner'
   - Choose 'Manual' in the 'Enable Server Side Scanner' tile.
   - Click the purple 'PHP' icon to download the file
   - Upload the file to a publicly accessible location on your site
   - Enter the URL of the file in the space provided

- Click 'Test and Save'. The scanner will be enabled if the test is successful.
  - See **Manual Configuration** for guidance on this.

Once done, cWatch will run scheduled scans on all files hosted on the website.

Open the 'Server Side Scan' interface

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

From the server side scan section you can:

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

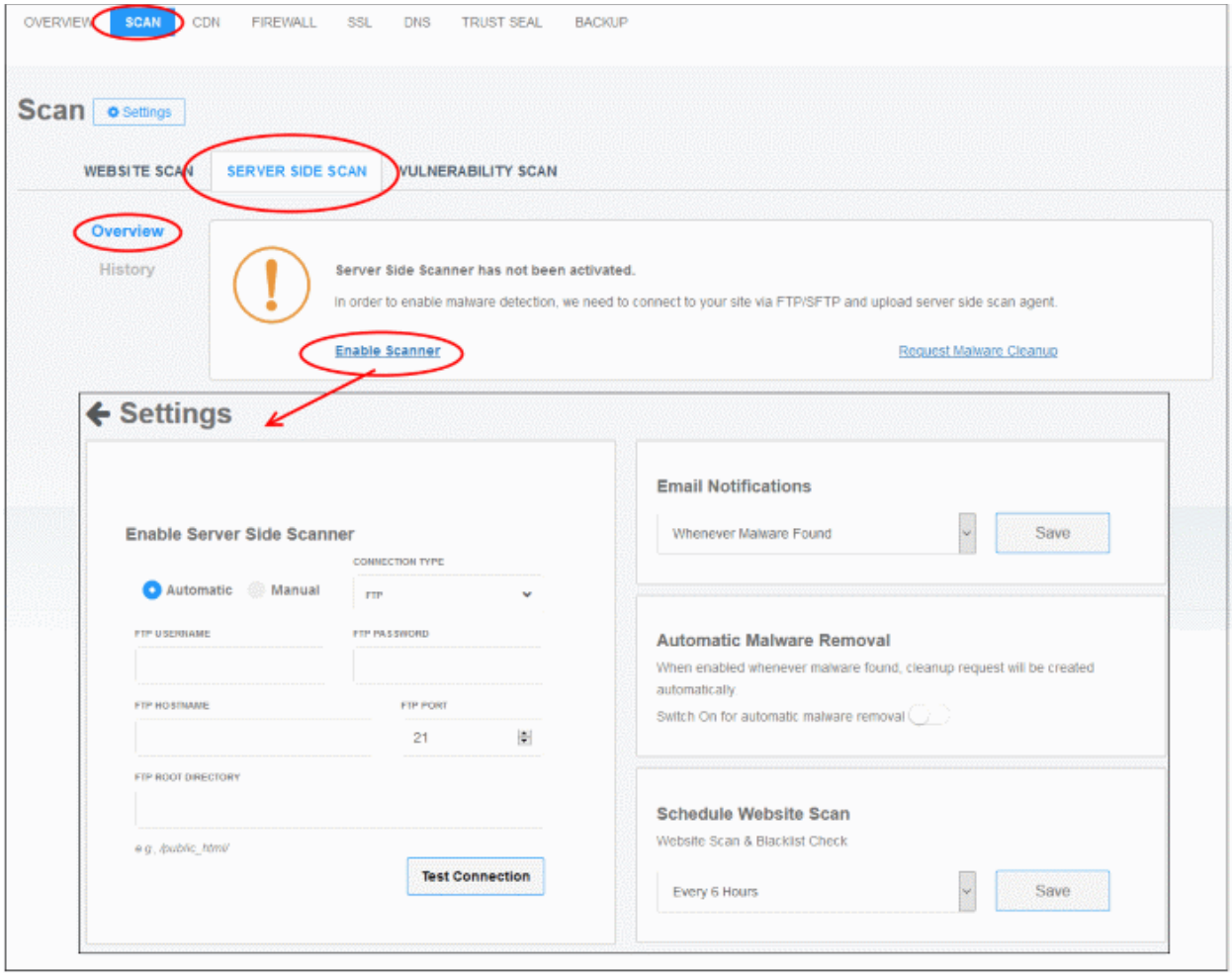
See the following section for more help on malware scans:

- **Configure Malware Scan Settings**
  - **Automatic configuration**
  - **Manual Configuration**
- **Run Malware Scans and View Results**
- **Configure Notification and Automatic Malware Removal**

4.2.2.1 Configure Malware Scan Settings

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

- Select the target site from the menu at top-left of the dashboard
- Click the 'Scan' tab then 'Server Side Scan' > 'Overview'
- Click 'Enable Scanner':



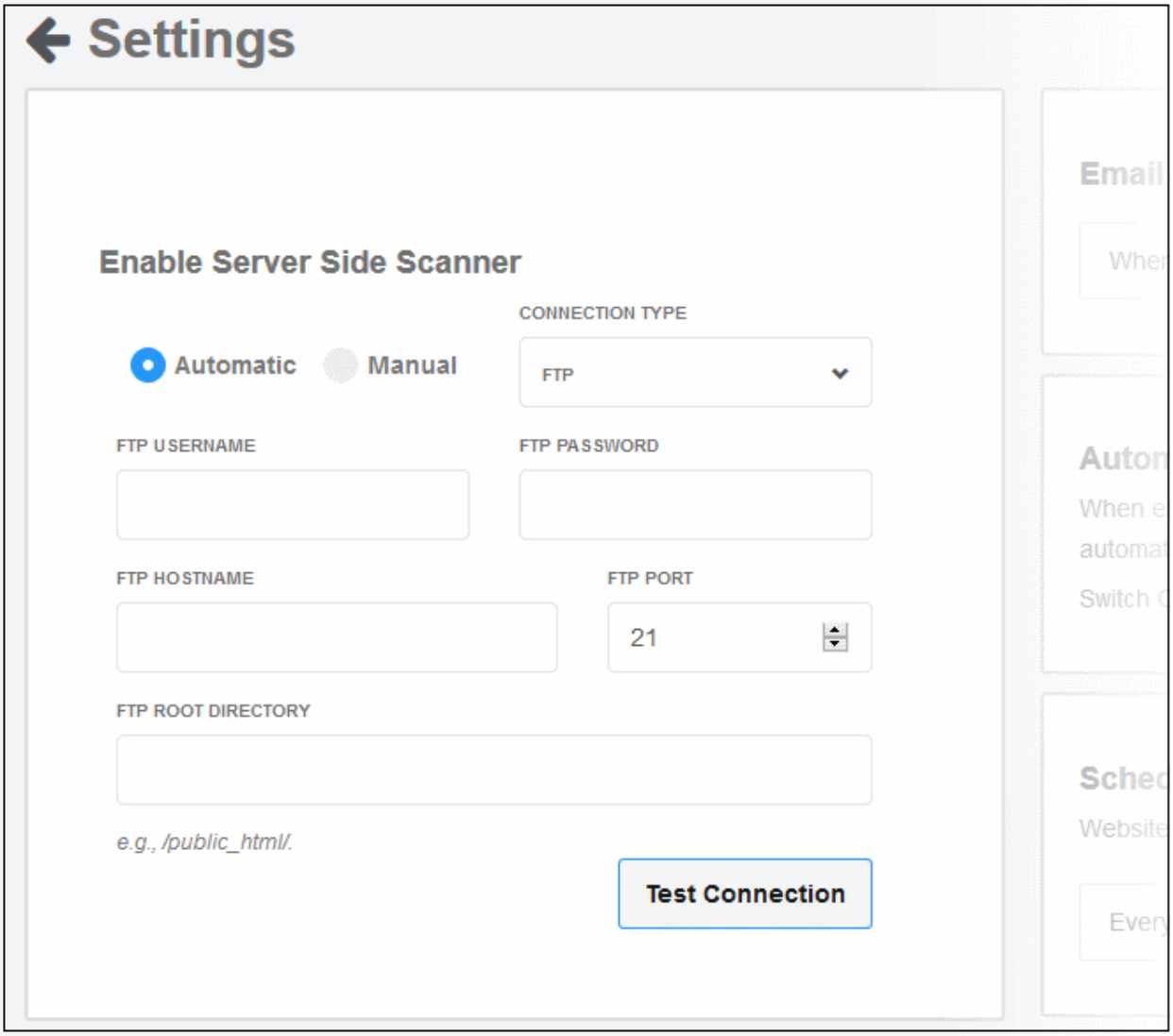
See the following sections for help with:

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

4.2.2.1.1 Automatic Configuration

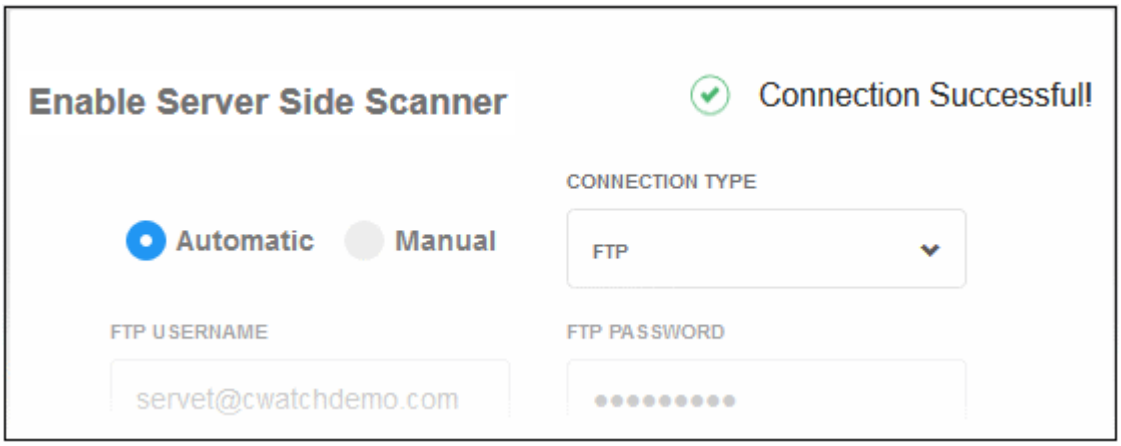
You need to provide FTP details for your site to enable automatic configuration. cWatch will use the details to upload the scanner agent.

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Server Side Scan' > 'Overview'
- Click 'Enable Scanner'
- Select ‘Automatic’ in the server side scanner box:



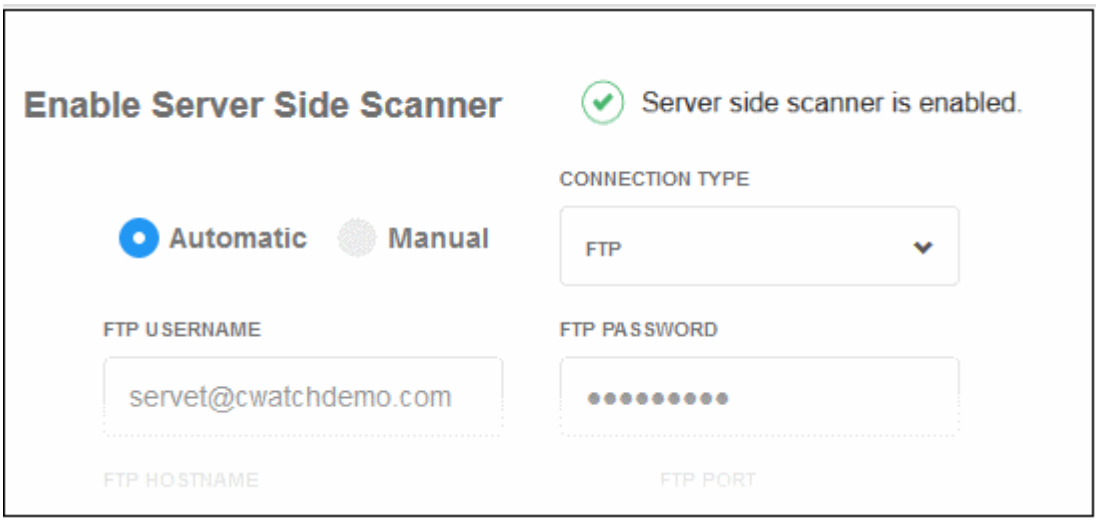
FTP / s/FTP Settings - Table of Parameters	
Parameter	**Description**
Connection Type	Choose FTP or sFTP (secure FTP) as required.
FTP Username / FTP Password	Enter the username and password of your FTP server
Hostname	IP or hostname of your web-server
Port	By default, FTP / sFTP connections use ports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

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



- Click 'Save'

cWatch will upload the agent to your site. You will see 'Server side scanner is enabled' message if everything is successful:

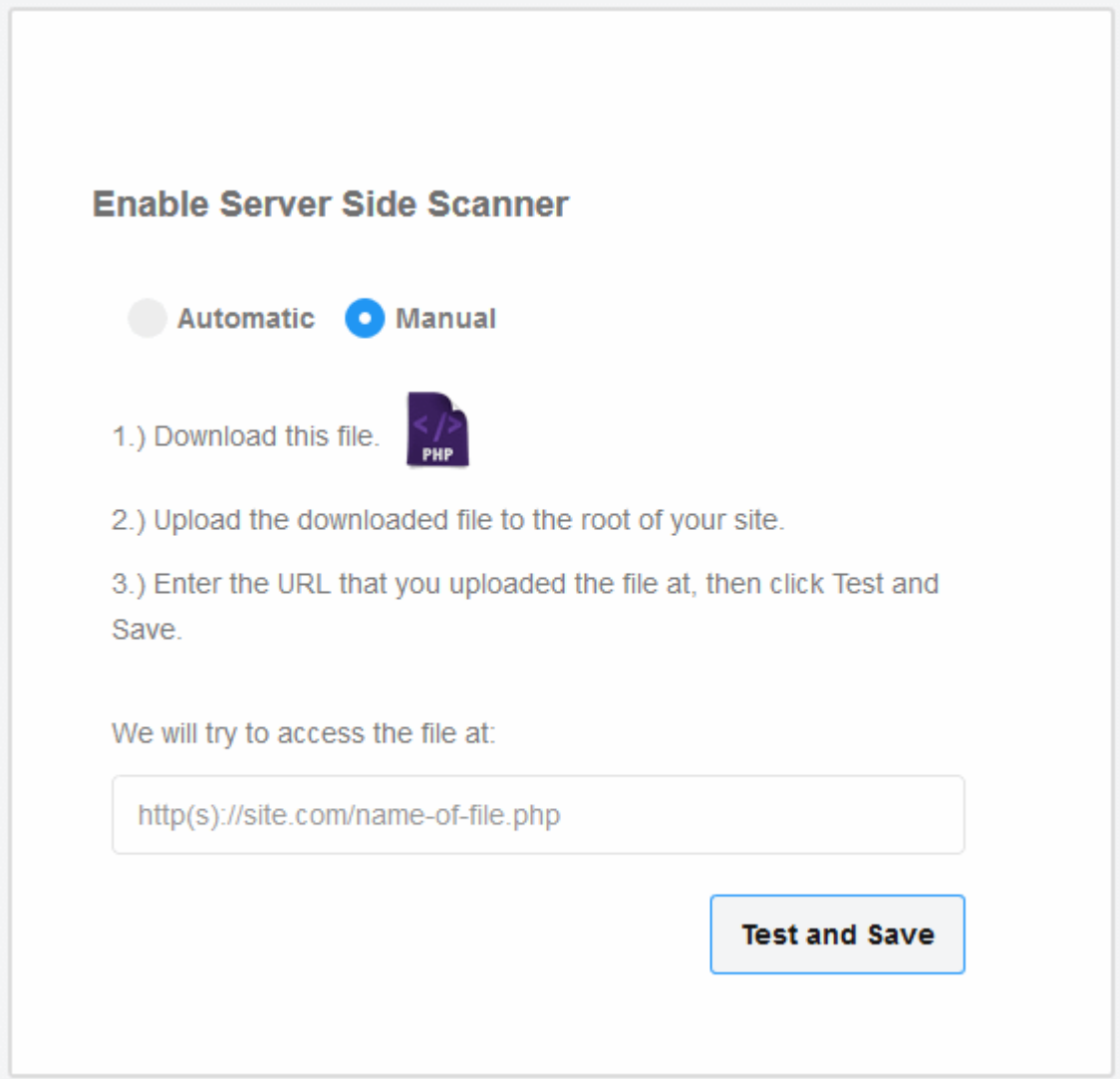


- Note. Our technicians will also use these FTP settings to access your site IF you request them to remove malware

4.2.2.1.2 Manual Configuration

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

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Server Side Scan' > 'Overview'
- Click 'Enable Scanner'
- Select ‘Manual’ in the server side scanner box:

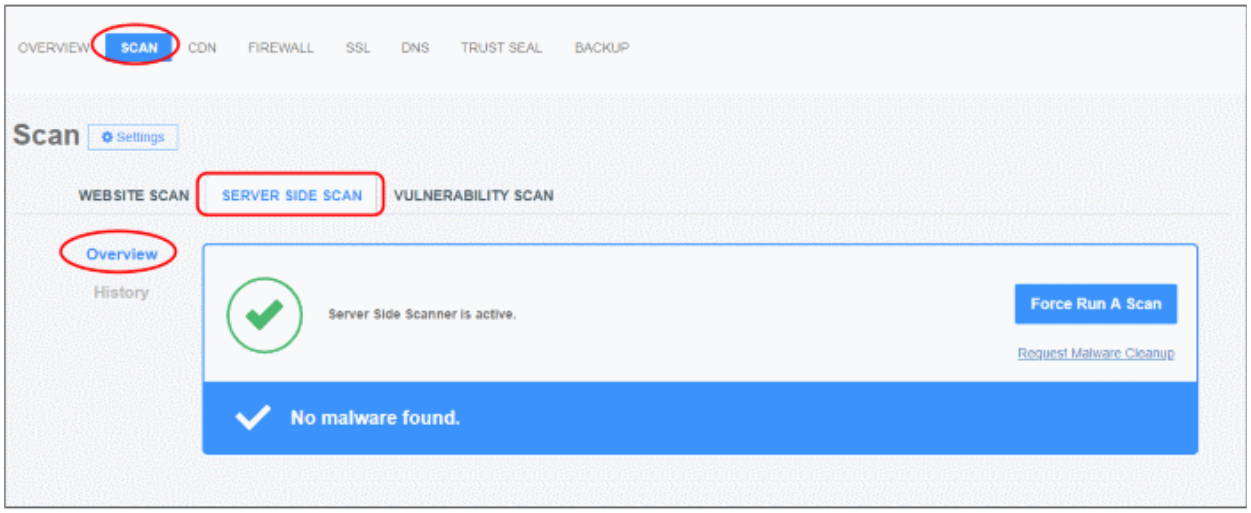


- Download the PHP file in step 1
- Upload the file to the root folder of your website. The file should be publicly accessible.
- Enter the URL of the uploaded file in the text field.
- Click 'Test and Save' to run the check.
- Malware scans on the web files in your server will begin if the check is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

4.2.2.2 Run a Malware Scan and View Results

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

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



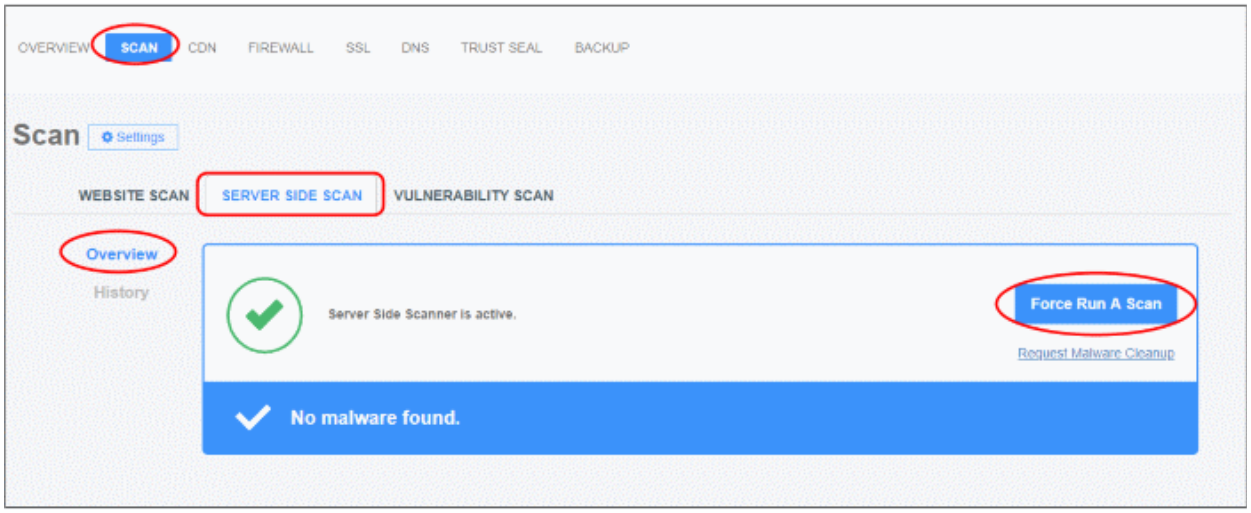
- The overview page shows details about any malware found on the site. Click the history link to view current and previous scan results.

From this interface you can:

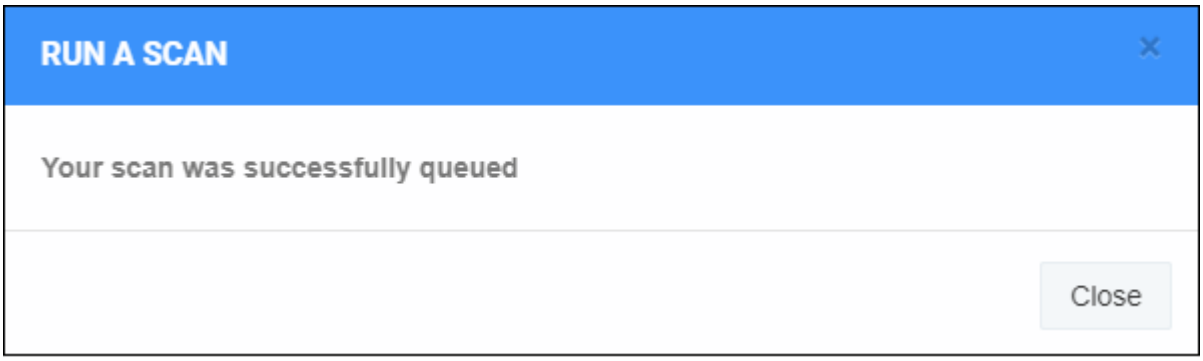
- **Start a manual scan**
- **Submit a malware cleanup request**
- **Start a scan and request a cleanup in a single step**
- **View malware scan results**

Start a manual scan

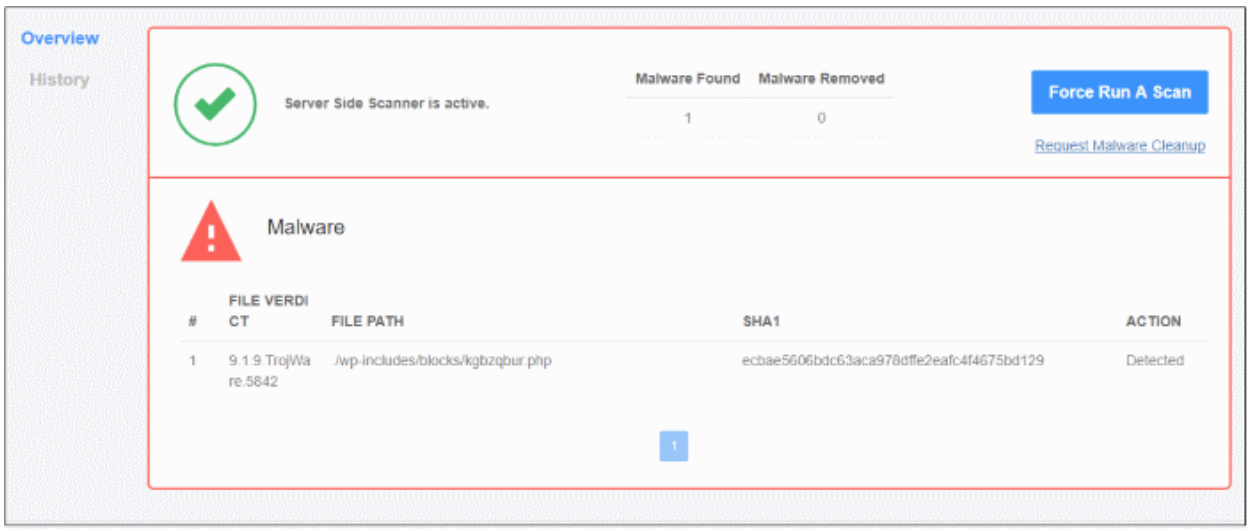
- Open the cWatch dashboard
- Select a website from the menu at top-left
- Click the 'Scan' tab then 'Server Side Scan' > 'Overview'
- Click the 'Force Run a Scan' button:



The request is created and the following message shown:



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



- The upper pane shows the number of malware found and removed.

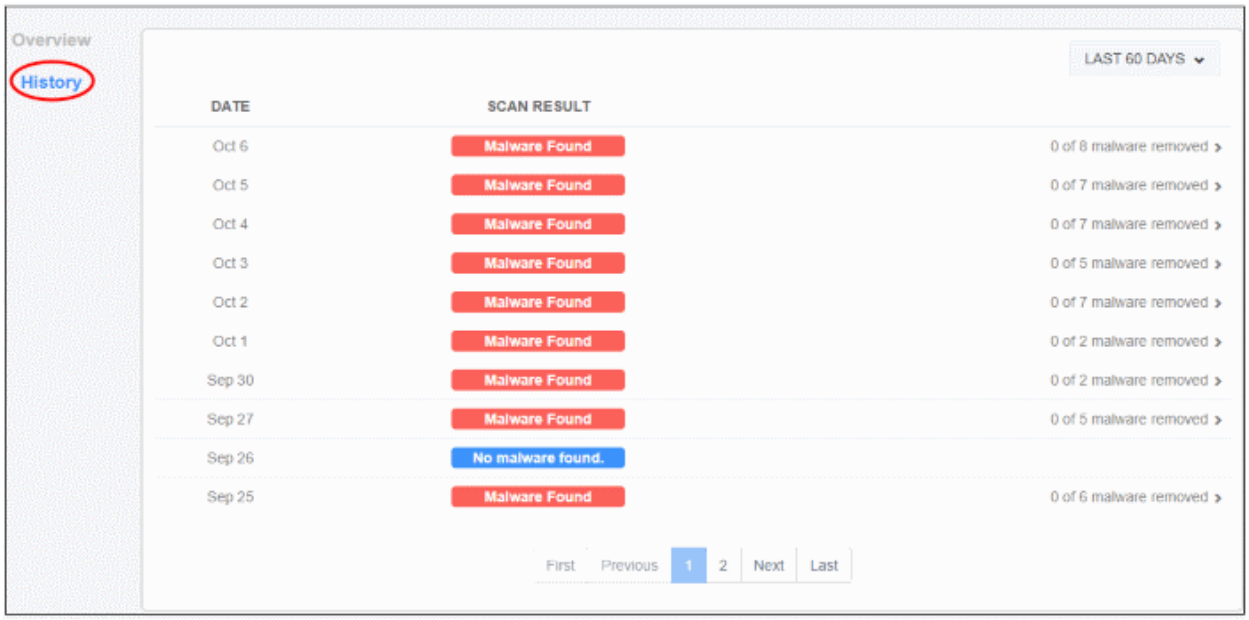
File Verdict – Name of the malicious item

File Path – Location of the item on your webserver

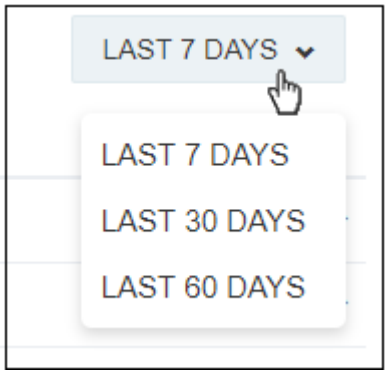
SHA1 – File hash of the malicious item. Hash values are used by Comodo, and every other antivirus company, to identify malicious files.

Action – The current status of the malware.

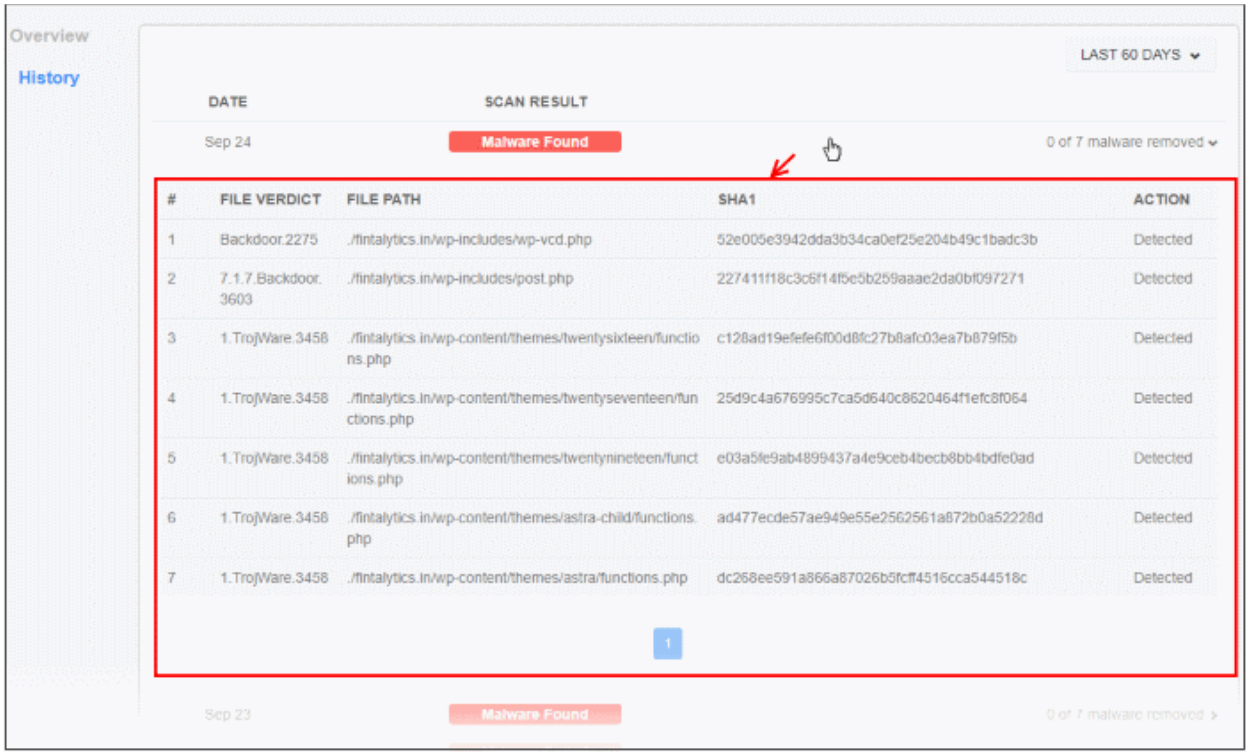
- Click the history link to view the results of past malware scans:



- Select the result period at top-right:



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

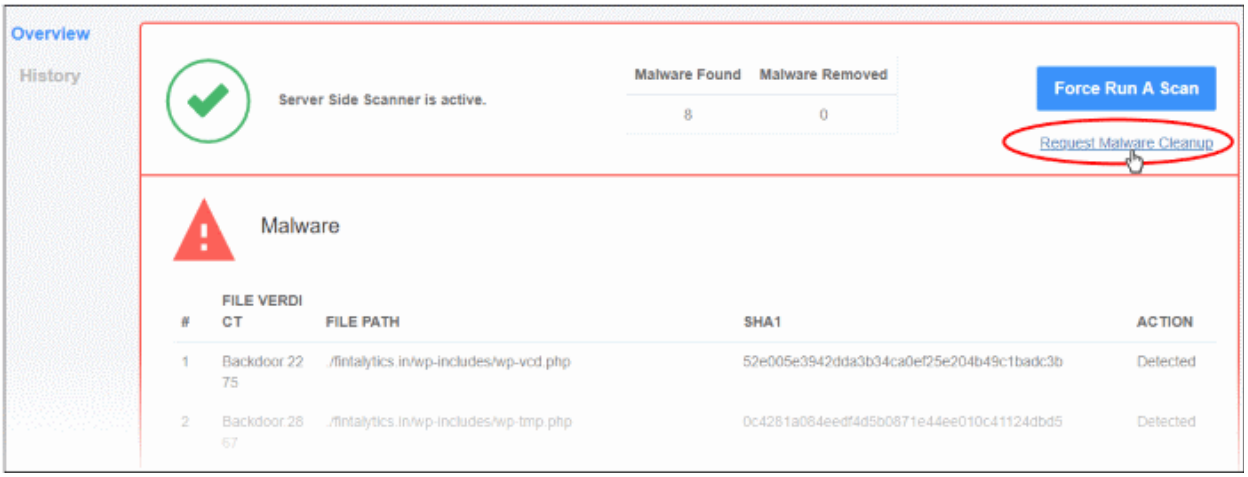


- Click the row again to collapse the details.
- Request Malware Cleanup - Instruct Comodo technicians to remove the malware. See the next section for more on this.

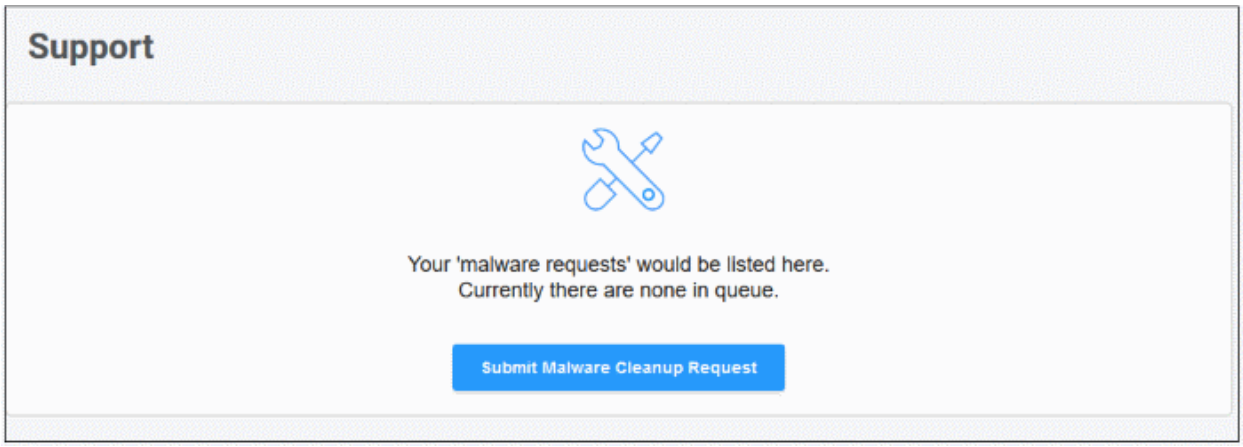
Submit a malware cleanup request

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

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



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

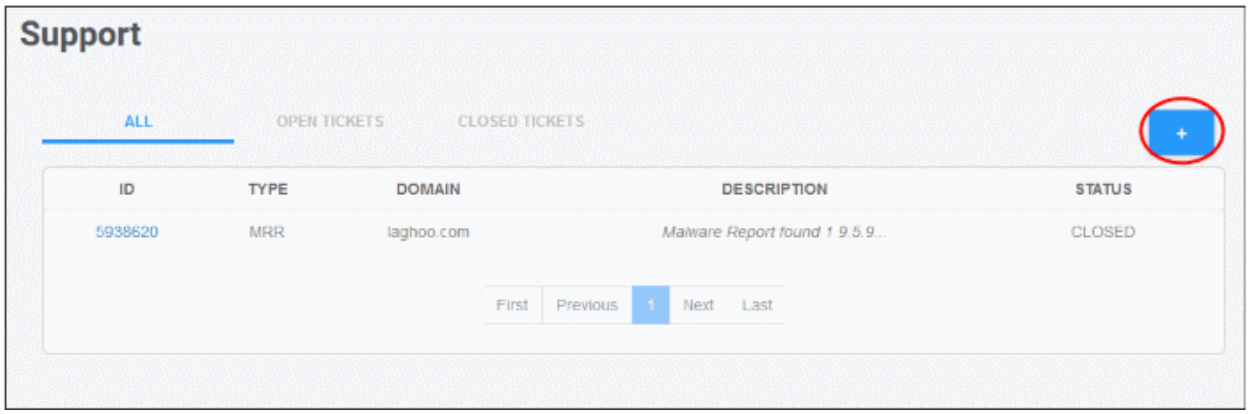


The screen above is shown if you have not yet submitted any requests.

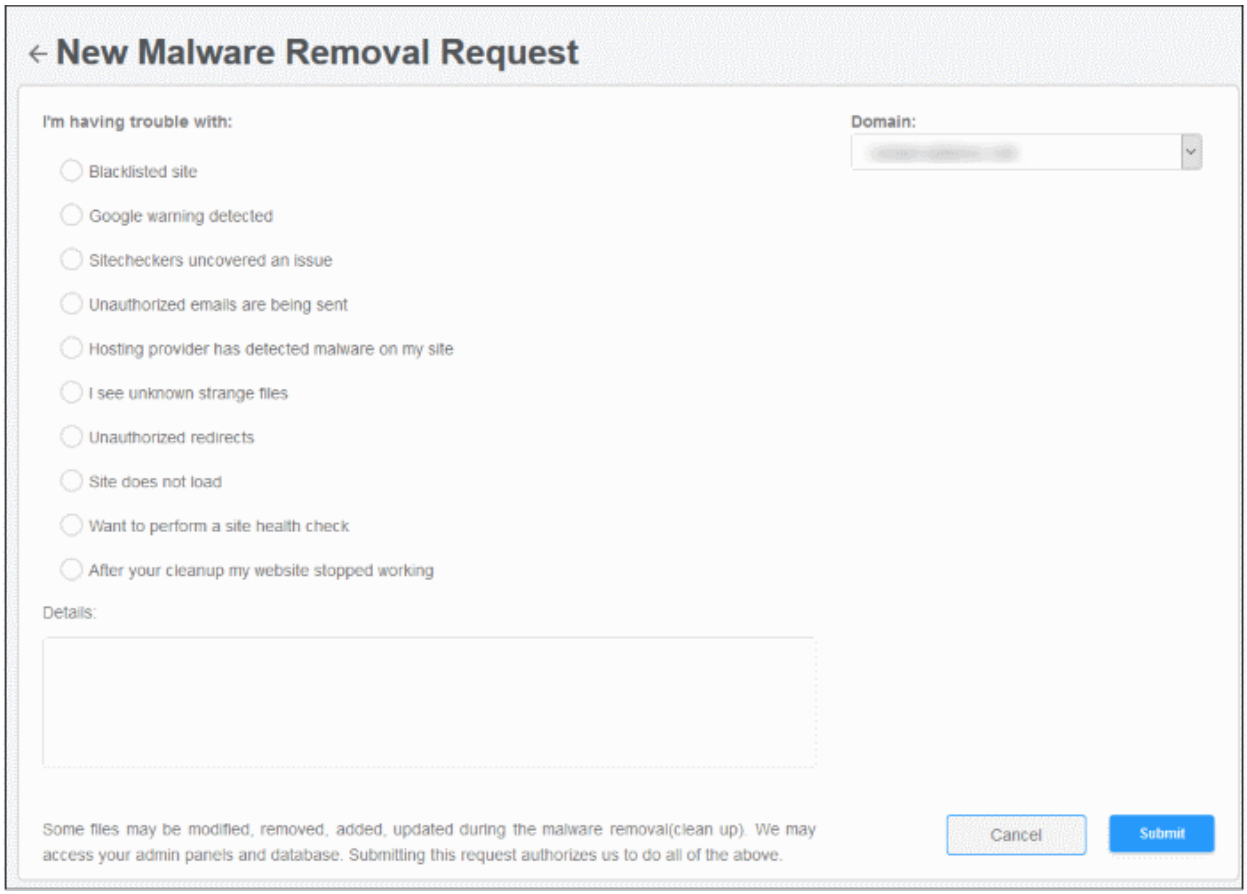
- Click 'Submit Malware Cleanup Request'

  OR

- Click the '+' button:



This opens the removal request form:



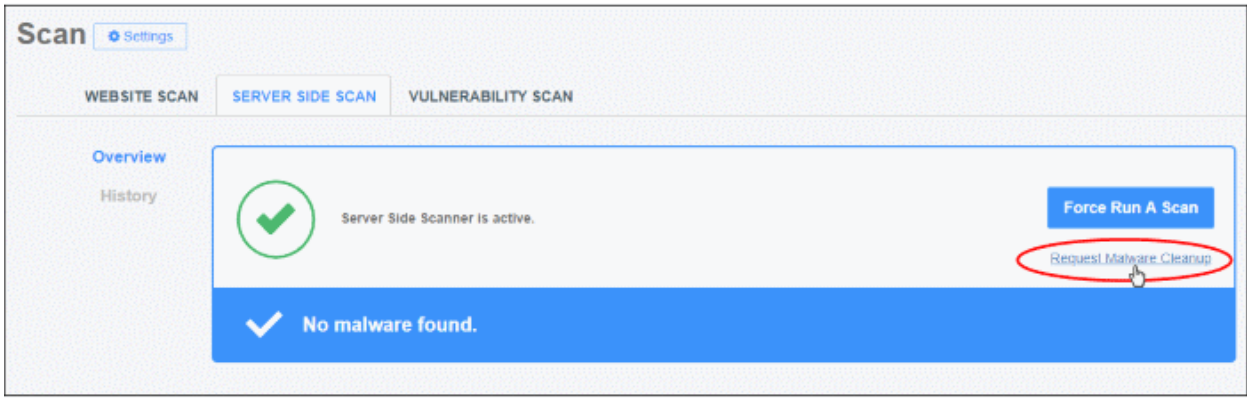
- Select all issues affecting your site (optional)
- Enter any further information you feel is important in the 'Details' box
- Click 'Submit'.
- A request ID is created. Our technicians will access your site to remove the malware and remediate the issues.
    - Click 'Request ID' if you want to message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

You will see the following when the cleanup is complete:

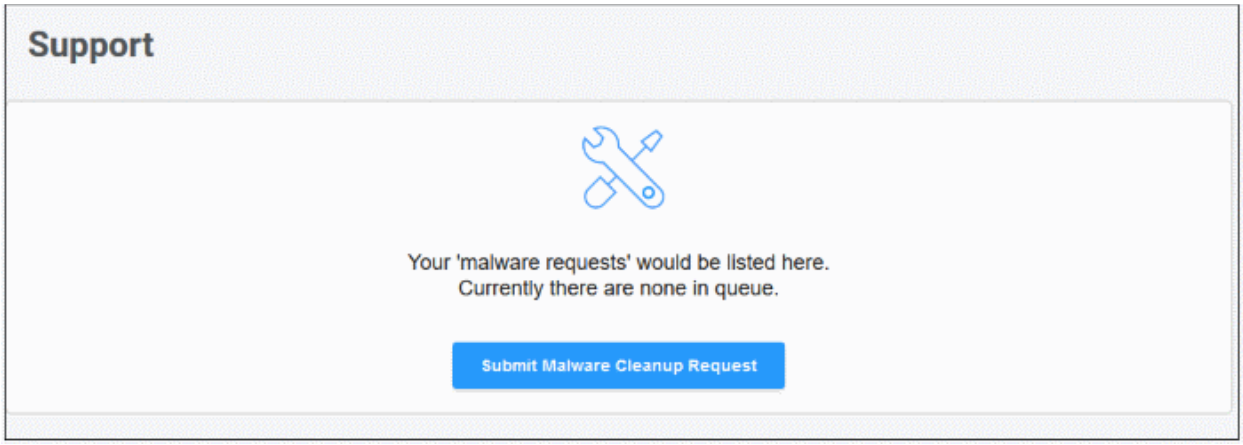
- **Download Cleanup Report** – The report itemizes each piece of malware removed.

Start a manual scan and request cleanup in one step

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



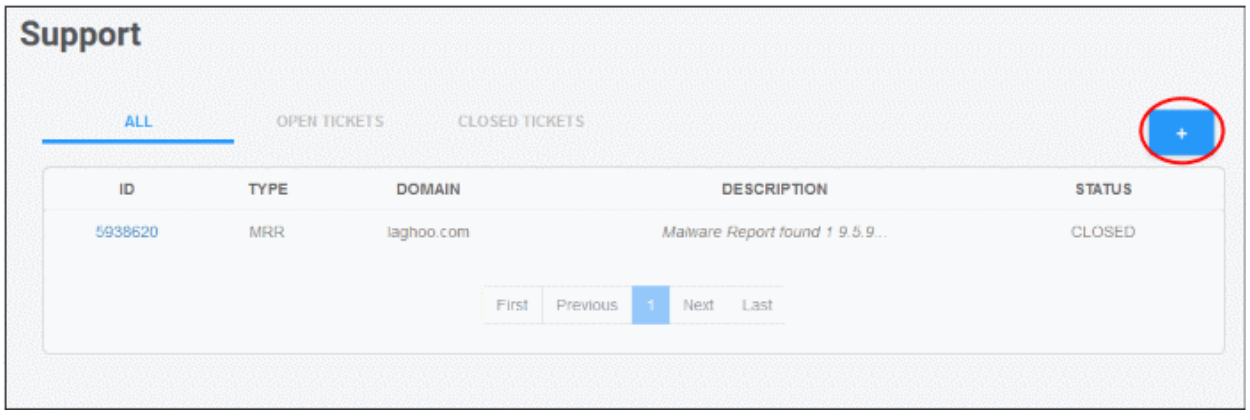
- Click 'Request Malware Cleanup'
- You will be taken to the support page to create a ticket:



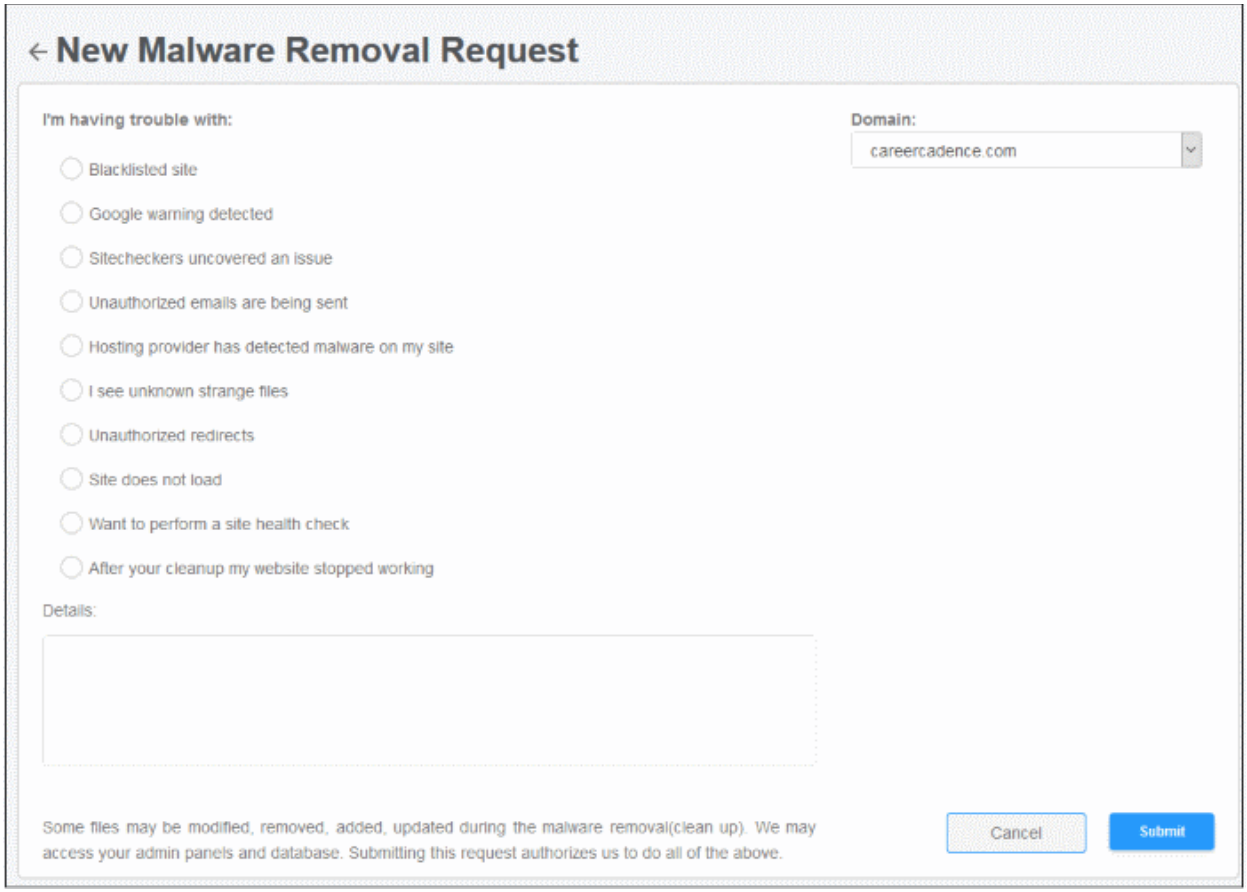
The screen above is shown if you have not yet submitted any requests.

- Click 'Submit Malware Cleanup Request'

  OR
- Click the '+' button:



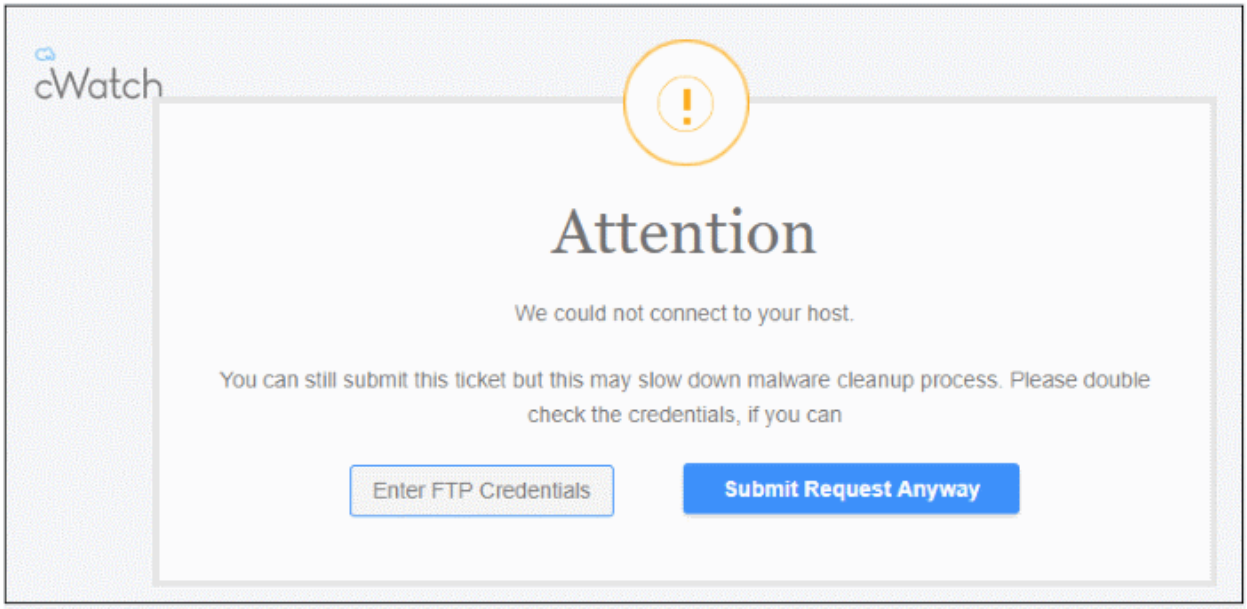
This opens the removal request form:



- Select all issues affecting your site
- Enter your message to the technician in the 'Details' text box
- If the website has already been enabled for malware scan, click 'Submit Request'.
    - The scan will start immediately.
    - A cleanup request is created if the scan finds malware.
    - Our technicians will access your site to remove malware and remediate any other issues you reported.
    - Click 'Request ID' if you want to send a message to the technician while the cleaning is in progress.
    - View the cleanup report after the completion of cleaning as described **above**.
- If malware scanning has not been enabled on the site then you need to upload the scanner agent to the site. Note - The following option only appears if malware scanning is not enabled, or if the FTP credentials have changed.

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

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



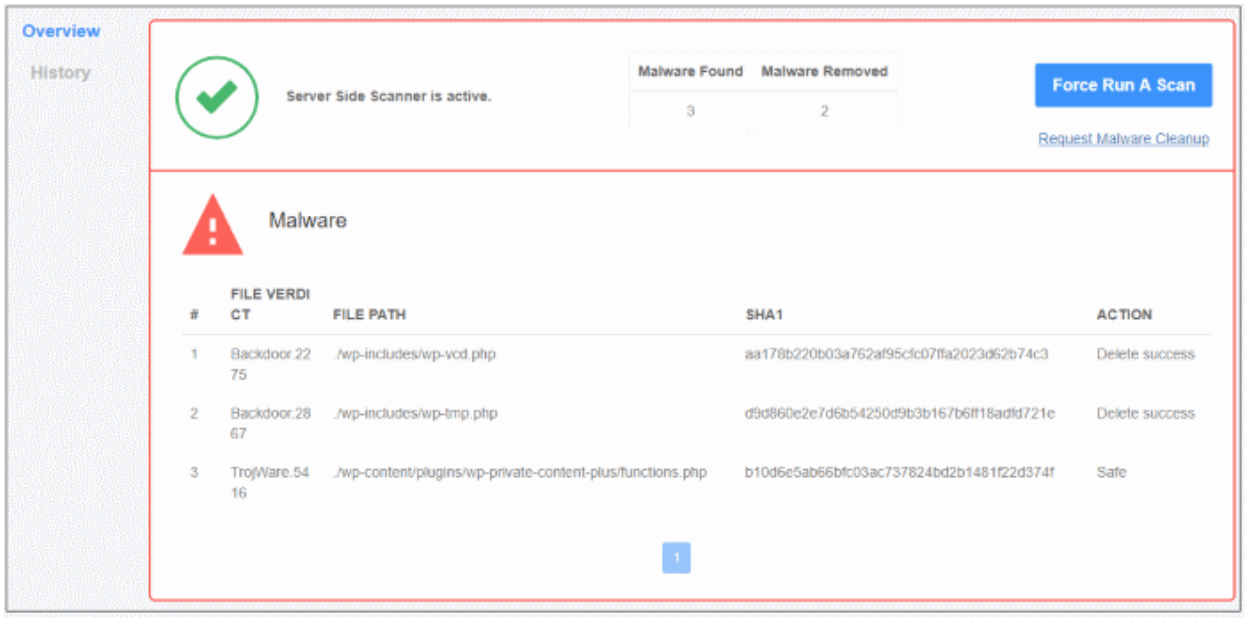
Comodo recommends you provide FTP details for quicker resolution of the request.

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

View malware scan results

The 'Server Side Scan' page shows the results of all scheduled and manual scans. You can also create a malware cleanup request for our technicians.

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



The upper pane shows malware found vy the latest scan which was removed by our technicians.

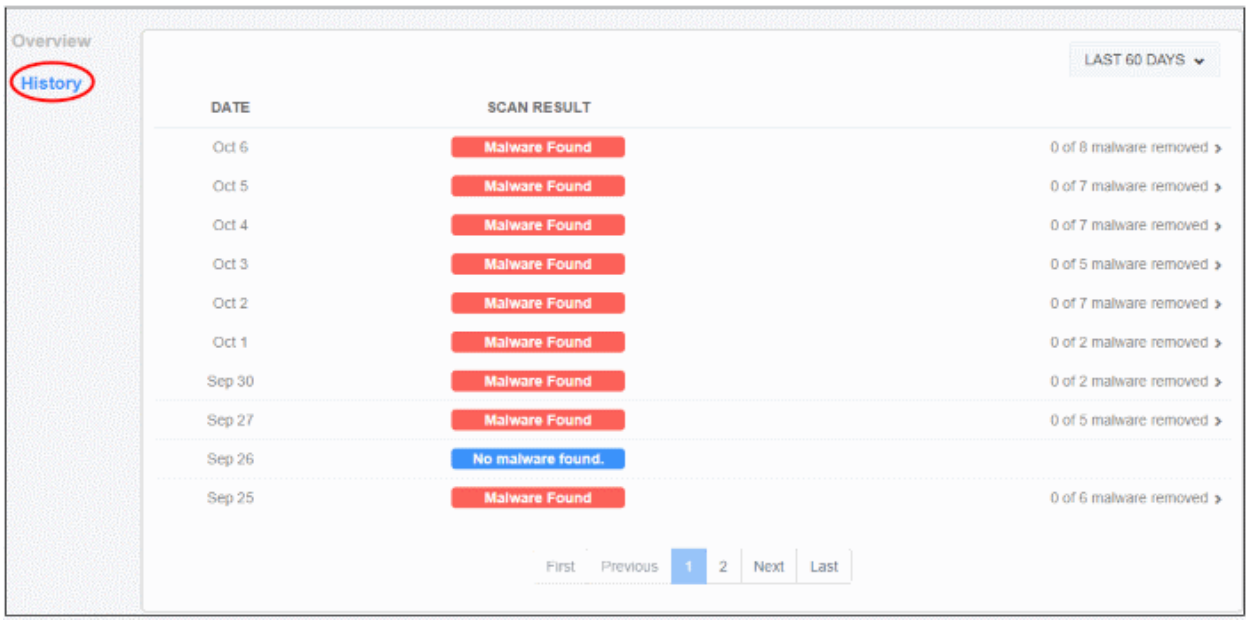
File Verdict – Name of the malicious item

File Path – Location of the item on your webserver

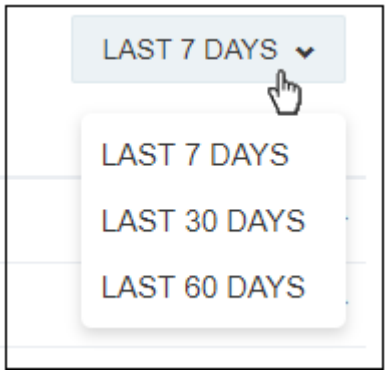
SHA1 – File hash of the malicious item. Hash values are used by Comodo, and every other antivirus company, to positively identify malicious files.

Action – The current status of the malware.

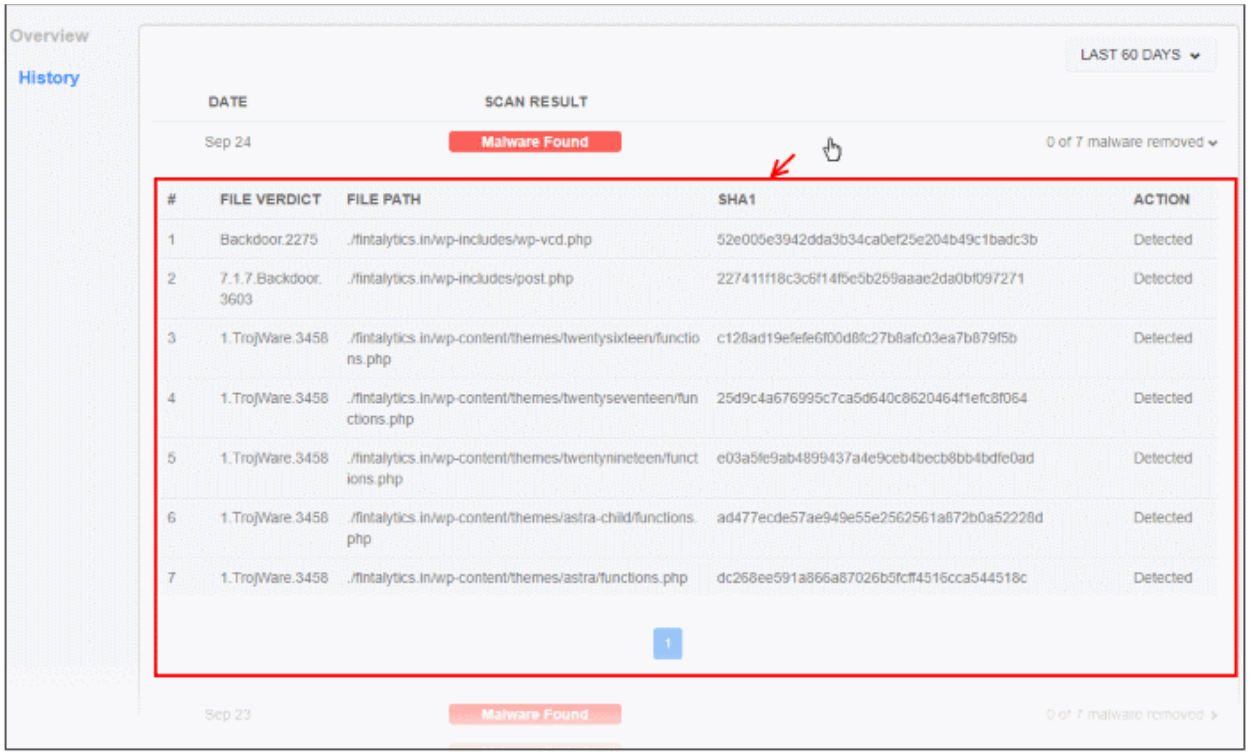
- Click the history link to view the results of past malware scans:



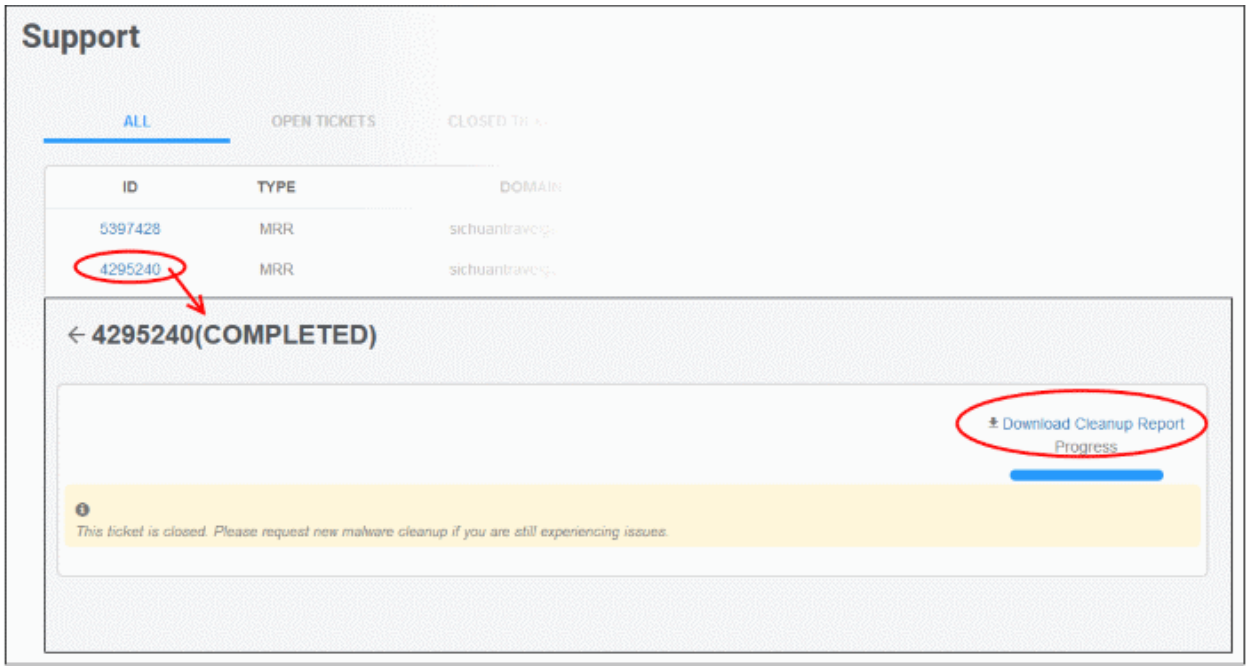
- Select the result period at top-right:



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



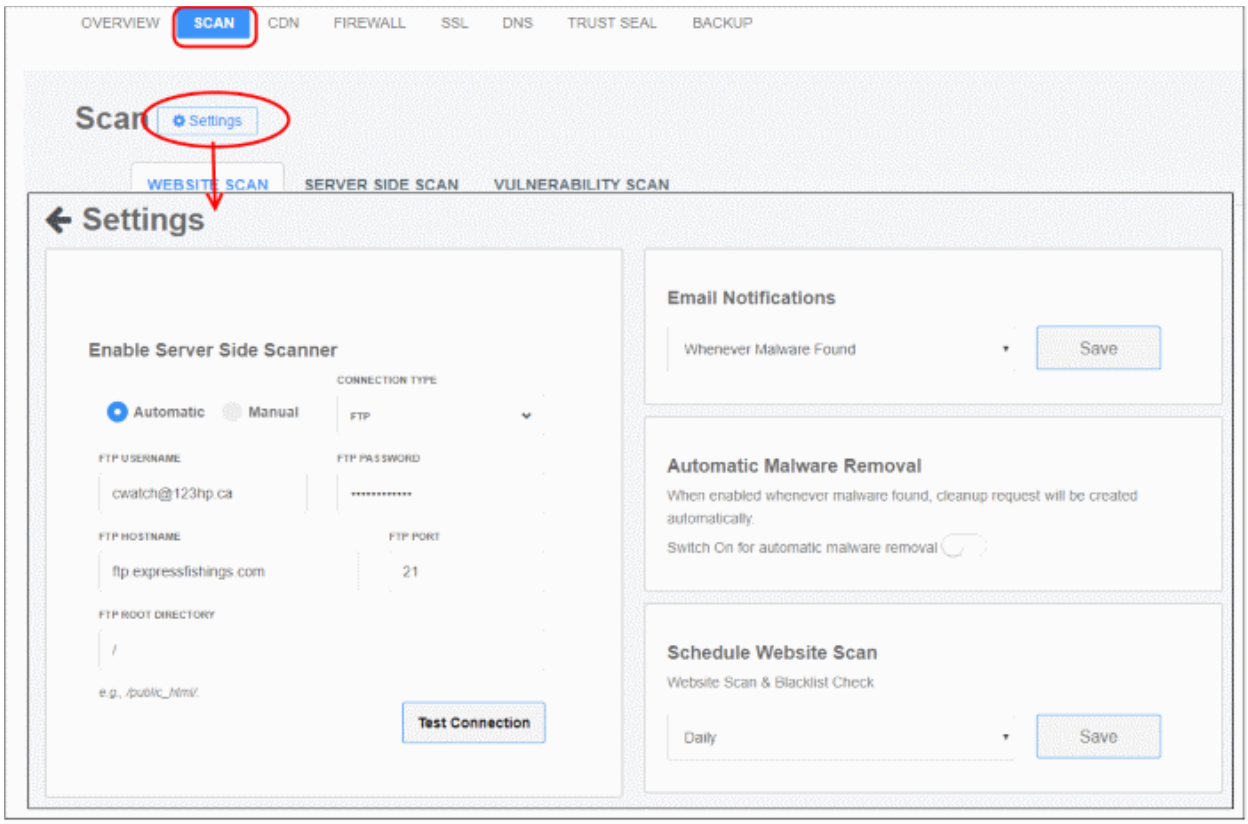
- Click the row again to collapse the details.
- Click 'Request Malware Cleanup' in the overview screen to instruct Comodo technicians to remove the malware.
- To download a cleanup report, go to support page then click the request ID:



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

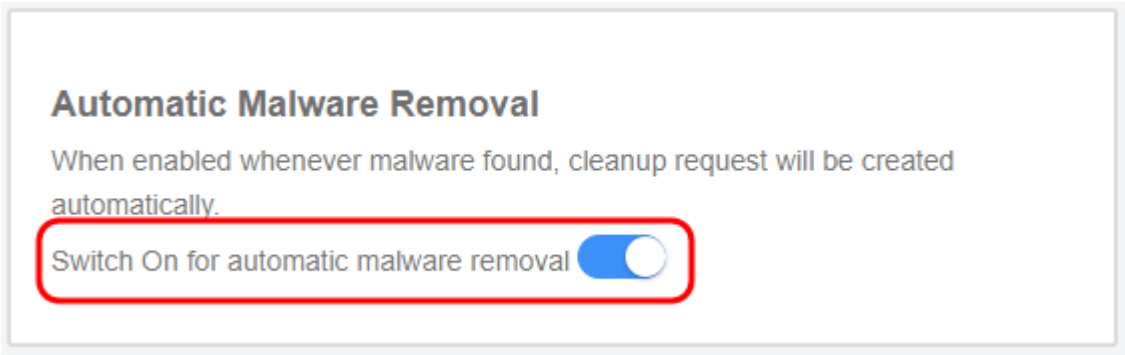
4.2.2.3 Configure Notifications, Automatic Malware Removal and Schedule Website Scan

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



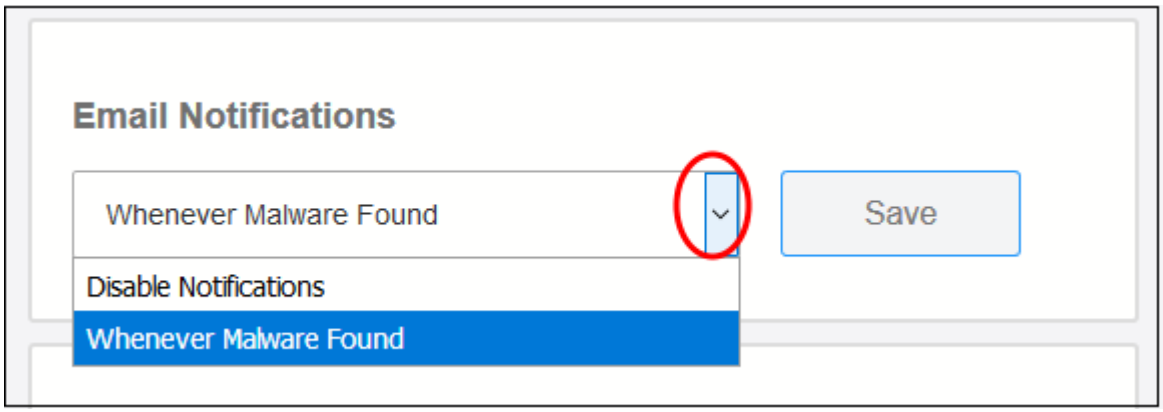
Automatic Malware Removal:

- You can configure cWatch to submit a malware removal request if threats are discovered on your site. You can enable this setting on a per-website basis.
- Auto-removal is enabled by default for 'Pro' and 'Premium' licenses. The scan and cleanup automatically take place according to your schedule..
- Use the switch highlighted below to enable/disable the feature:



Email Notifications

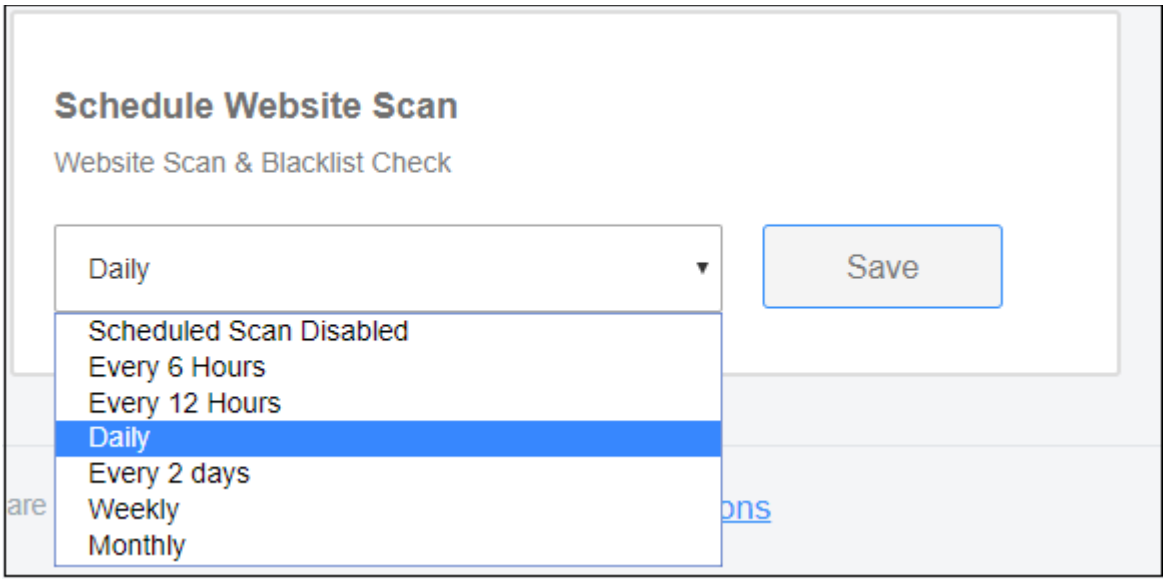
Email notifications are enabled by default for all license types. The notifications are sent to the registered email address for the account.



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

Schedule Website Scan

Choose how often you want the scans to run:



- Click 'Save' to apply your changes

4.2.3 Vulnerability Scans

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

You can run two types of vulnerability scan:

1. CMS Vulnerabilities

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

2. OWASP Top Ten Threats

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

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

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

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

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

4.2.3.1 CMS Vulnerability Scans

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

The content management system (CMS) scanner inspects your core site, plugins and themes to identify vulnerabilities in your current version.

The scanner supports the following types of CMS:

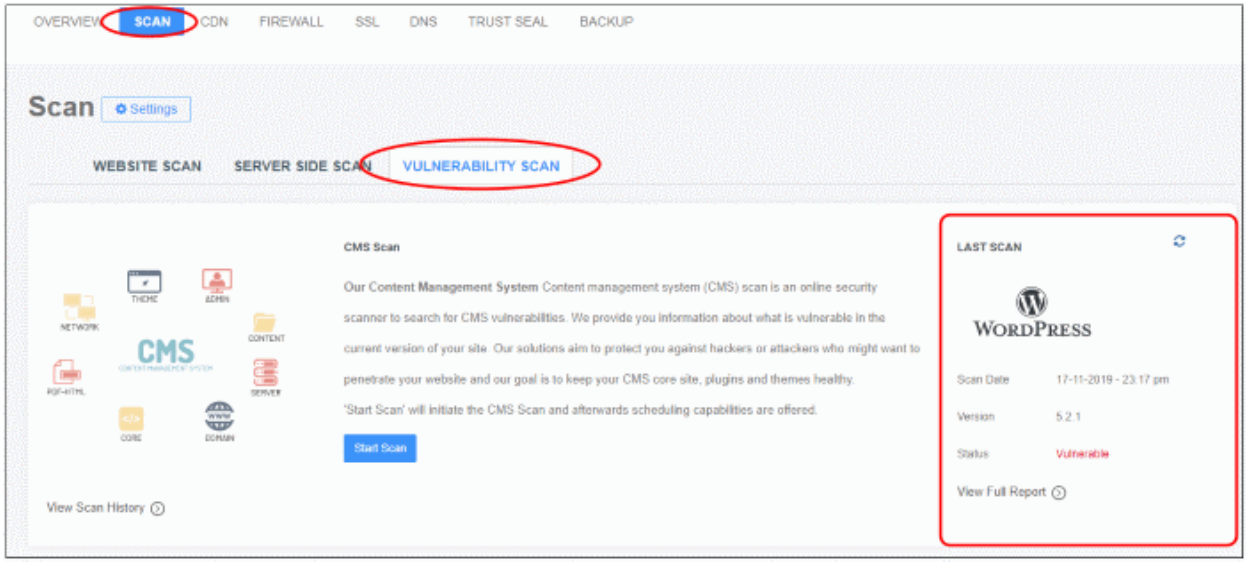
- WordPress
- Joomla
- Drupal
- ModX
- Typo3

See the following for more help:

- **The scan interface**
- **Run an on-demand scan**
- **View detailed results of the last scan**
- **View the results of previous scans**

The scan interface

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



The last scan area on the right shows the results of the most recent scan.

- **Scan Date** - When the most recent discovery was run.
- **Version** - The version number of the CMS that was scanned. This is the CMS version that your site runs on.
- **Status** - Whether the website has vulnerabilities or not.
  - **Not Vulnerable** - No weaknesses detected.
  - **Vulnerable** - Security threats found. Click on the row to view more details and fix advice.
  - **Failed** - Scan did not run for some reason.

- CMS format not identified - Shown if the site doesn't use a supported CMS, or because cWatch couldn't detect the CMS type for other reasons.

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

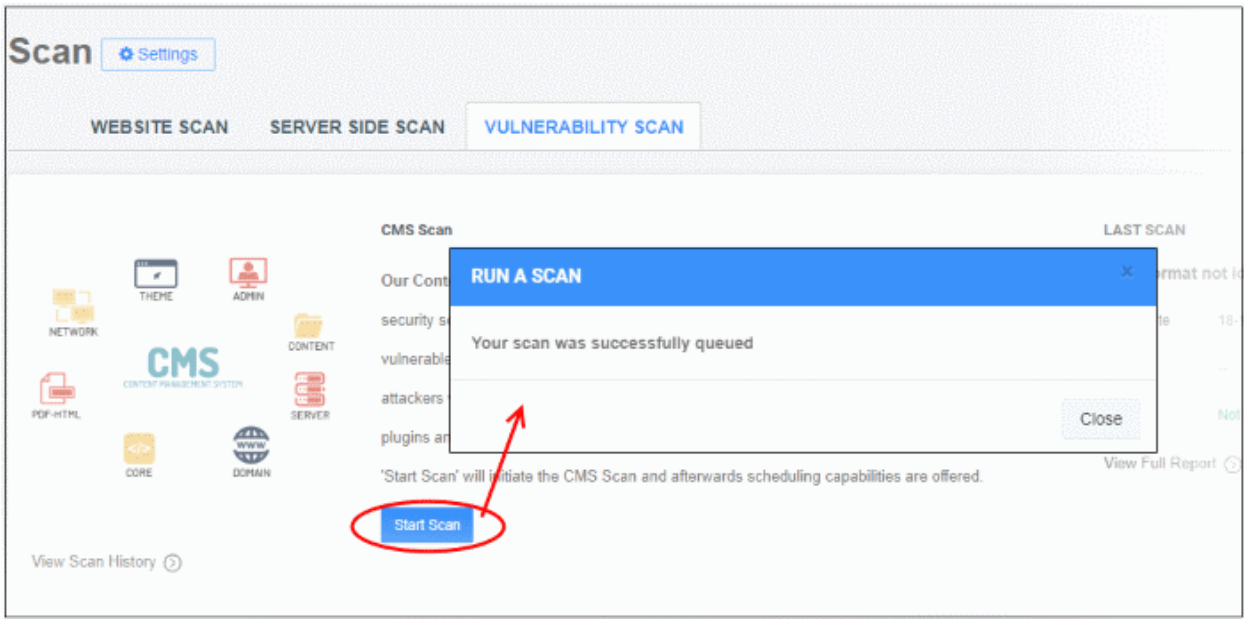
The pane lets you:

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

Start an on-demand CMS scan

You can manually start a CMS scan at anytime:

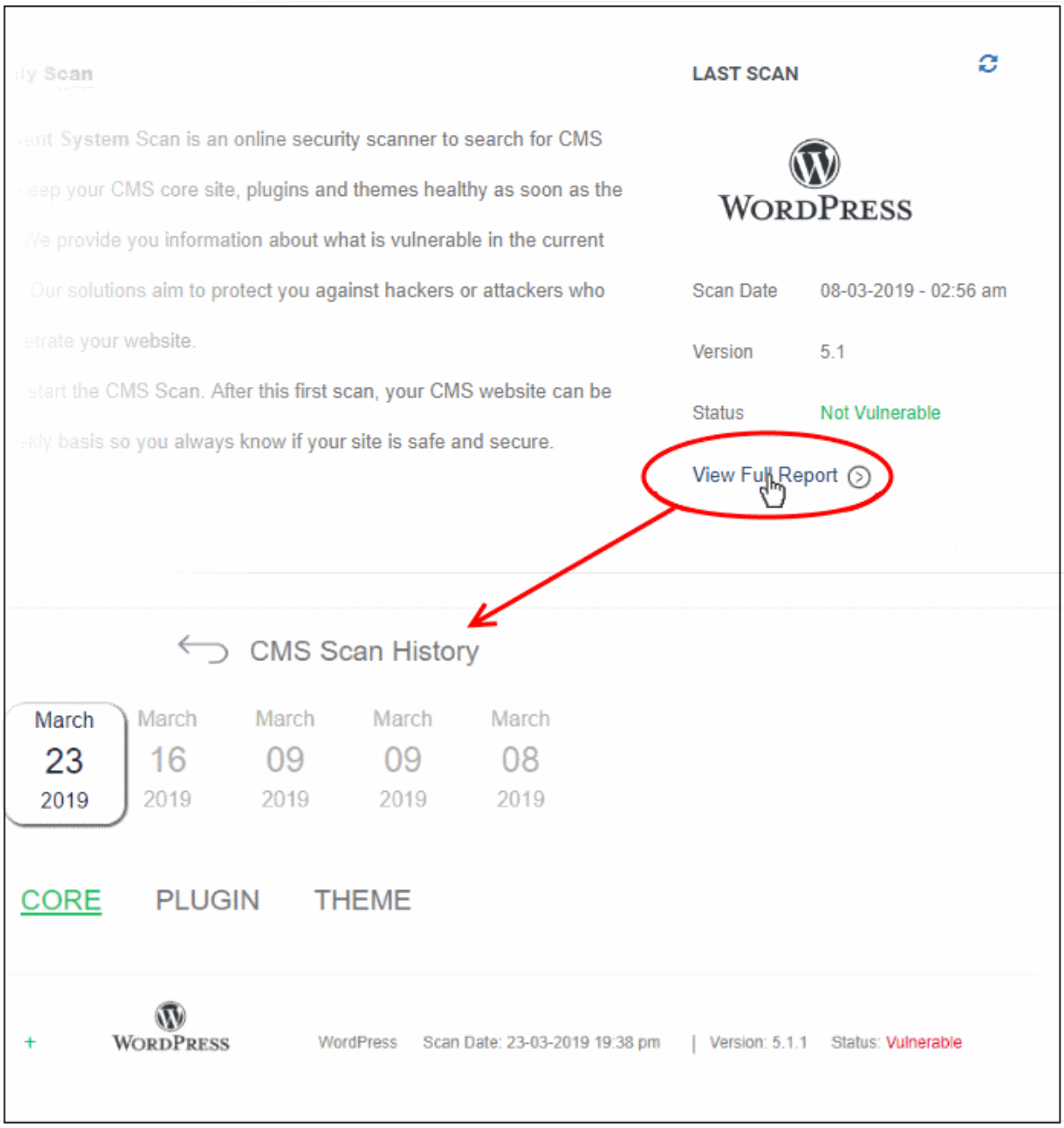
- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability Scan'



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

View detailed results

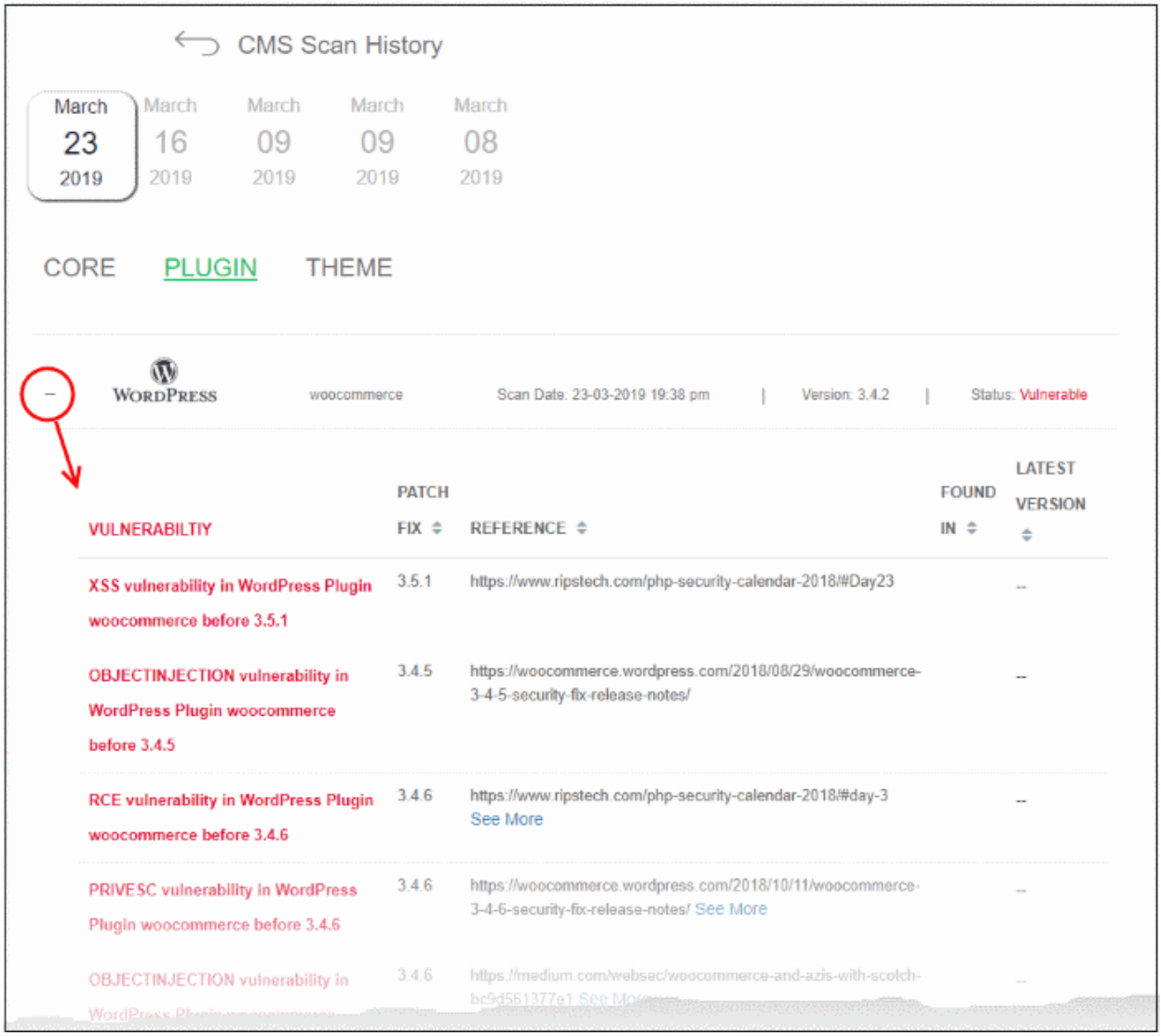
- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability Scan'
- Click 'View Full Report' under 'Last Scan' in the CMS scan pane as shown below:



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:



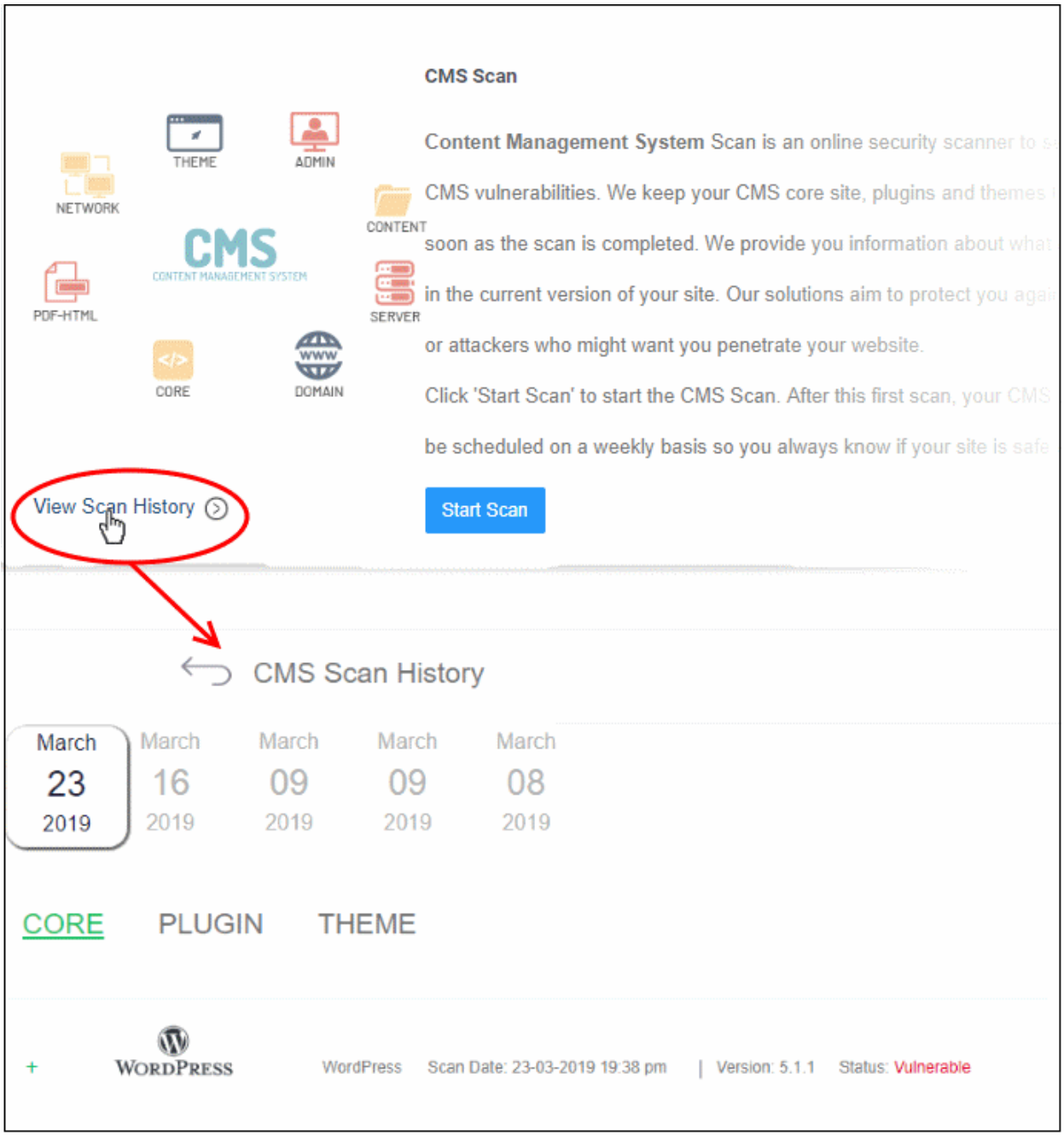
CMS Vulnerabilities - Column Descriptions	
Column Header	**Description**
Vulnerability	A short description of the weakness
Patch Fix	The version of the CMS in which the vulnerability was fixed. Update your CMS to this version to remove the vulnerability from your site.
Reference	Links to detailed information 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 'Scan' tab then 'Vulnerability Scan'
- Click 'View Scan History' in the 'CMS Scan' pane



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

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

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

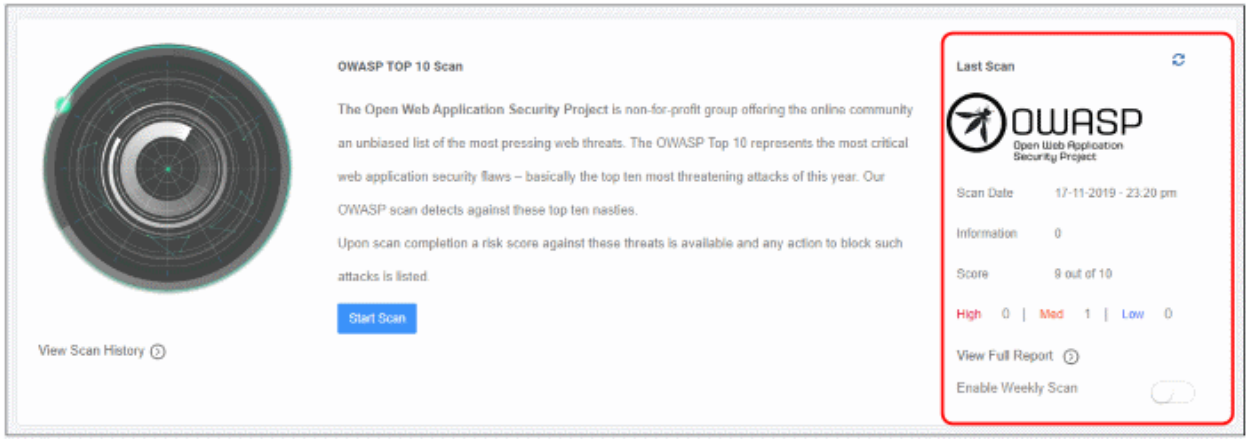
4.2.3.2 OWASP Top 10 Vulnerability Scans

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

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

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.

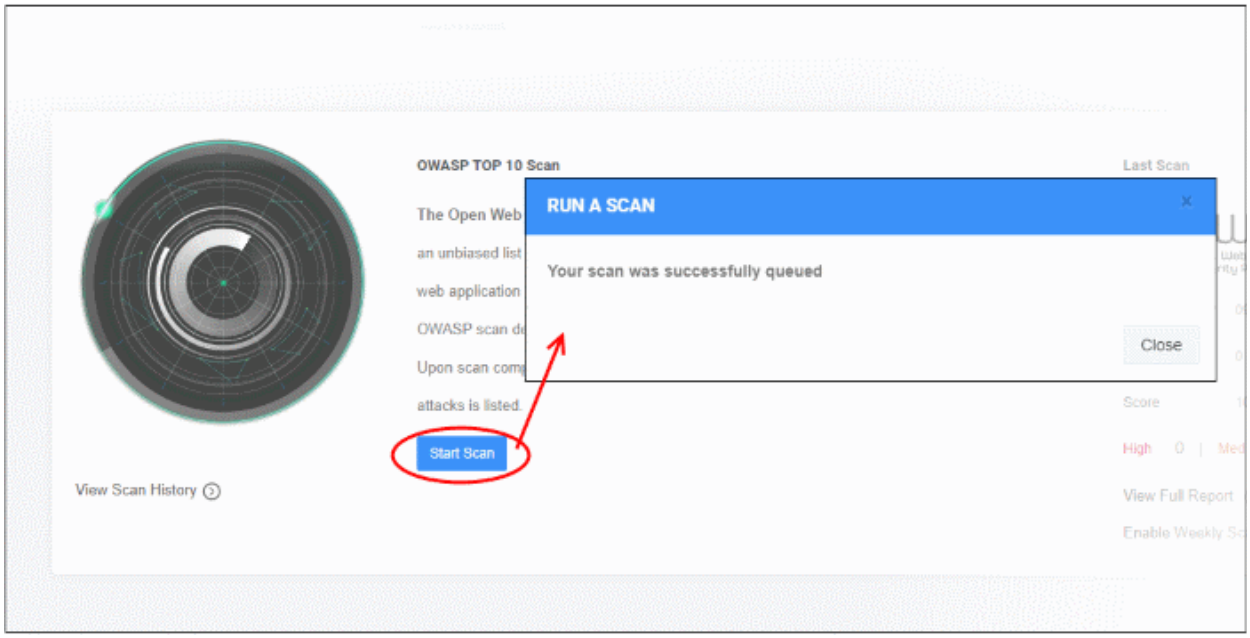
The pane lets you:

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

Run an on-demand scan

You can manually start a vulnerability scan at anytime:

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability Scan'
- Click 'Start Scan' in the 'OWASP Top 10 Scan' pane:

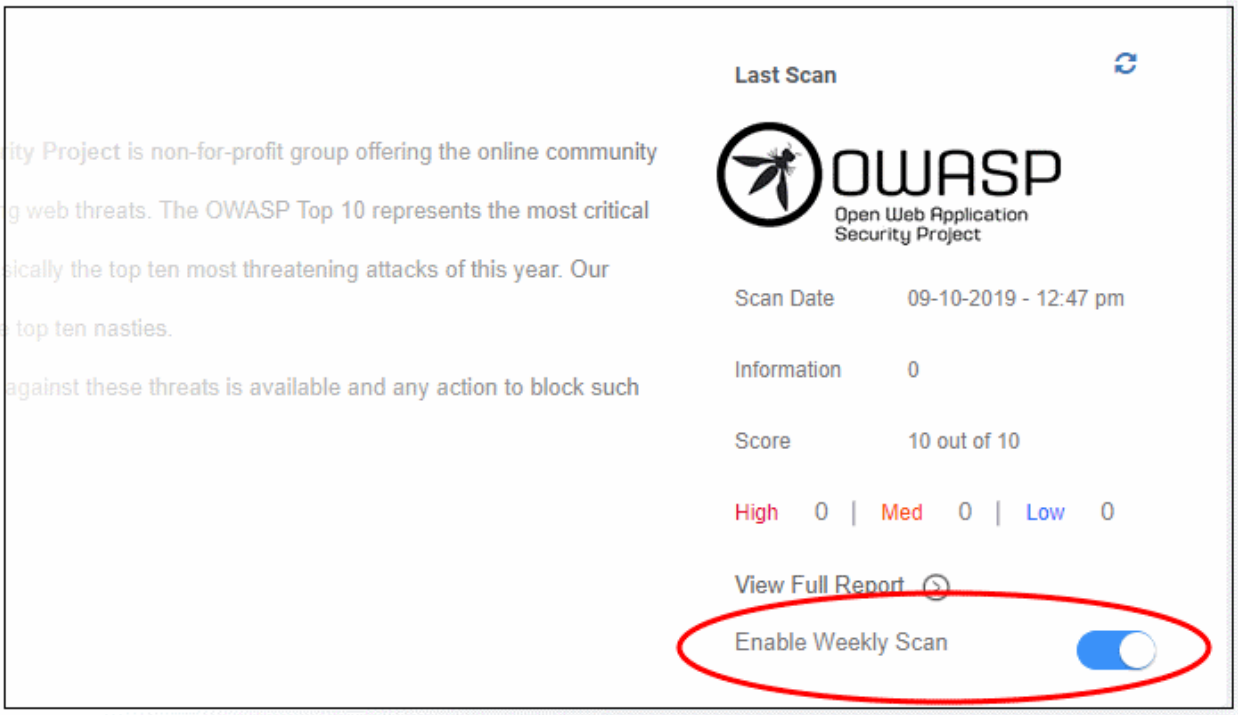


- cWatch will begin scanning the domain for OWASP top 10 vulnerabilities.
- Scan results are shown in the 'Last Scan' box on the right
- Click the 'Refresh' icon at top-right to reload the results of the scan
- Alerts will be generated if any vulnerabilities are found.
- Click 'View Full Report' for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

Schedule a scan

You can enable an automatic, weekly OWASP scans on any of your websites

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

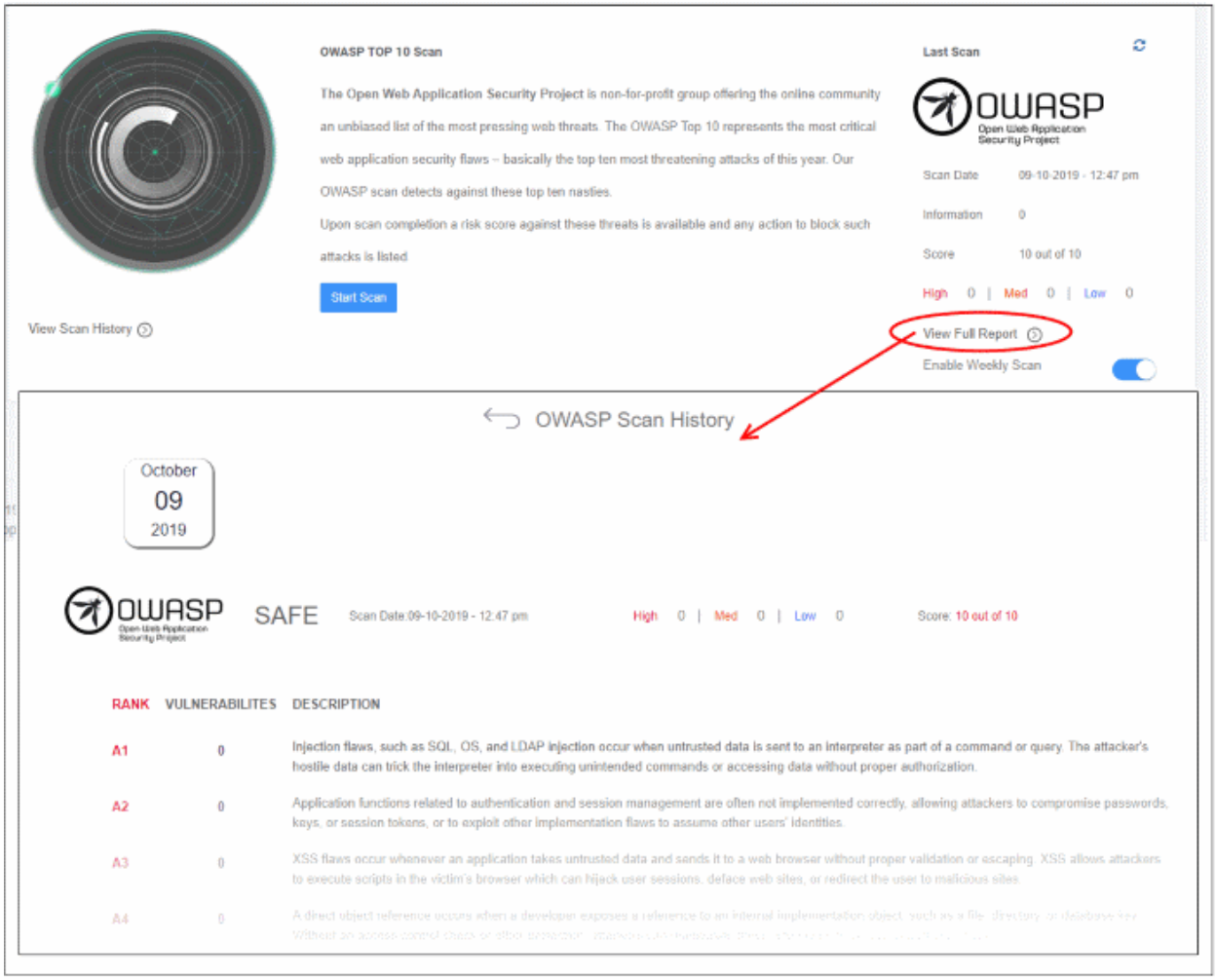


- Weekly scans will start the next day and will run at the same day/time every week after that.
- For example, if you enable the weekly scan at 6:00 PM on Friday, the scans will run every Saturday at 6:00 PM.

View detailed results of the last scan

- Select the target website from the menu at top-left
- Click the 'Scan' tab then 'Vulnerability Scan'
- 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.

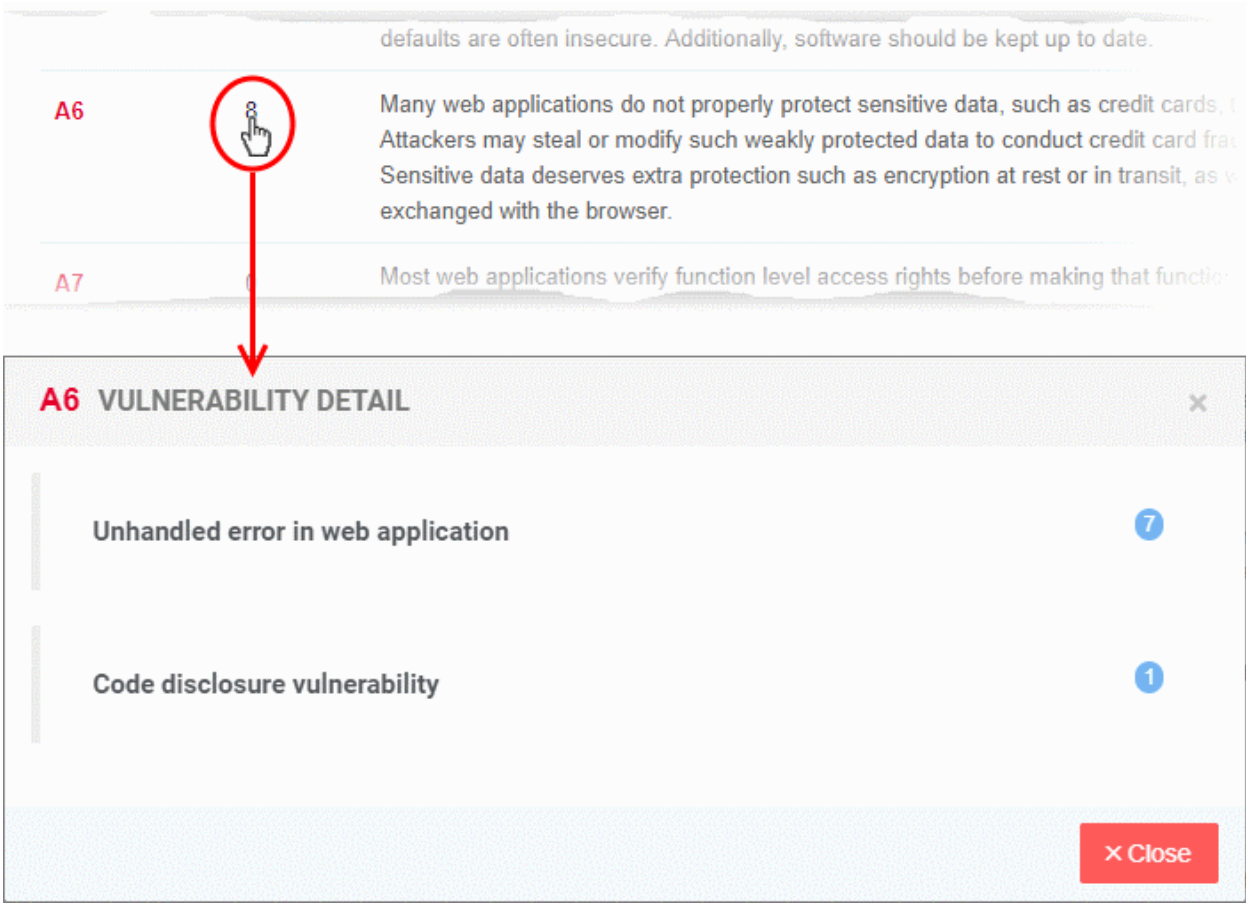
View detailed vulnerability information

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

- Click the 'Scan' tab then 'Vulnerability Scan'
- Click 'View Full Report' under 'Last Scan' in the 'OWASP Top 10' Scan pane

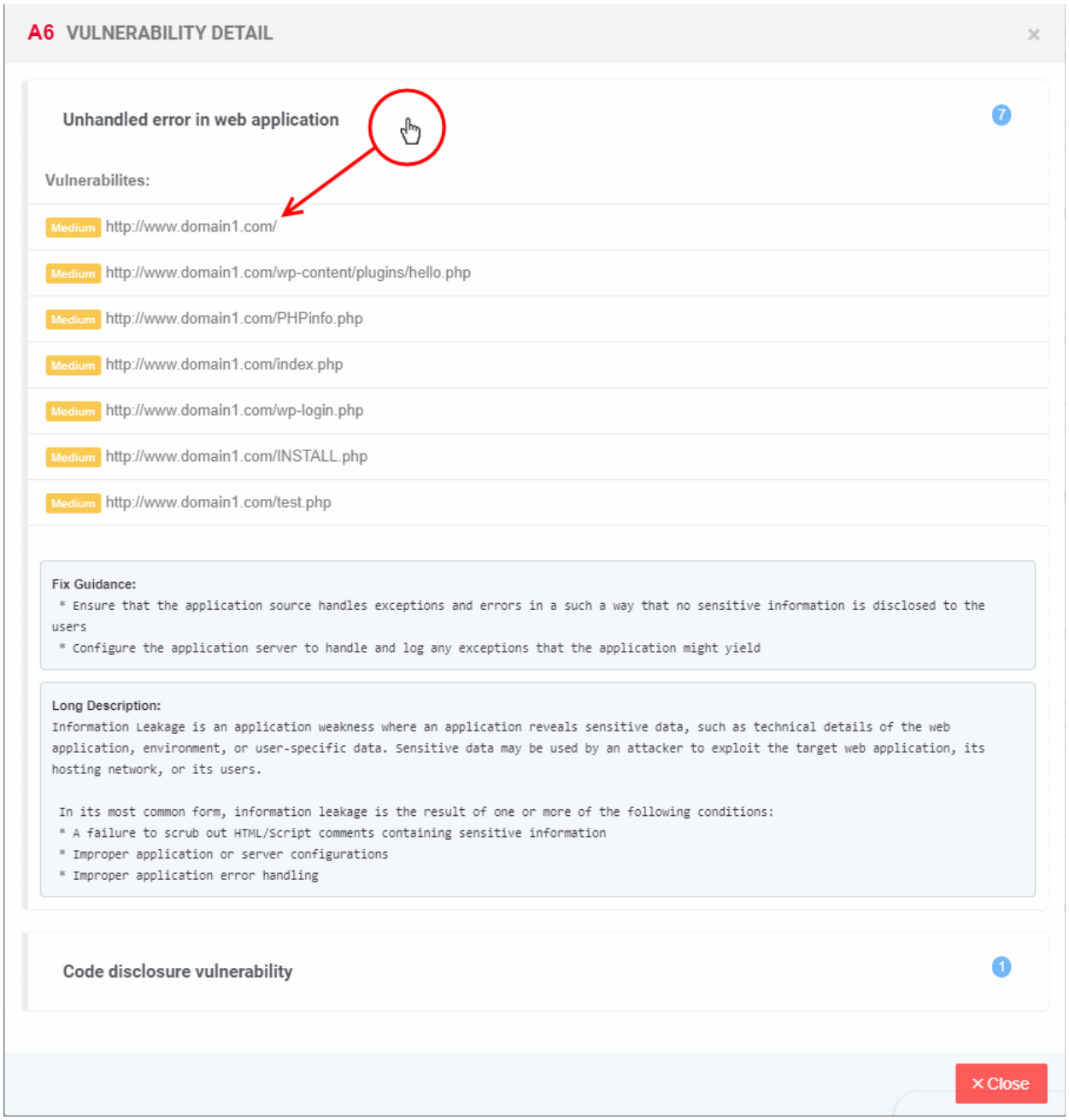
The numbers of vulnerabilities identified in each of the top ten OWASP vulnerability categories is shown as a list.

- 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:

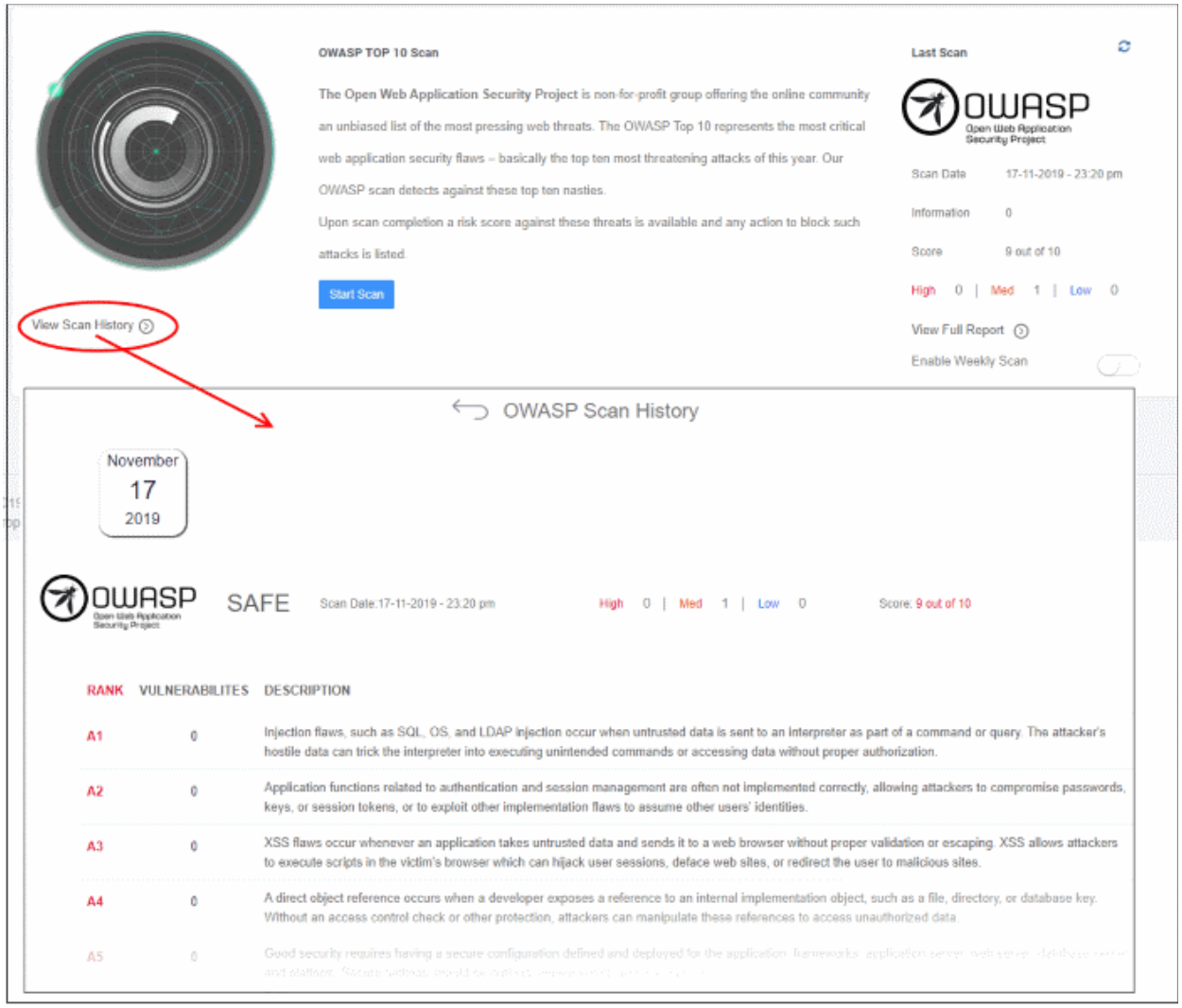


- The 'Vulnerabilities' pane shows a list of affected files with their risk level.
- The 'Fix Guidance' pane summarizes the fix recommendations.
- The 'Long Description' pane contains detailed background information on the threat

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 'Scan' tab then 'Vulnerability Scan'
- 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.

4.3 Content Delivery Network

- Select a website from the drop-down at top-left
- Choose 'CDN'
- Your cWatch license includes a content delivery network (CDN) for your websites. The service will improve page load-times for your customers and improve the reliability/uptime of your site.
- You can use the service by changing your domain's authoritative DNS to Comodo, or by adding a CNAME entry to your DNS records.
- Comodo Authoritative DNS name server (NS) details are provided in 'CDN' > 'Settings' > 'Activation'. The CNAME entry is generated by cWatch. See **Activate CDN for a Website** for more details.

Once activated and configured, the CDN service will:

- Accelerate performance by delivering site content from data centers closest to your visitor's location.

- Forward event logs to the Comodo CSOC team who will monitor the traffic for unusual behavior and threats.
- Provide Comodo web application firewall protection for your domains. The CSOC team constantly improves the Mod Security rules in Comodo web application firewall to provide cutting edge protection for our customers.

See the following sections for more help on CDN configuration:

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

4.3.1 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 CDN. Alternatively, you can add a CNAME entry to your DNS records.

See the following links for more help:

- **Register your site with Comodo DNS**

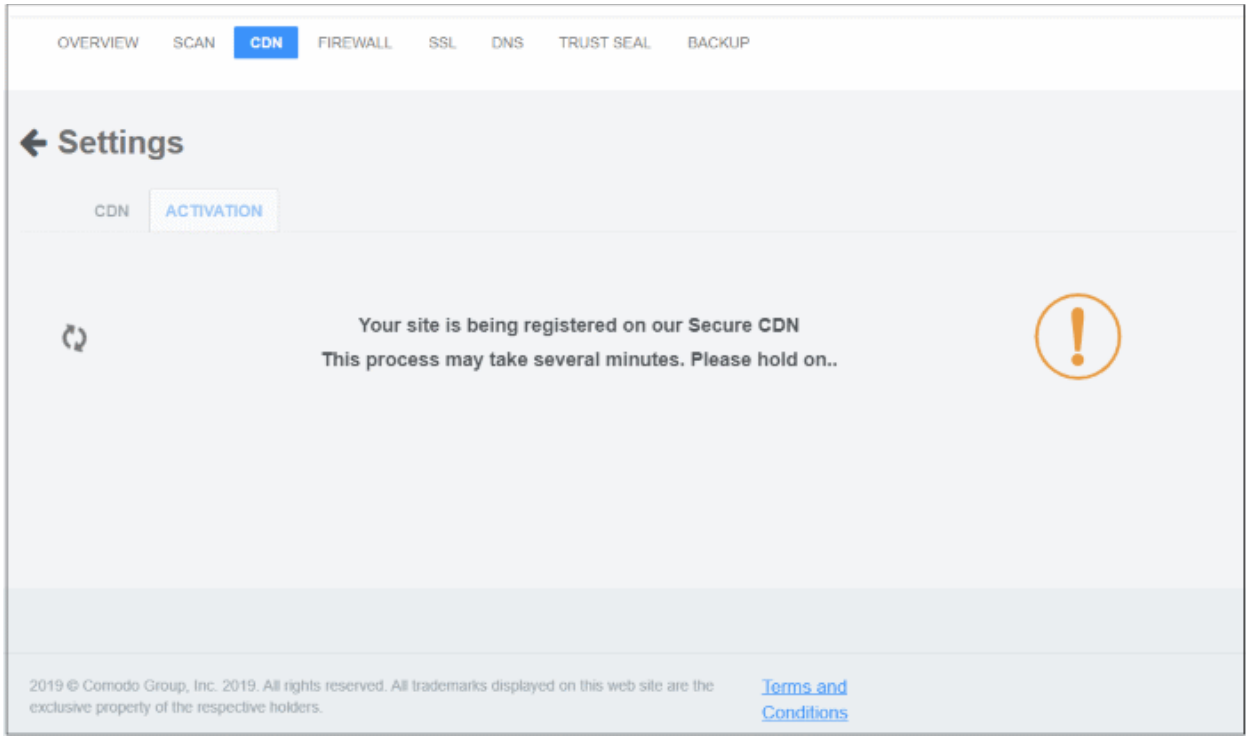
Activate the CDN:

- **Option A - Change your authoritative DNS to Comodo DNS**
- **Option B - Add a CNAME to your DNS**

Register your site with Comodo DNS

- Select the target website from the menu at top-left
- Click the 'CDN' tab
- Click 'Settings'
- Click the 'Activation' tab

cWatch automatically registers your site with the CDN service:



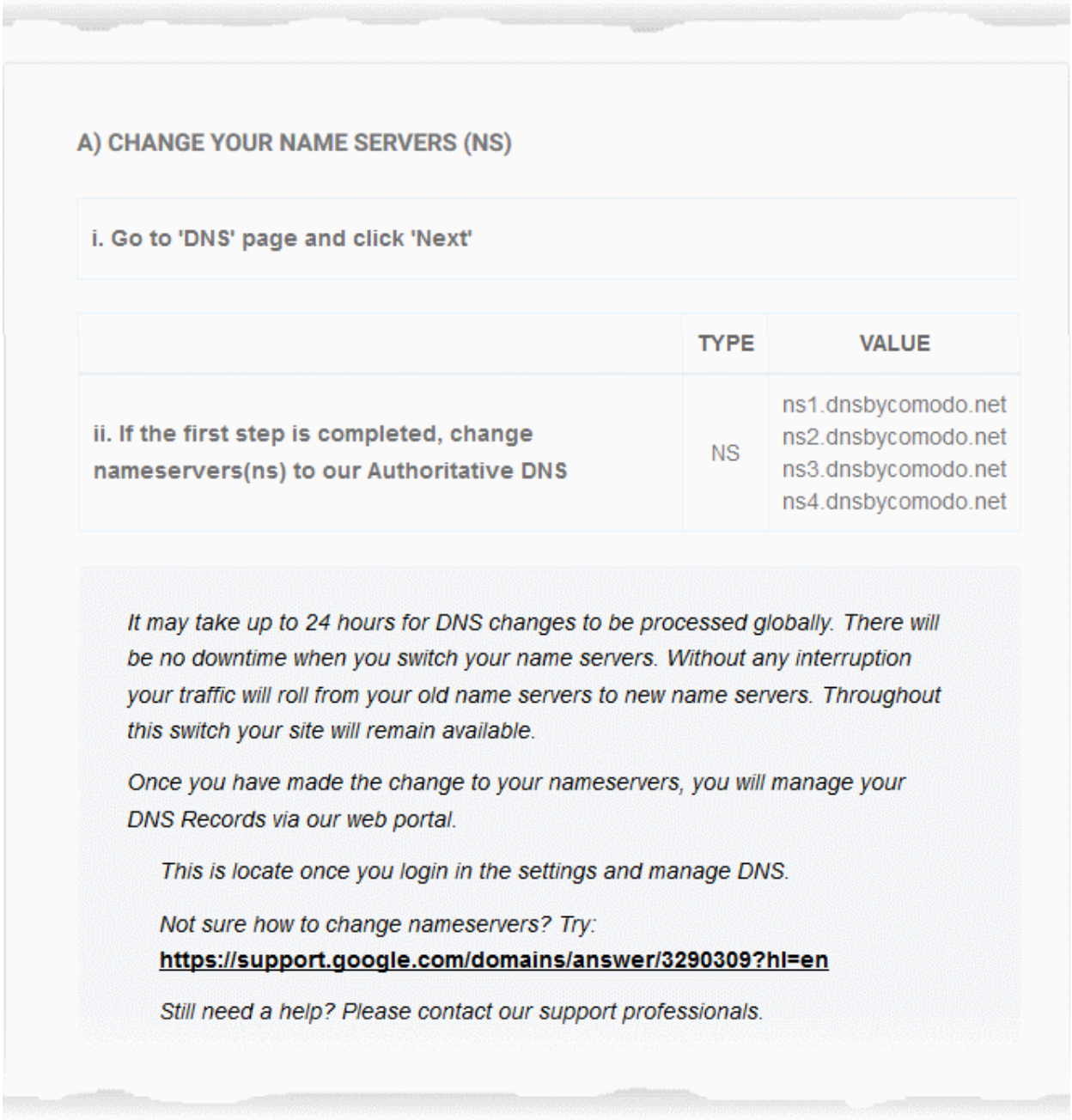
Next, use one of these two methods to configure your site to use our DNS:

- **Change your authoritative DNS to Comodo DNS**
- **Add a CNAME to your DNS**

Note – You should also configure SSL settings in cWatch to avoid interruptions to HTTPS traffic. See **SSL Configuration** for more on this.

Option A - Change your authoritative DNS to Comodo DNS

- Click CDN > Settings > Activation
- Comodo name servers are shown in the 'value' column:



A) CHANGE YOUR NAME SERVERS (NS)

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

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

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

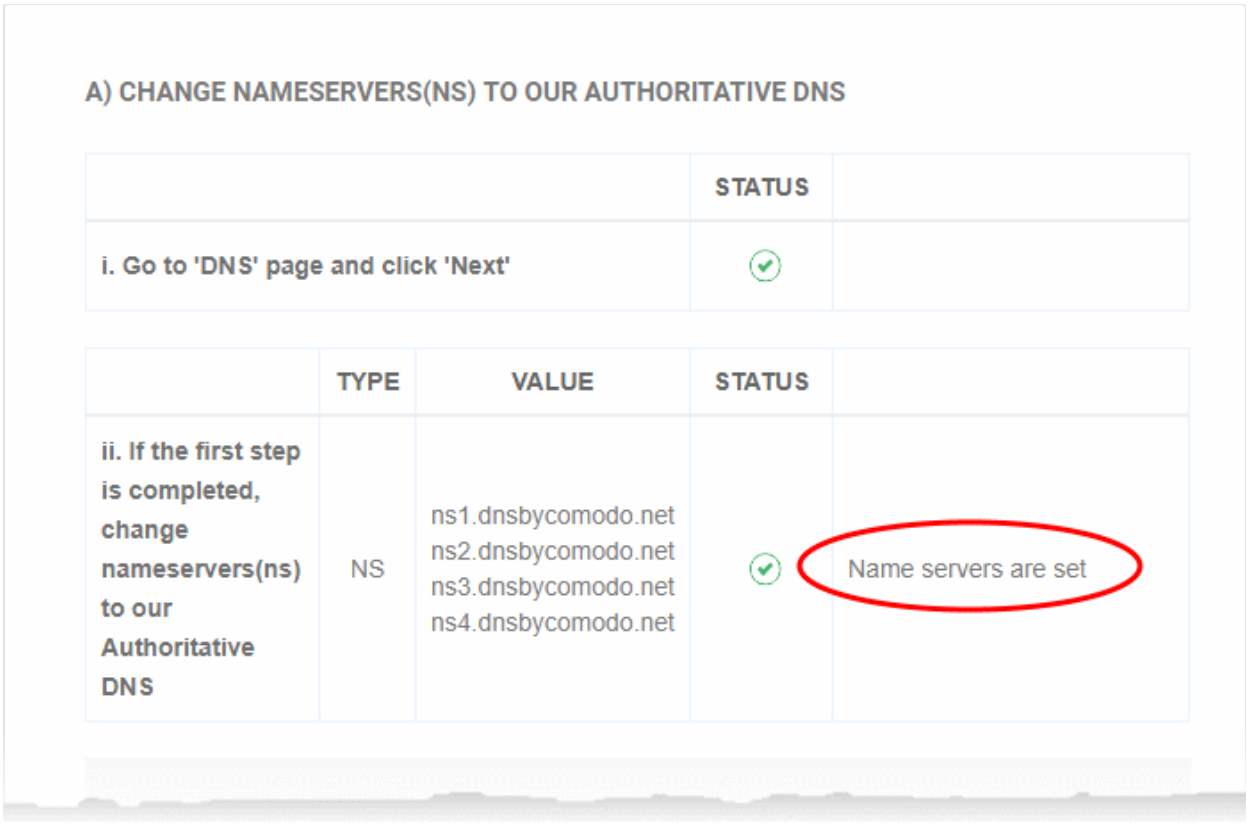
Once you have made the change to your nameservers, you will manage your DNS Records via our web portal.

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

Not sure how to change nameservers? Try:
https://support.google.com/domains/answer/3290309?hl=en

Still need a help? Please contact our support professionals.

- Go to your site's DNS management page and enter the new name servers.
- See **https://support.google.com/domains/answer/3290309?hl=en** if you need more help with name server changes.
- It may take up to 24 hours for the update to propagate. The status column will say 'Name servers are set' once the change is live:



A) CHANGE NAMESERVERS(NS) TO OUR AUTHORITATIVE DNS

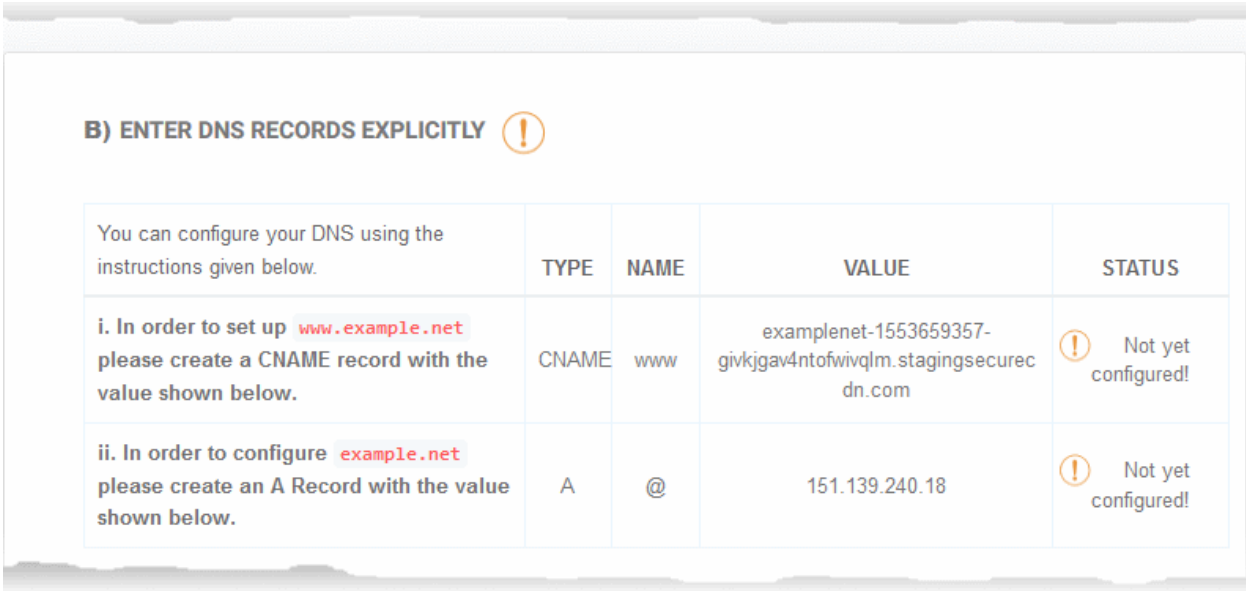
	STATUS	
i. Go to 'DNS' page and click 'Next'	✓	

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

- After changing to Comodo DNS, you need to use cWatch to manage your DNS settings going forward.
- For example, changes to your MX records must be done in cWatch, not in your web host's DNS management page.
- You can access the management page as follows:
  - Select a website from the drop-down at top-left
  - Click the 'DNS' tab to manage the site's DNS records
- See '**Manage DNS Records**' if you want further help with this.

Option B - Add a CNAME to your DNS

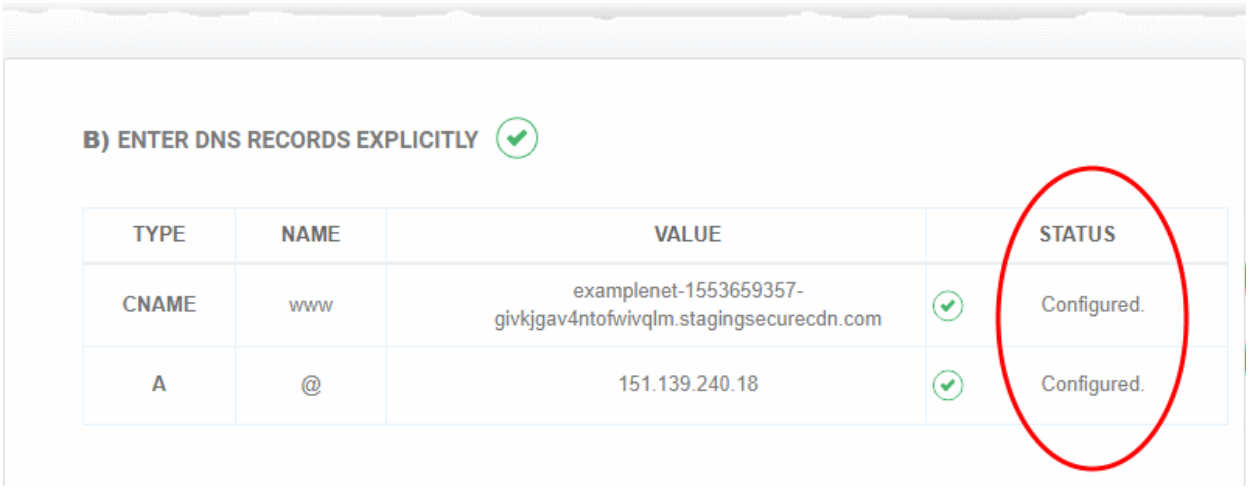
- Click 'CDN' > 'Settings' > 'Activation'
- The CNAME and A records for your site are shown in section B:



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!

- Go to your website's DNS management page and enter the 'CNAME' and 'A' records
- See **https://support.google.com/a/topic/1615038?hl=en** if you need more help to add records.
- DNS propagation may take around 30 minutes depending on your hosting provider.
- The status column will say 'Configured' once the change is live:



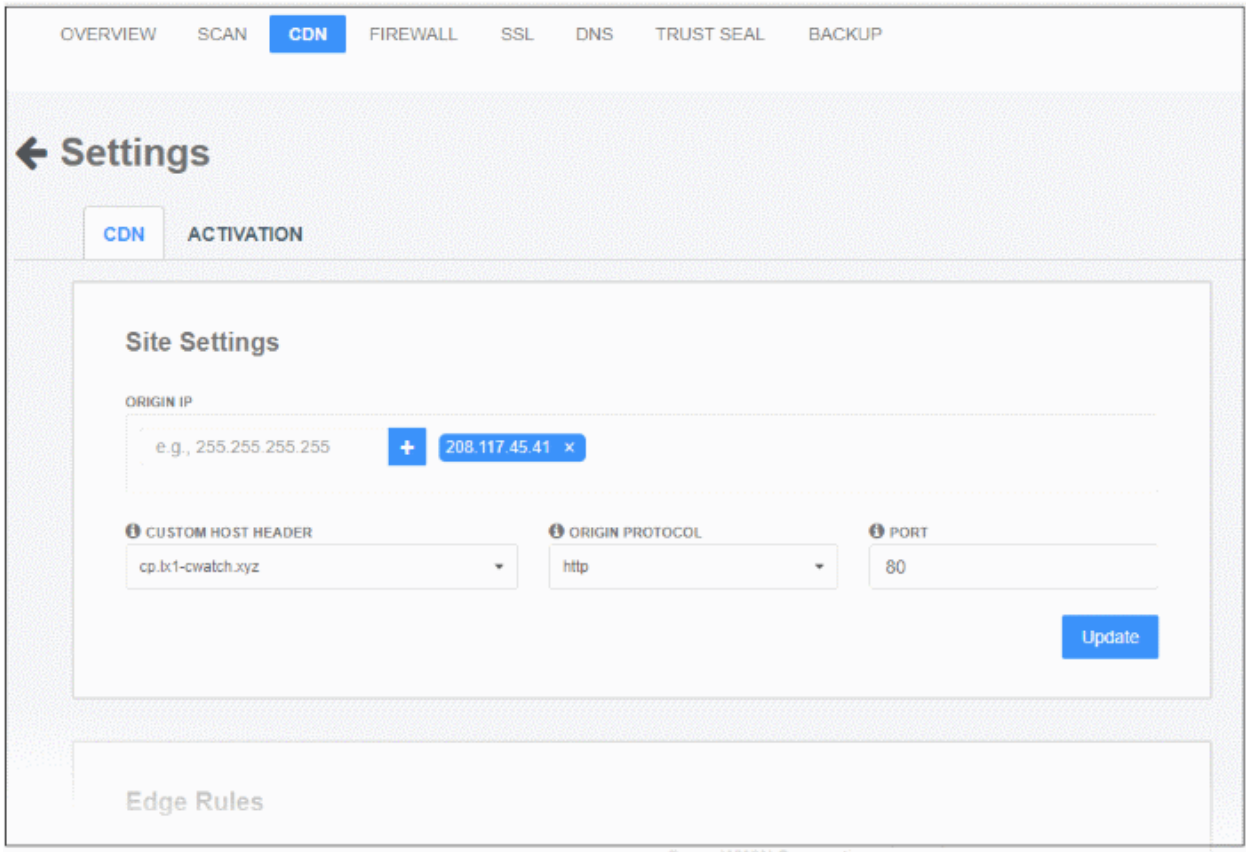
B) ENTER DNS RECORDS EXPLICITLY

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

4.3.2 CDN Settings

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

- Open the cWatch dashboard
- Choose the target website from the drop-down at top-left
- Click 'CDN' > 'Settings' > 'CDN'



Click the following links for help with each box on the settings screen:

- **Site Settings**
- **Edge Rules**
- **Cache Settings**
- **Purge Files**
- **Quick Configuration**

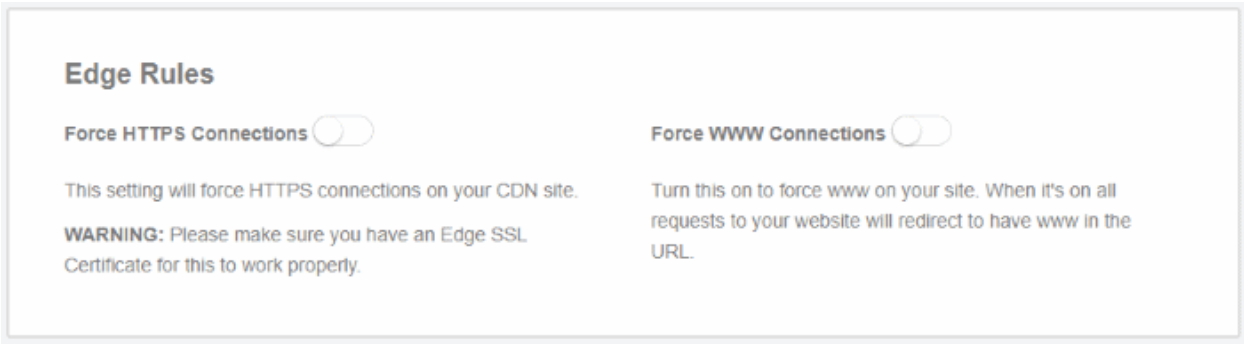
Site Settings

- **Origin IP** – The website's IP address. The CDN will collect the site's content from this IP.
  - Enter the site's IP then click the '+' button. You can add multiple origin addresses. The CDN will load balance from the list of origins.
- **Custom Host Header** – Enter the domain name of the origin website. For example, simply enter **www.yourwebsite.com**

  Background – If you don't complete the custom host header field, then the CDN will simply retrieve the default website at the origin IP. While this is OK if there is only one site hosted in the IP, it can be problematic if the IP hosts multiple sites. By specifying your domain, you tell the CDN exactly which website to collect.
- **Origin Protocol** - Select whether is hosted over HTTP or HTTPS. Choose the https or http version of your URL as appropriate.
- **Port** – The port number on the origin that the CDN should connect to.

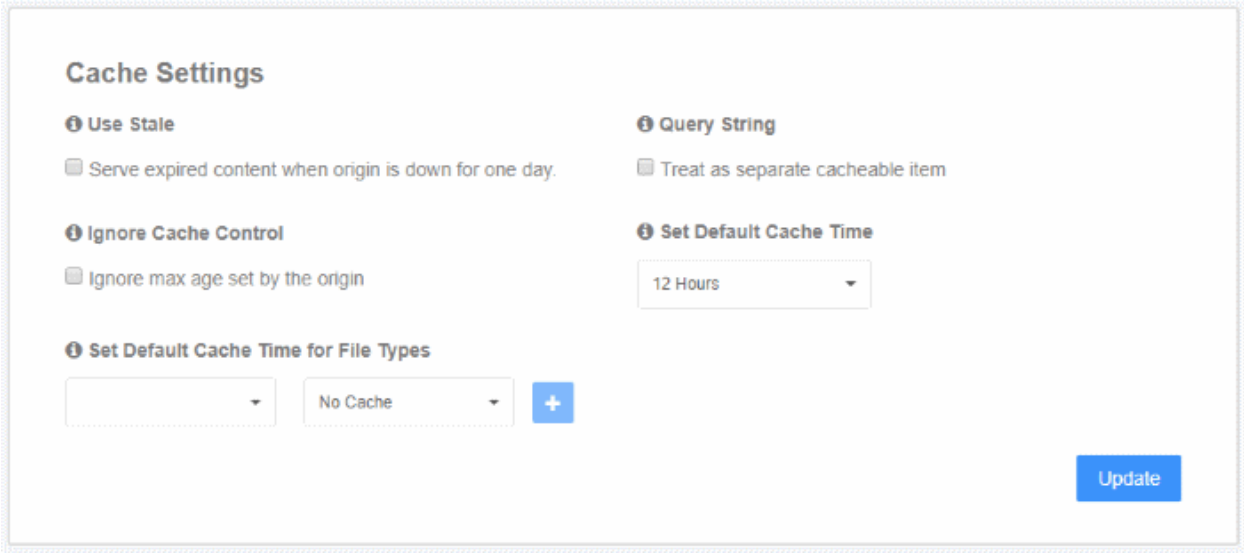
Click 'Update' to save your changes.

Edge Rules



- **Force HTTPS Connections** – Ensures your site is only ever served over a secure, HTTPS, connection. Any requests made over HTTP will be converted to HTTPS. Make sure that you have uploaded your SSL certificate to CDN edge servers. See **SSL Configuration** for help to do this.
- **Force WWW Connections** – Resolves all requests for your domain to the www version. For example, requests for **https://your-website.com** will be redirected to **https://www.your-website.com**

Cache Settings

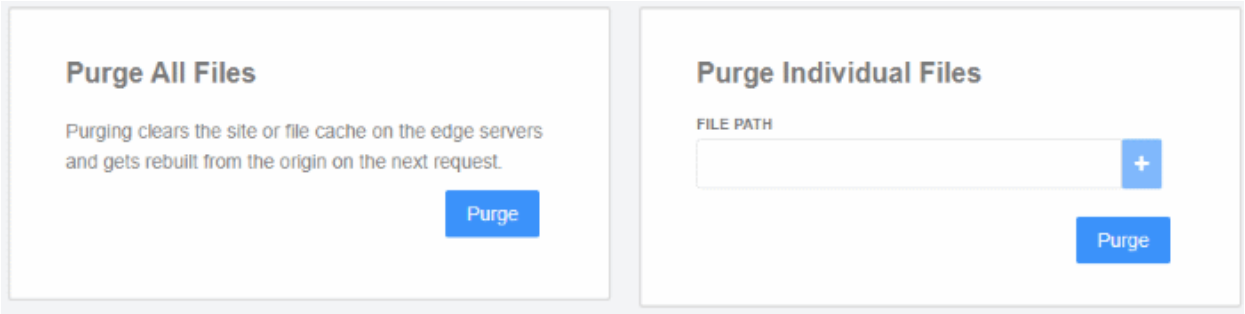


- **Use Stale** – Enable to serve cached-but-expired content to your visitors if your site is not-reachable for 24 hours or more. This is useful to ensure you keep a web-presence if your server is hit by problems.
- **Query String** - Web-pages with a query string (e.g.'?q=something') will be cached as separate files. CDN updates the cached files whenever the original pages are updated.
- **Ignore Cache Control** – Enable this to invalidate cache settings on the origin. Selecting this option will automatically disable 'Use Stale' setting above.
- **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.
- **Set Default Cache Time for File Types** – Define how long files should be cached before they are forced to request a new copy from your origin.
  - Select the file type from the first drop-down and set the cache time in the second. Click '+' to add the file type. Repeat to add more file types.

Click 'Update' to save your changes.

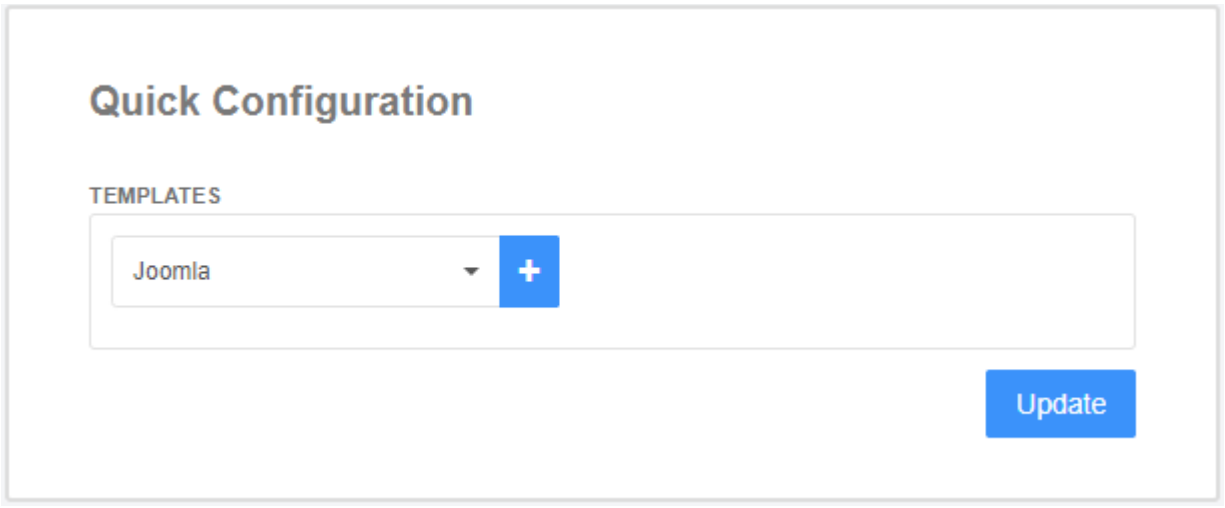
Purge Files



- **Purge All Files** – Manually remove all cached files so the CDN is forced to check your website the next time the files are requested.
- **Purge Individual Files** - Remove specific files from the cache so that the CDN is forced to check your website the next time these files are requested.
  - Enter the URI of the file in the box then click the blue '+' button
  - Repeat the process to add more files
  - Click 'Purge'

Quick Configuration

Tell cWatch the content management system (CMS) used to develop your site. Doing so helps accelerate CDN setup and performance. While cWatch supports all content management systems, quick configuration currently only supports Joomla and WordPress.

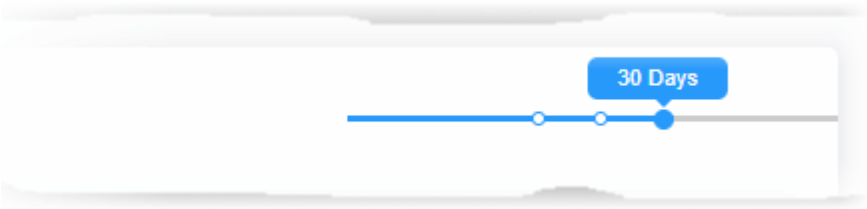


- Select a CMS type and click the '+' button. Repeat to add more types.
- Click 'Update' to save your settings.

4.3.3 View CDN Metrics

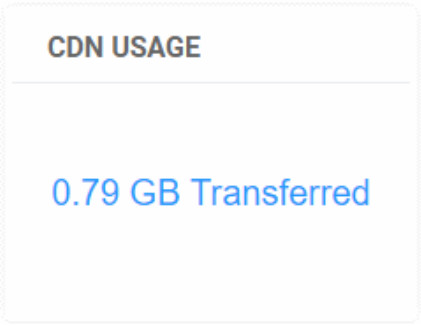
The metrics page shows your site's traffic usage, the origins of your traffic, and page error/status codes.

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



The page contains the following charts:

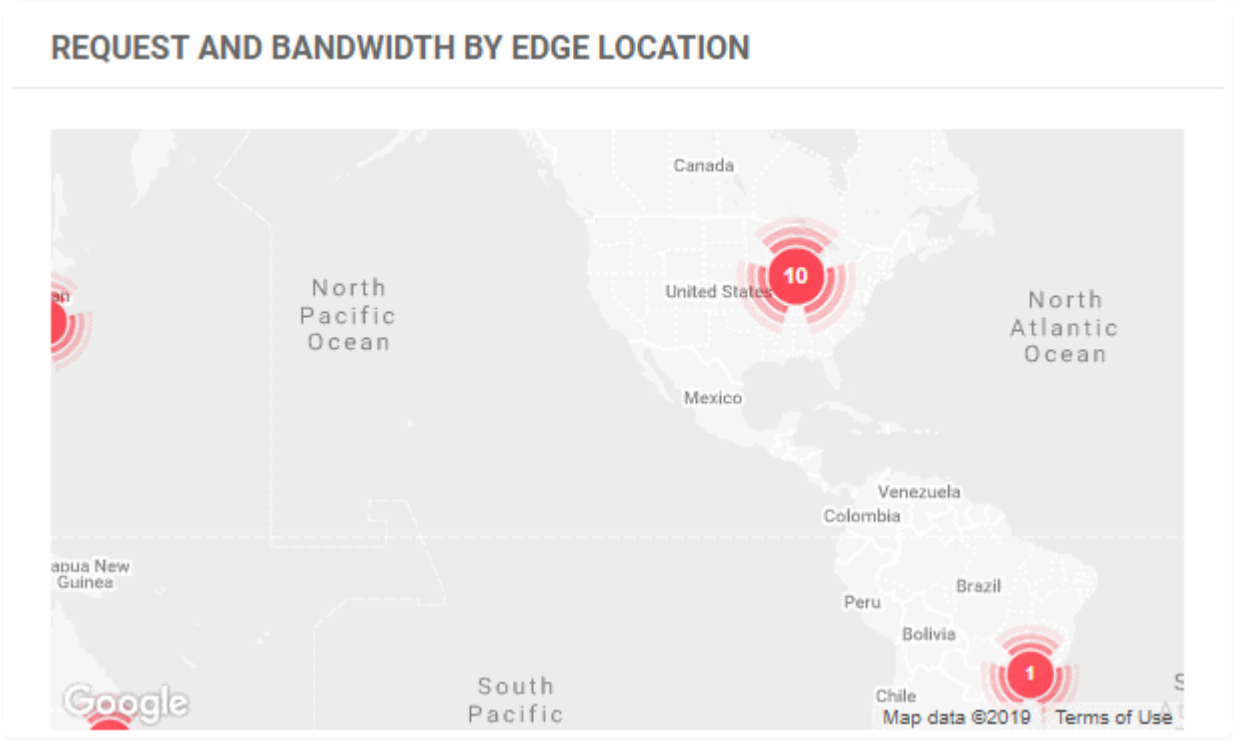
CDN Usage



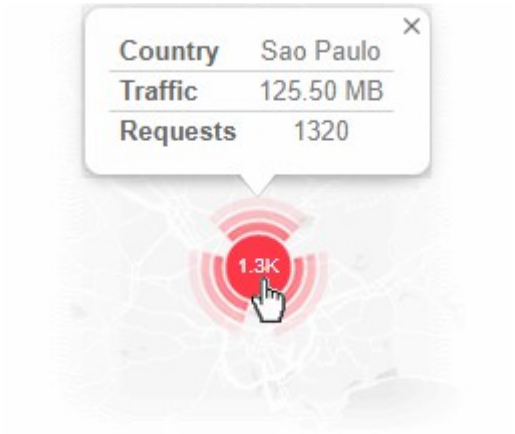
How much data the CDN has handled on behalf of your site.

Request and Bandwidth by Edge Location

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

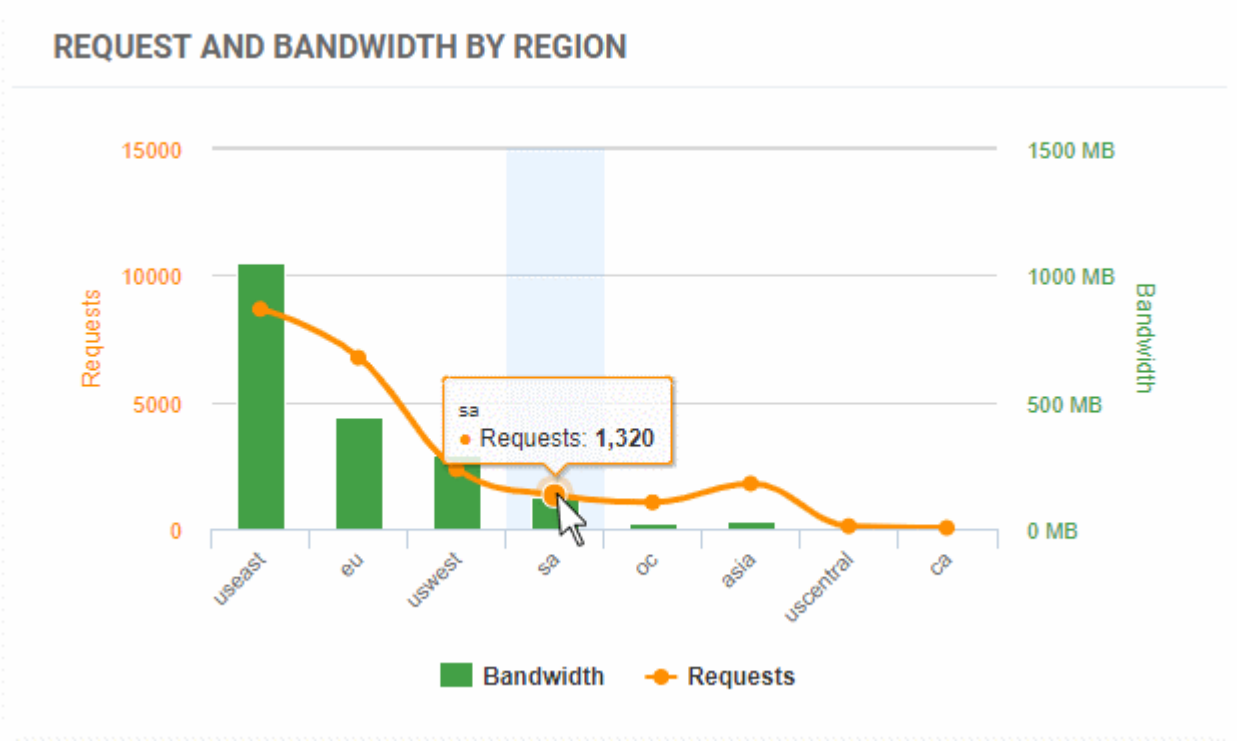


- Click on a hot-spot to view traffic and request volume from that area:



Request and Bandwidth by Region

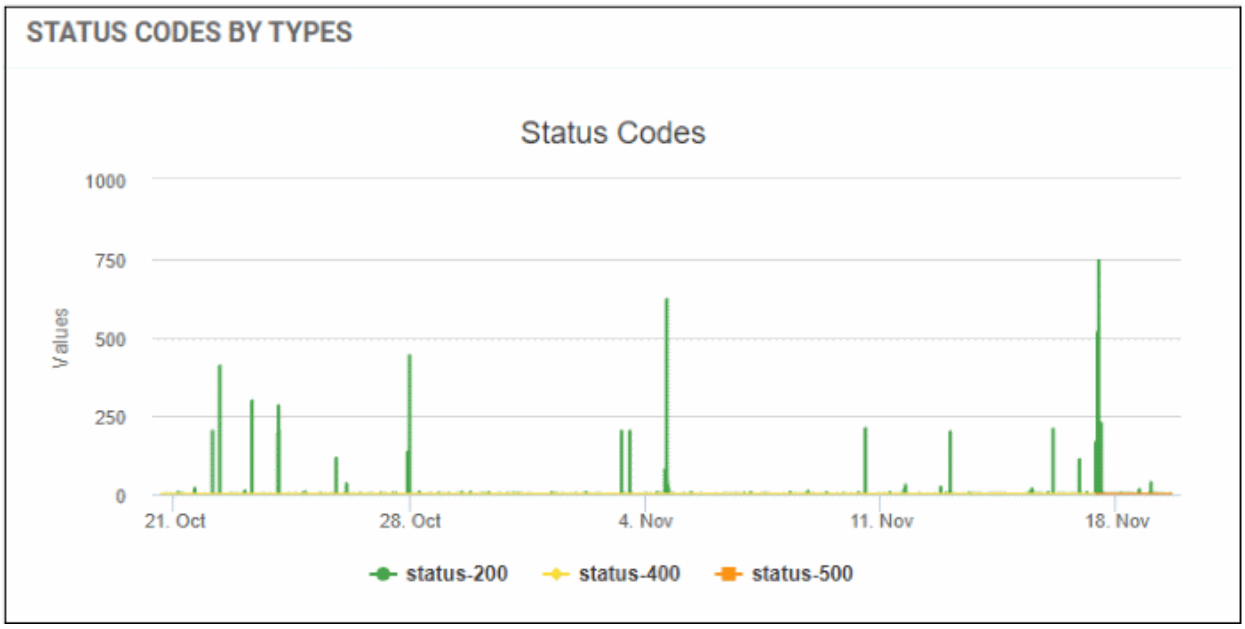
Shows the number of site requests and the amount of data downloaded by each continent.



- Select a portion of the graph to zoom-in
- The yellow line shows the number of requests from different regions
- The green bars show the amount of traffic downloaded by different regions

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

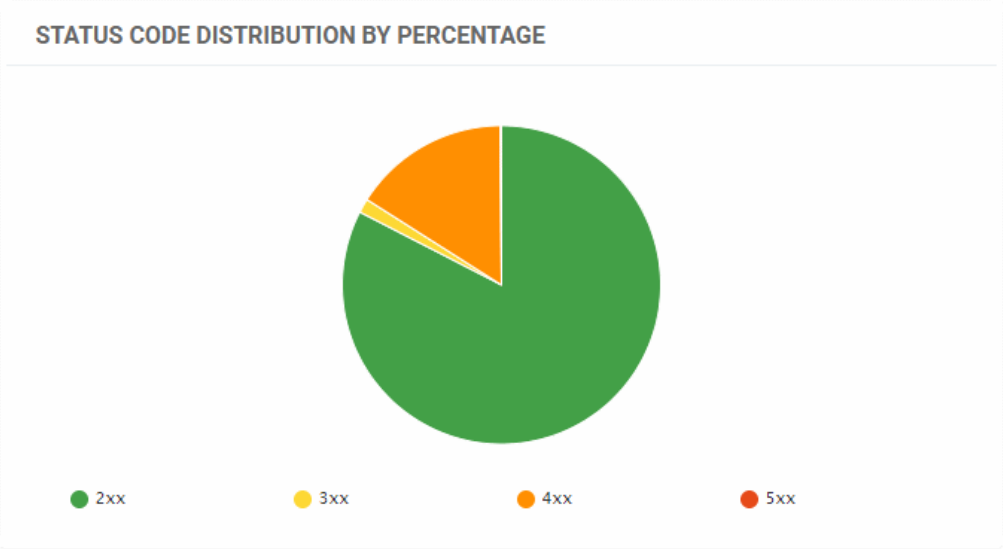
- You can choose the time period using the slider at top-right.

Status Code Distribution by Percentage

- A more detailed breakdown of HTTP response codes from your site within the set time period.

  HTTP status codes are as follows:

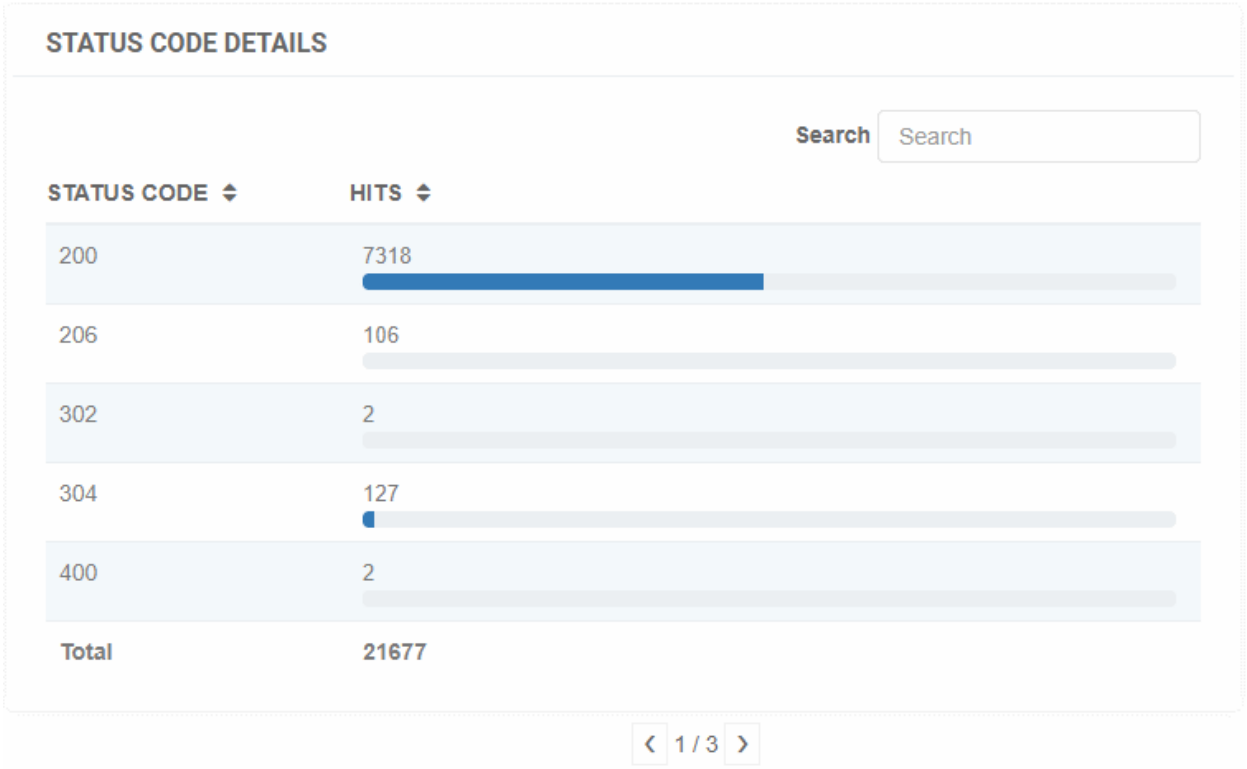
  - 1xx Informational responses.
  - 2xx Success.
  - 3xx Redirection.
  - 4xx Client errors.
  - 5xx Server errors.



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

Status Code Details

- Lists how many of each HTTP response code were shown in the selected time period.
- '200' class codes - Success. Page displayed correctly/The server was able to fulfil the request
- '300' class codes - Redirection. The user requested a page but was redirected to a different page.
- '400' class codes – Errors. The requested page could not be provided for some reason.
- A more detailed explanation of each code is available at **https://en.wikipedia.org/wiki/List_of_HTTP_status_codes**.



- 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

4.4 Firewall

- Select a website from the drop-down at top-left
- Click the 'Firewall' tab.

The firewall section contains real-time statistics about attacks blocked on your site. You can also configure firewall settings, create custom firewall rules, and view results from the cyber security operation center.

Please see the following links for help with each section:

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

4.4.1 WAF Statistics

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.

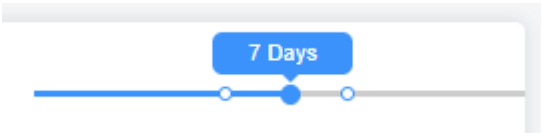
You can also choose the action taken on future threats from the same source. cWatch updates your WAF rules accordingly.

Notes:

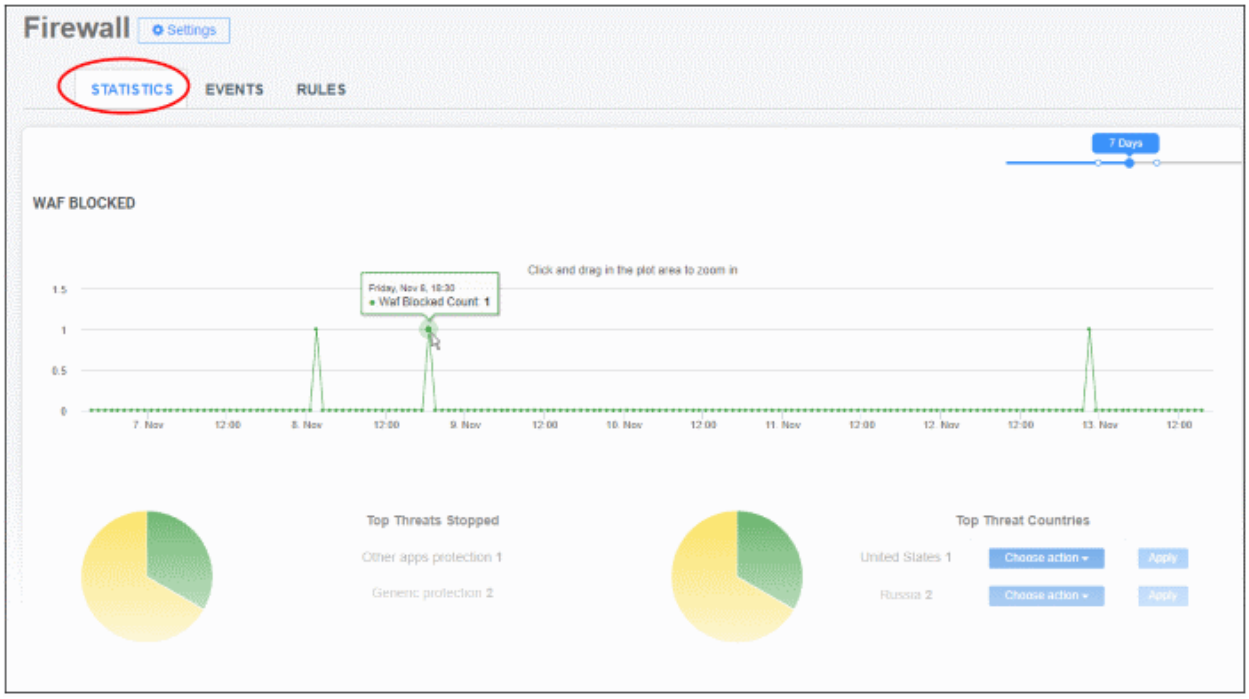
- The web application firewall is only available on 'Pro', 'Premium' and 'WAF Starter' licenses.
- To enable the firewall, you need to change the authoritative DNS of the site to Comodo Secure DNS. See **DNS Configuration** for help with this.

View WAF statistics

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Firewall' tab
- Open the 'Statistics' tab if not already open
- Select the period for which you want to view statistics from the slider at top-right:

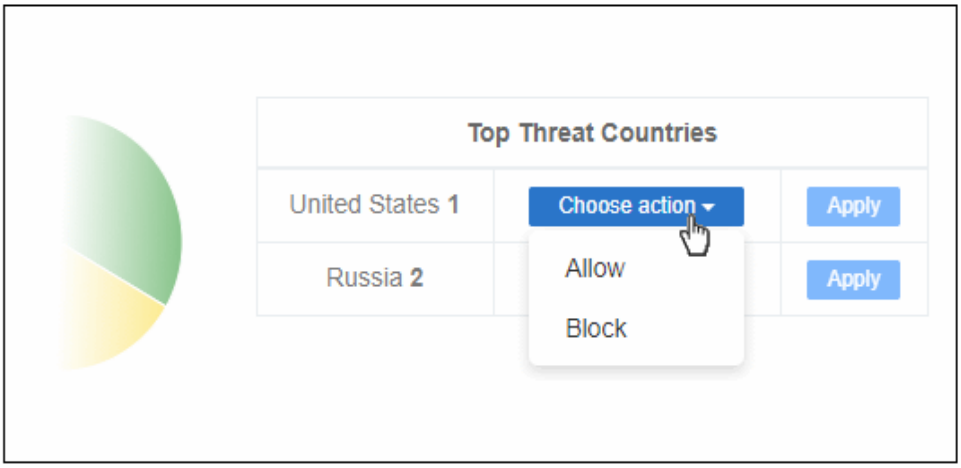


The 'WAF blocked' charts shows a history of attacks blocked by the firewall over time:



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.

- **Top 5 countries** - The 5 countries from which the highest number of attacks originated.
- **Choose action** - Specify how to deal with future traffic from the country:



- **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.

The action you choose above will create a custom rule for traffic from the country. Custom firewall rules require a 'Premium' license for the site.

Click 'Apply' to save your choice. See **Manage Custom Firewall Rules** for more details on managing custom firewall rules.

4.4.2 WAF Events

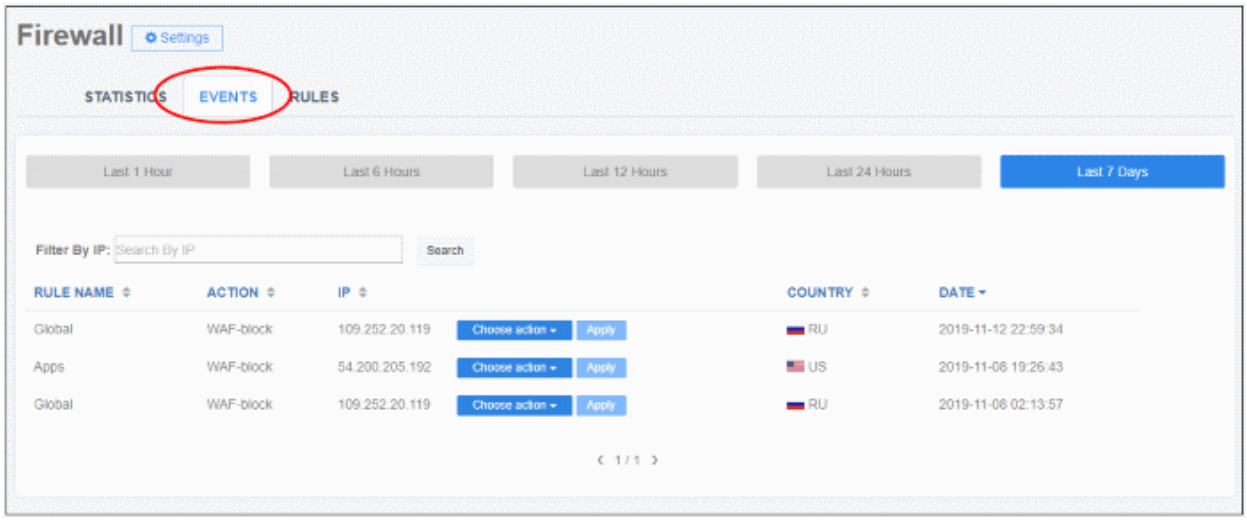
- The events page shows all traffic intercepted by a firewall rule.
- Event details include the source IP of the attempt, the rule that caught the attempt, and the action taken on the traffic.
- You can also choose how to deal with future incidents of the same type from the same source.

Notes:

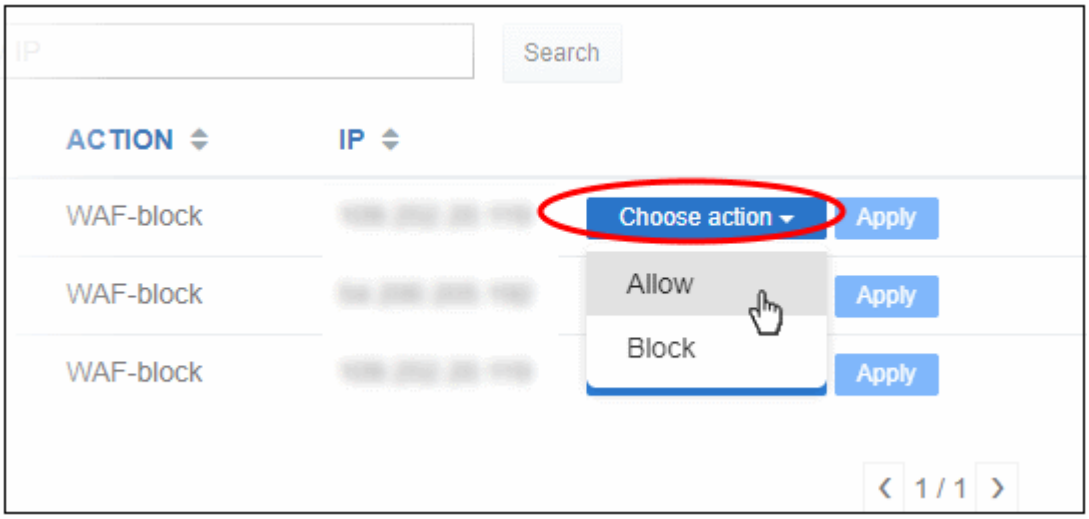
- The web application firewall is only available on 'Pro', 'Premium' and 'WAF Starter' licenses.
- To enable the firewall, you need to change the authoritative DNS of the site to Comodo Secure DNS. See **DNS Configuration** for help with this.

View WAF Events

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



- **Rule Name** - The firewall rule that intercepted the access request
- **Action** - The activity of the access request on the website
- **IP** - The 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
- **Choose action** - Specify how to deal with future traffic from the same IP address.



- **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.

The action you choose above will start a wizard to create a custom firewall rule. Custom firewall rules require a 'Premium' license for the site.

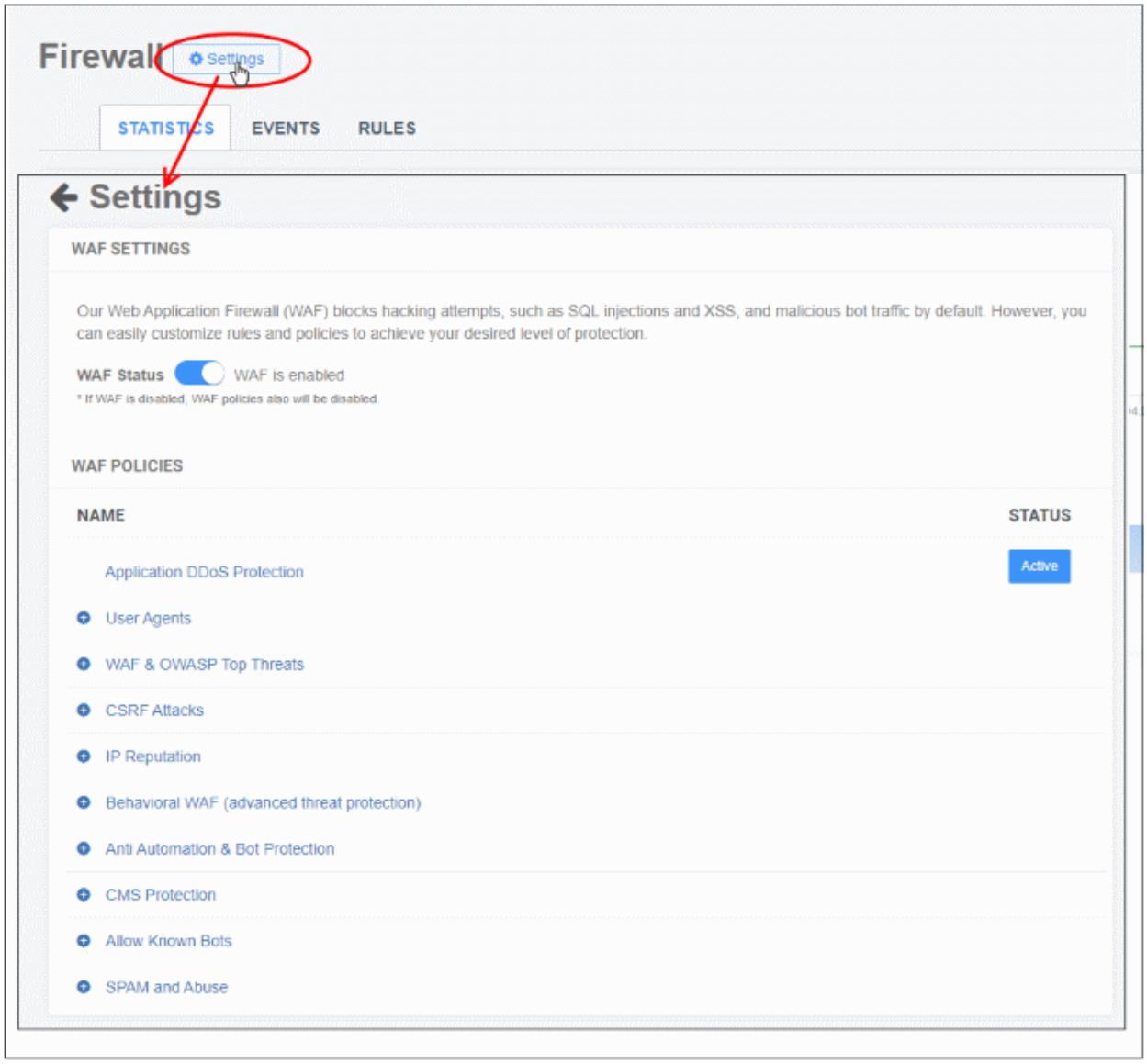
Click 'Apply' to save your choice. See **Manage Custom Firewall Rules** for help on custom firewall rules.

4.4.3 Configure WAF Policies

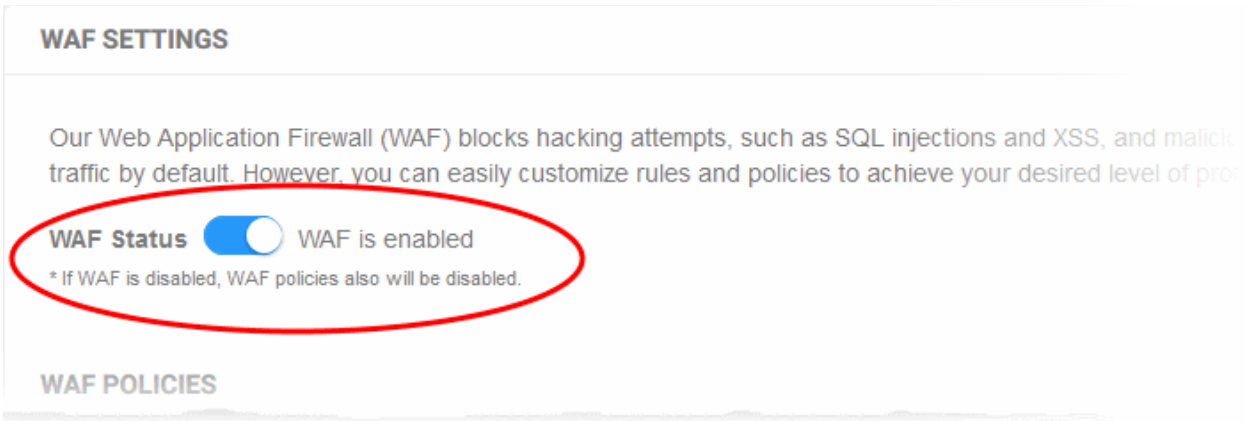
- A firewall policy is a collection of firewall rules designed to filter traffic for a website. Firewall policies protect the site from a vast range of internet threats, including SQL injections, bot traffic and more.
- cWatch ships with built-in rules for the web application firewall (WAF) which provide the highest levels of protection for your website.
- There are several types of WAF policy, each with a set of constituent rules. You can enable or disable rules as required.
- You can create custom rules if required. See **Manage Custom Firewall Rules** if you want to learn about this.

Configure WAF settings

- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'Firewall' tab
- Click 'Settings' to open the 'WAF Settings' page



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

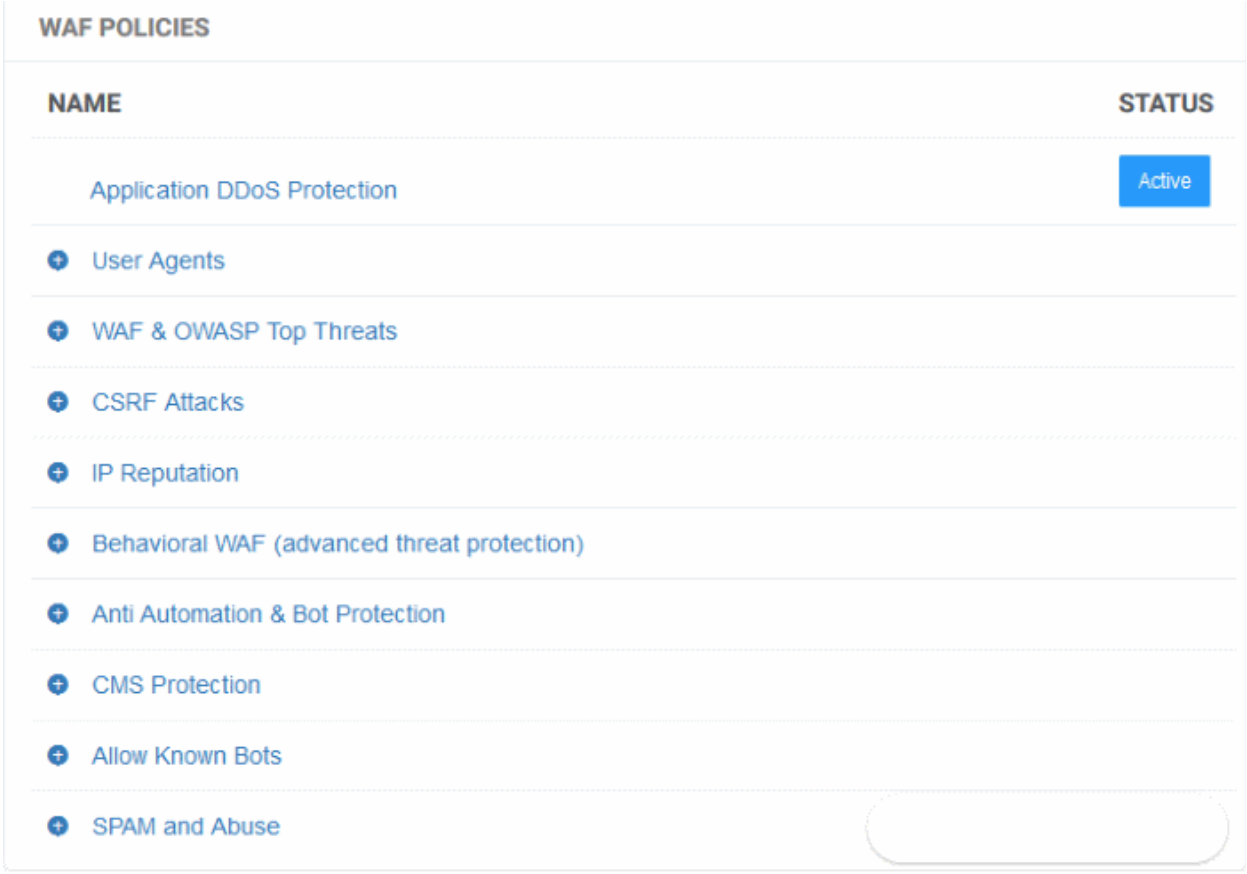


Note - If you disable WAF protection then all firewall policies and rules are deactivated, including custom rules. See **Manage Custom Firewall Rules** for more on rules.

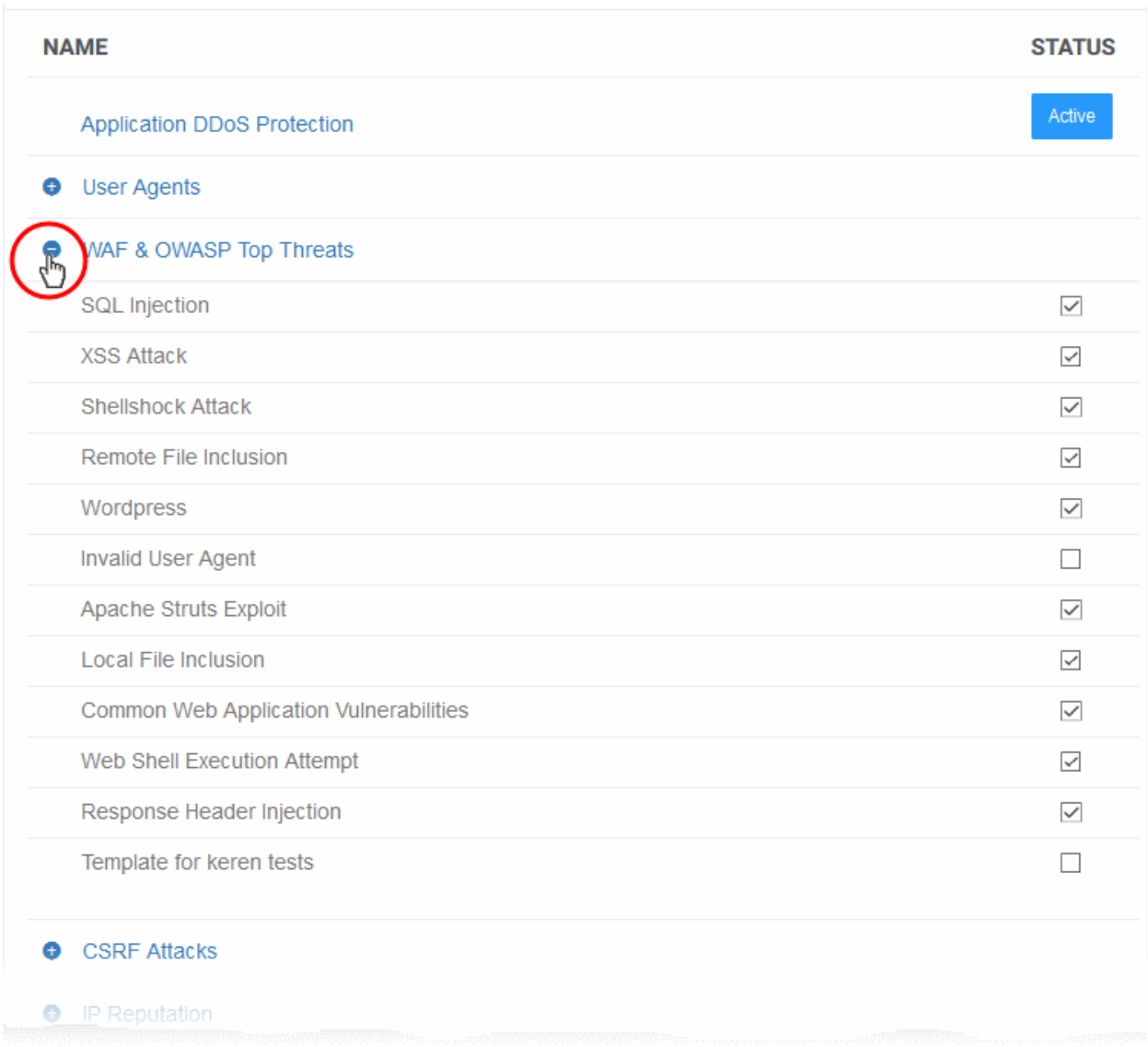
WAF Policies

- This area shows all firewall policies that have been saved on your account.

- Click the '+' symbol to view the constituent rules in a policy. You can enable / disable rules as required.



- **Status** - Indicates whether the firewall is enabled or not. 'Passive' indicates the firewall is disabled.
- Click the '+' symbol to view a policy's constituent rules:



- Use the check-boxes to enable or disable a particular rule.
- Changes are auto-saved and deployed to the site in approximately a minute.

4.4.4 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 or allow specific types of traffic.
- You can create custom rules for individual 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.

Note - The firewall prioritizes rules by action type. It does not use a 'ladder' system whereby rules are prioritized by their position in the list. Priority is as follows:

1. Allow
2. Block

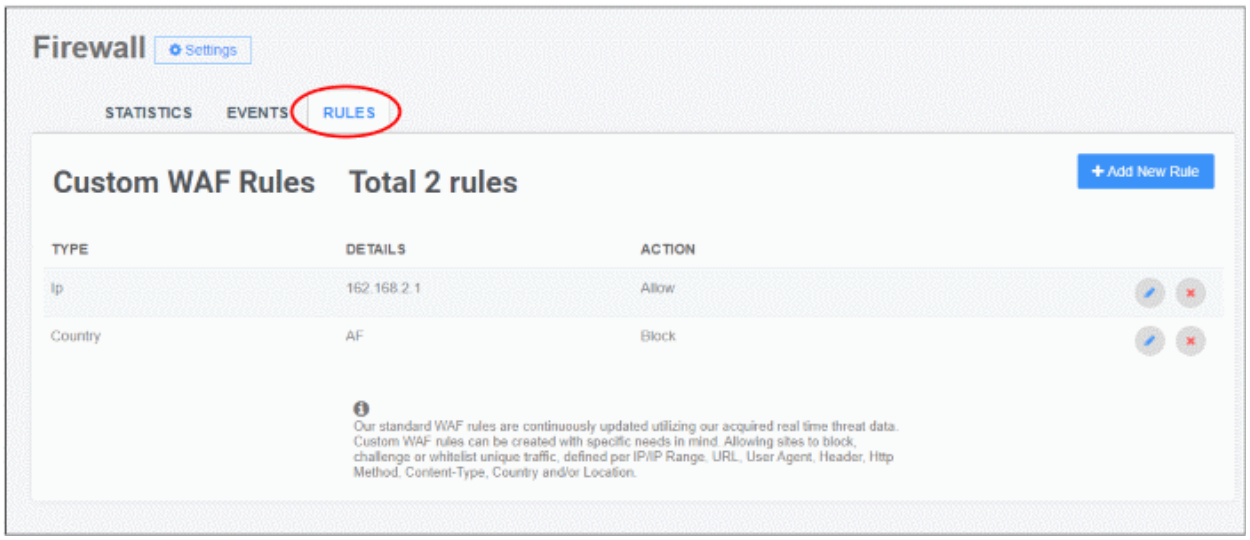
… so in the event of a conflict, 'Allow' rules overrule 'Block' rules.

Please use the following links for more help:

- **Open the rules interface**
- **Add a new firewall rule**
- **Edit a firewall rule**
- **Remove a firewall rule**

Open the rules interface

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



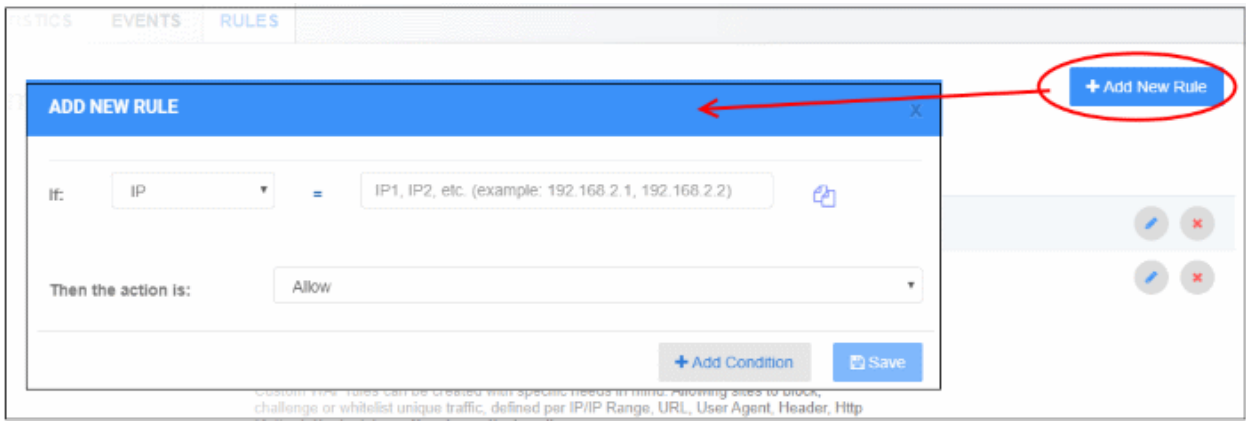
- **Type** - The traffic category targeted by the rule. For example IP, IP range, URL, country
- **Details** – The targeted item in the category. For example, if the type is 'Country', this column shows the two letter country code of the target country.
- **Action** - The process the firewall will execute on the target if the rule's conditions are met. Possible values are 'allow' or 'block'.

Please use the following links to find out more:

- **Add a new firewall rule**
- **Edit a rule**
- **Remove a rule**

Add a new firewall rule

- Select the target website from the menu at top-left
- Click 'Firewall' then the 'Rules' tab
- Click 'Add New Rule' at top-right



'IF' condition - 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 to which you want the rule to apply.
  - The rule will apply to traffic from all domain names which partially match the value entered here.
  - Select 'Exact Match' to apply the rule to only the domain you specify.
- **Header** - The HTTP header field.
- **HTTP Method** - Options are: Post, Get, Head, Put, Delete, Patch and Options.
- **Country** - Select a country from the drop-down

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 traffic requests for the target should be dealt with. The available options are:

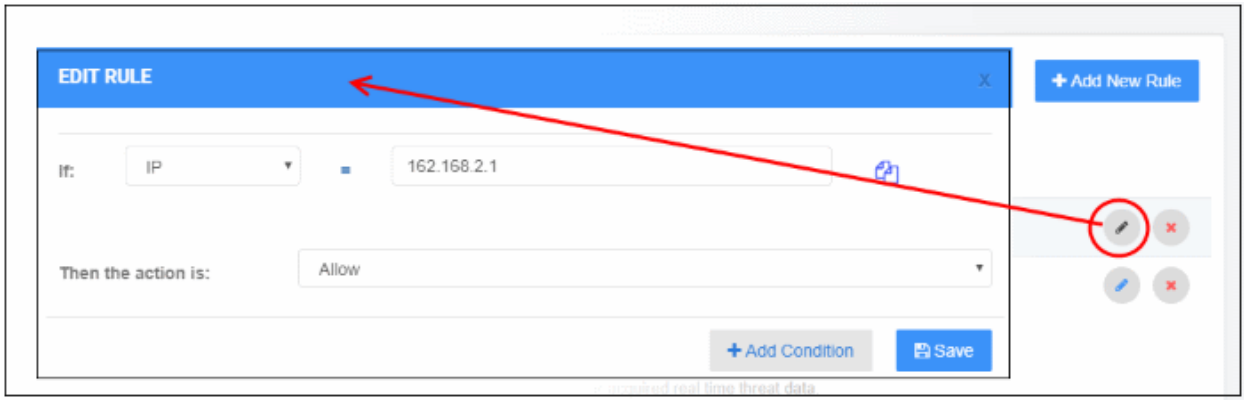
- **Allow** - All traffic from the source is permitted. This includes legitimate traffic, bots etc.
- **Block** - No traffic is allowed from the selected source. An error message is shown to users.

- Click 'Save' to add the new rule.

Edit a firewall 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

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 removed

- Click 'Delete Rule' to confirm

4.5 SSL Configuration

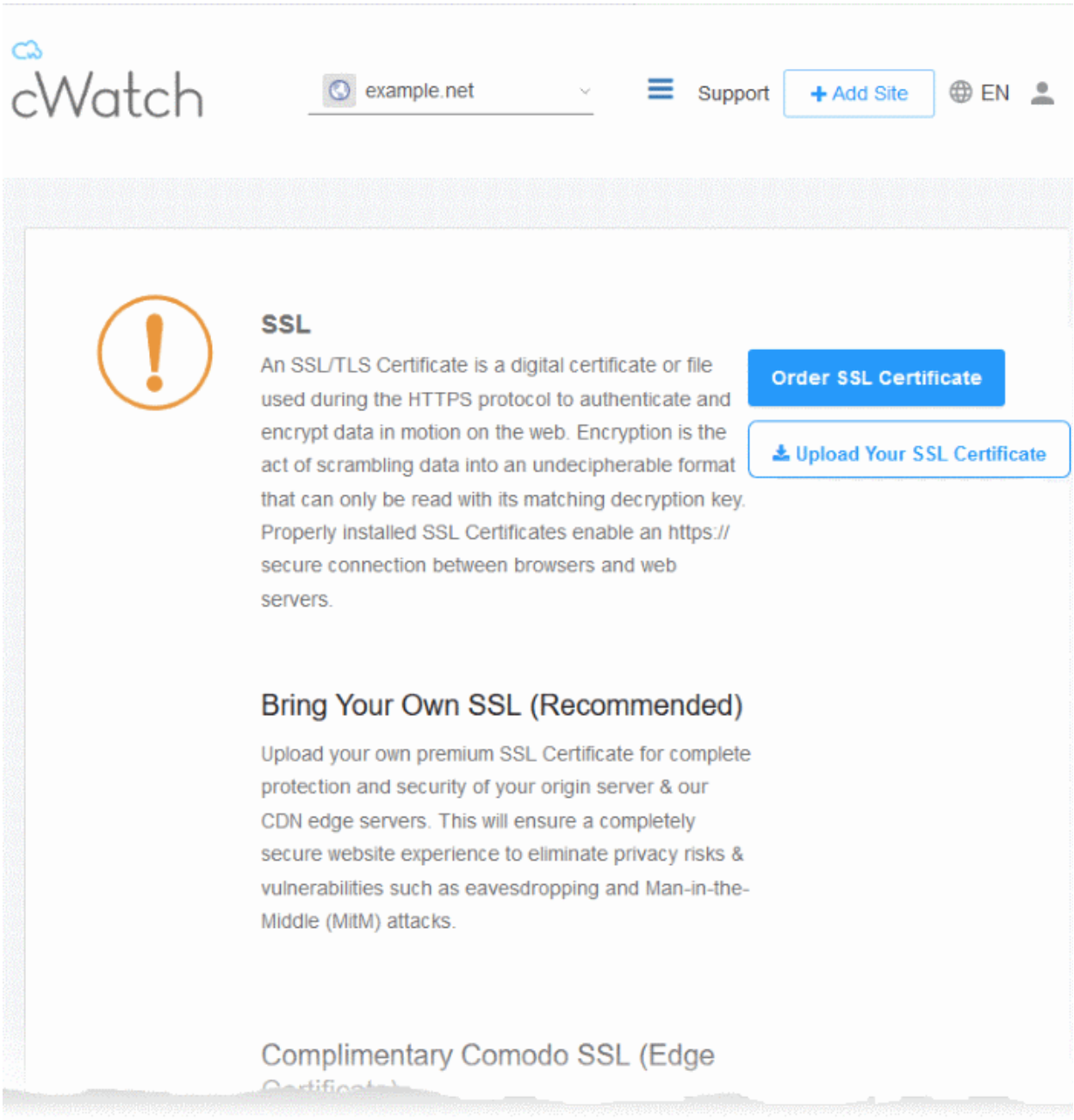
- Select a website from the drop-down at top-left and choose 'SSL'
  - SSL/TLS certificates identify a website's owner, and encrypt all data that passes between the site and a visitor's browser.
  - Sites that use an SSL/TLS certificate have a URL that begins with HTTPS. For example, https://www.example.com.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

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

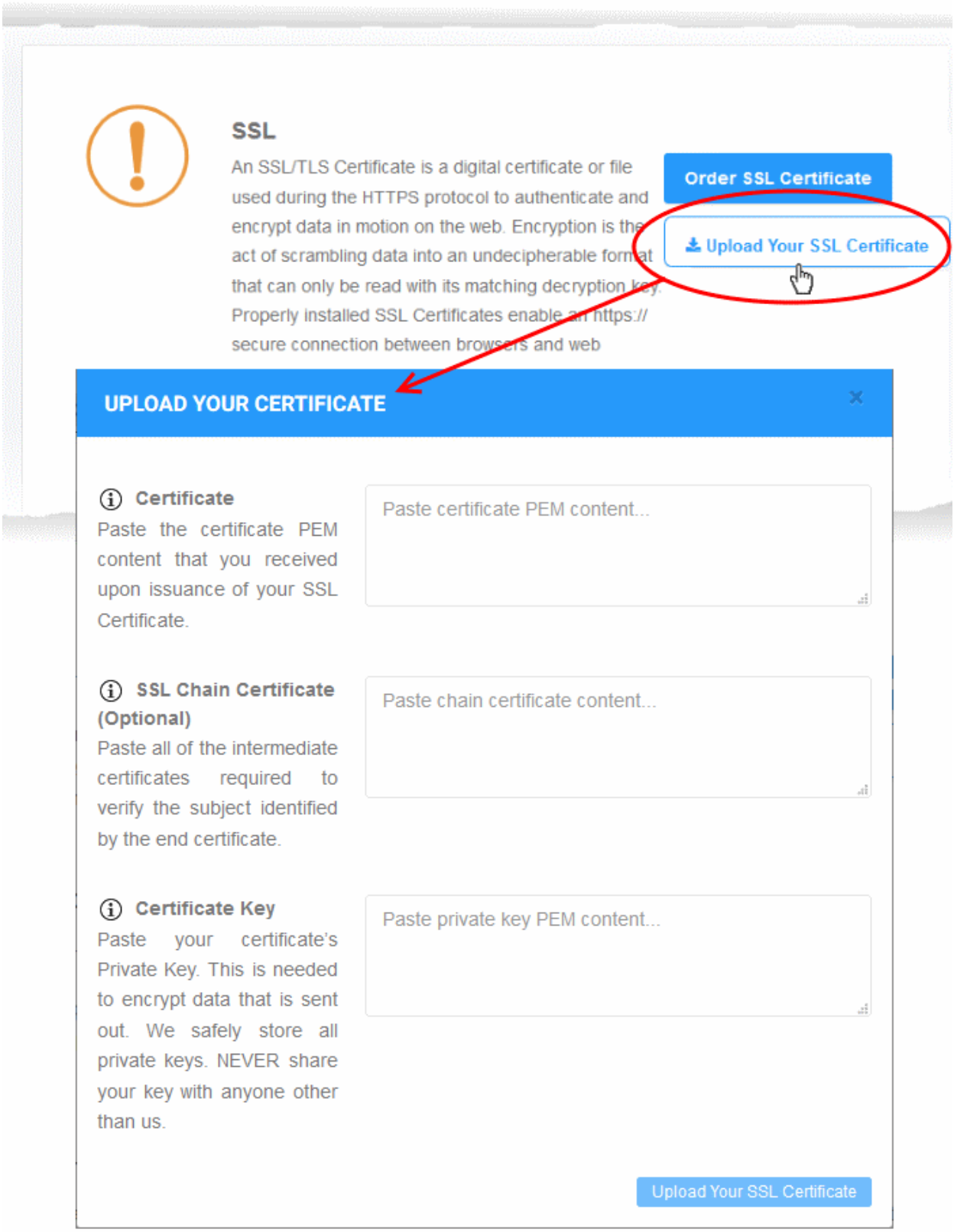
- **Bring your own SSL**
  - Upload your site's existing certificate to the cWatch CDN edge servers. Recommended for most customers.
  - This will secure the traffic between your site (the origin server) and the cWatch CDN.
  - See **Upload your own SSL Certificate** to find out how to deploy your certificate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

Upload your own SSL Certificate

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



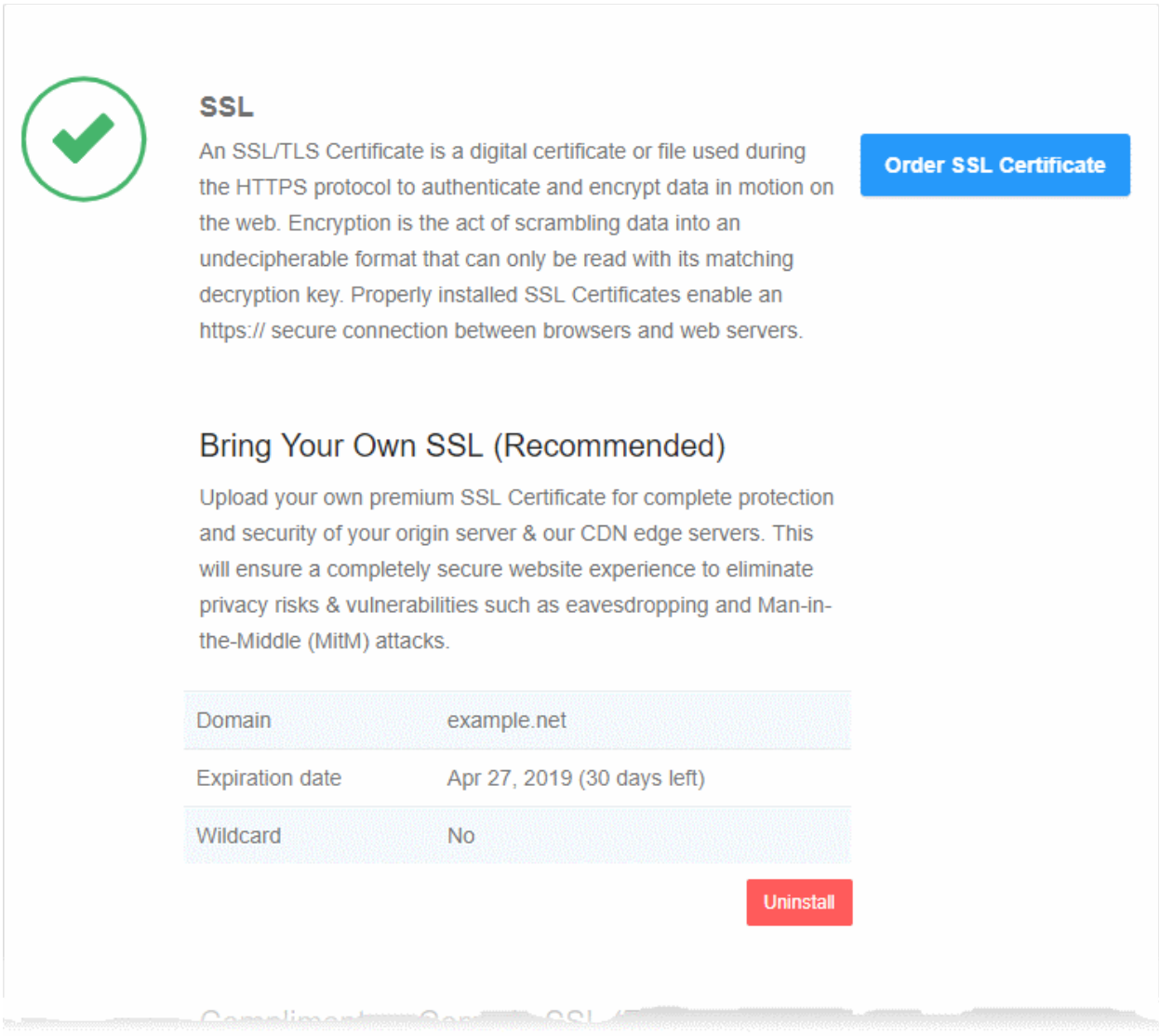
- Click 'Order SSL Certificate' if you do not already have a certificate on your site
  - You will be taken to SSL purchase page to buy a new certificate
  - You can install the certificate on your web-server then upload it to cWatch.
- Click 'Upload Your SSL Certificate' to submit your existing certificate:


SSL
An SSL/TLS Certificate is a digital certificate or file used during the HTTPS protocol to authenticate and encrypt data in motion on the web. Encryption is the act of scrambling data into an undecipherable format that can only be read with its matching decryption key. Properly installed SSL Certificates enable an https:// secure connection between browsers and web
Order SSL Certificate
Upload Your SSL Certificate
UPLOAD YOUR CERTIFICATE
Certificate
Paste the certificate PEM content that you received upon issuance of your SSL Certificate.
Paste certificate PEM content...
SSL Chain Certificate (Optional)
Paste all of the intermediate certificates required to verify the subject identified by the end certificate.
Paste chain certificate content...
Certificate Key
Paste your certificate's Private Key. This is needed to encrypt data that is sent out. We safely store all private keys. NEVER share your key with anyone other than us.
Paste private key PEM content...
Upload Your SSL Certificate

Upload Your Certificate - Form Parameters	
Parameter	**Description**
Certificate	Paste the content of your certificate. The content you are looking for is something like this: -----BEGIN CERTIFICATE----- MIICUTCCAfugAwIBAgIBADANBgkqhkiG9w0BAQQFADBXMQswCQYDVQQGE 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'

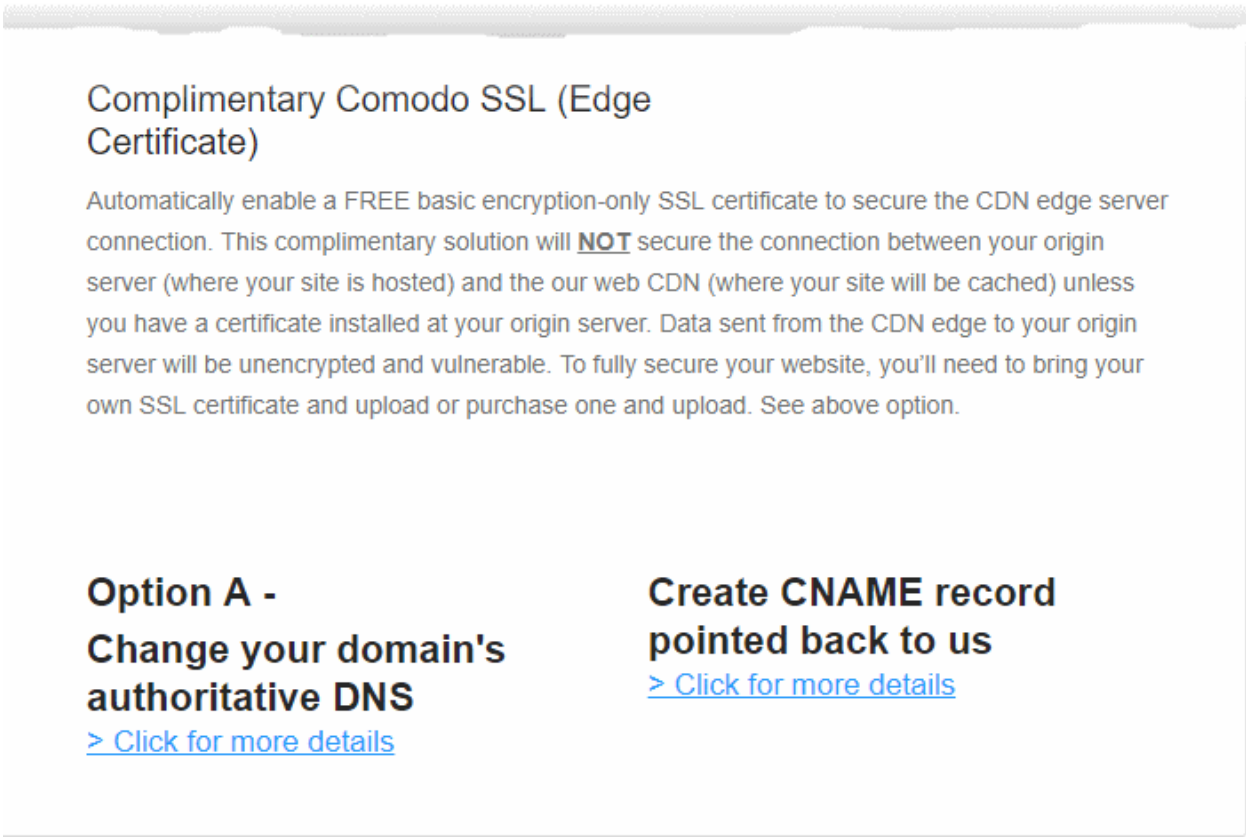
The SSL certificate will be uploaded to the CDN edge servers.



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
- 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

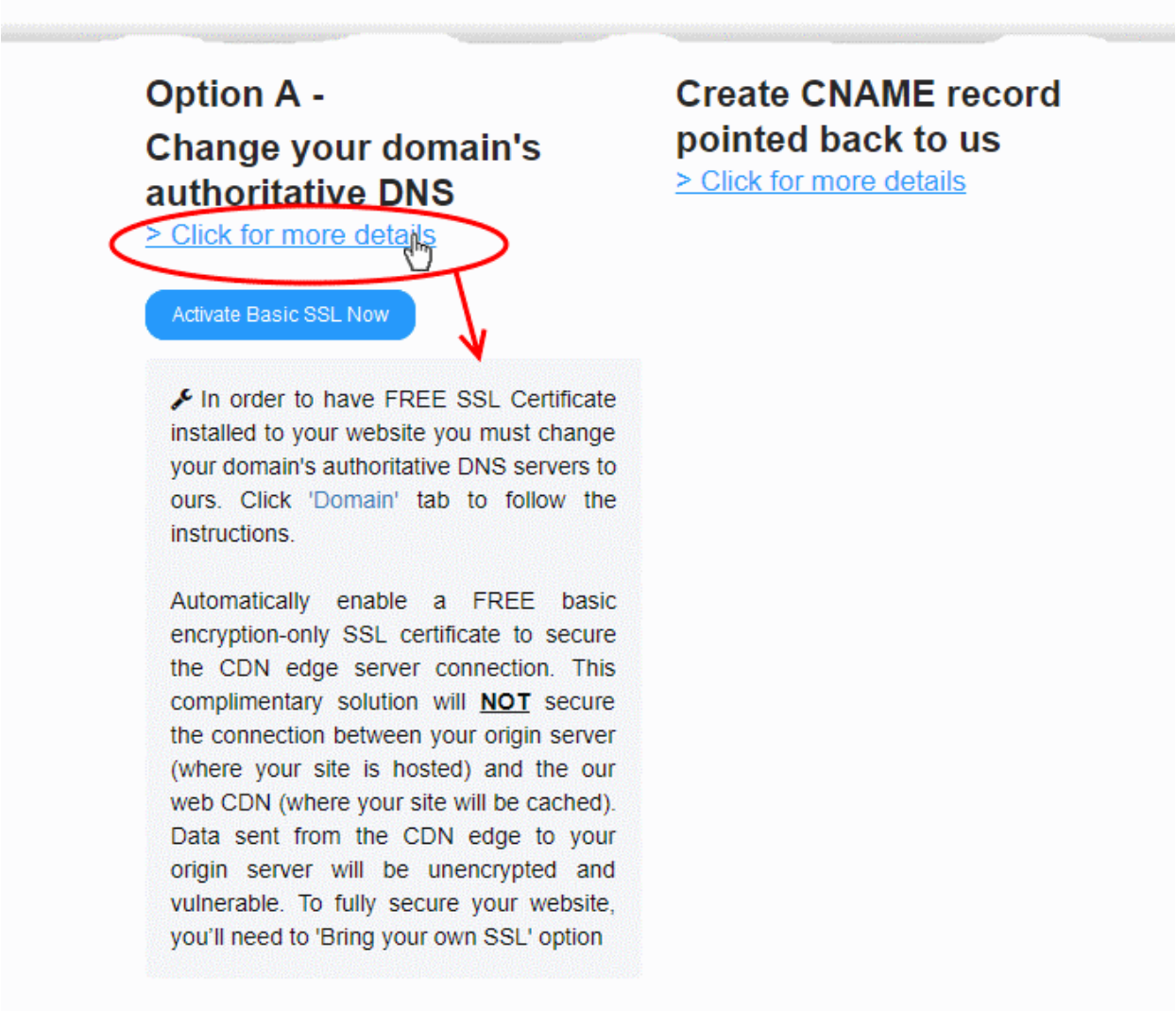
Option A - Change your domain's authoritative DNS servers to Comodo

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

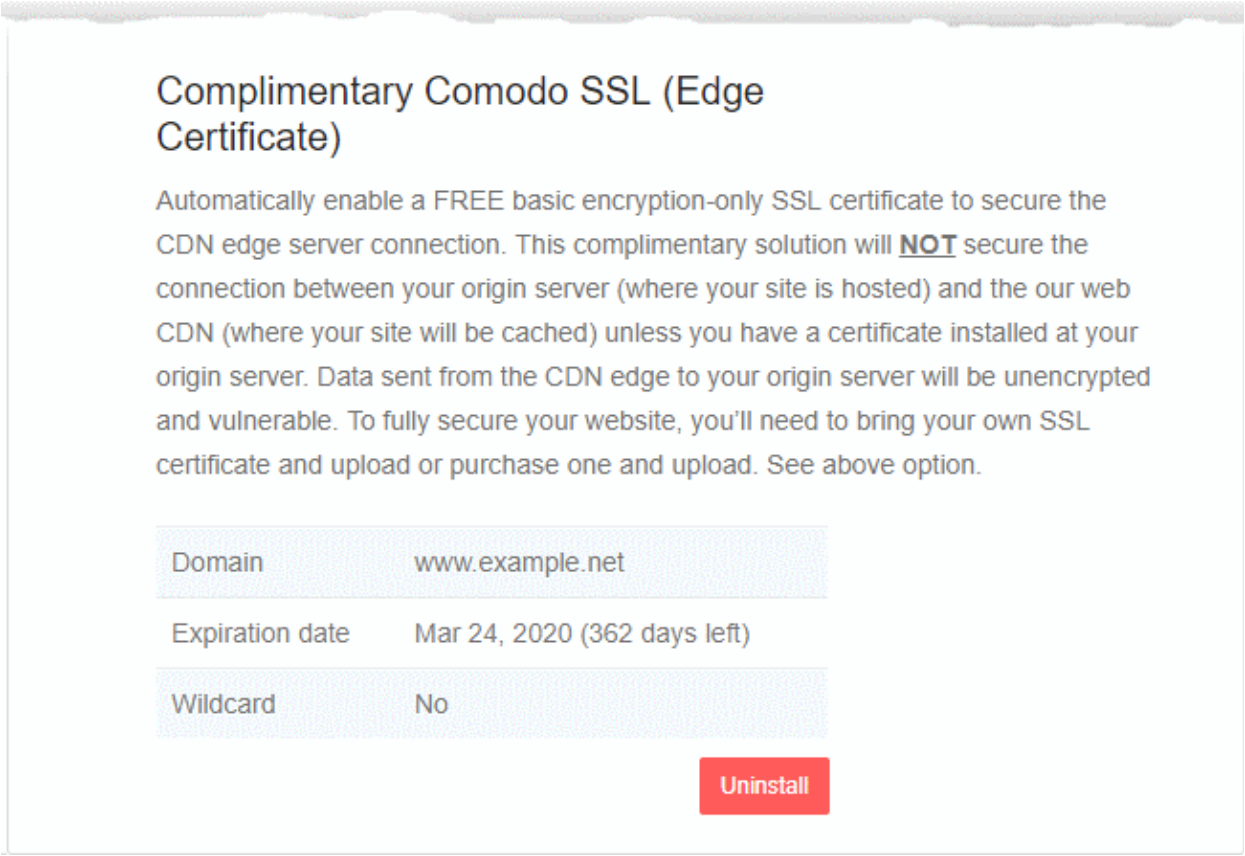
- The NS records are available in 'CDN' > 'Settings' > 'Activation', and in the 'DNS' pages of the site.

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'



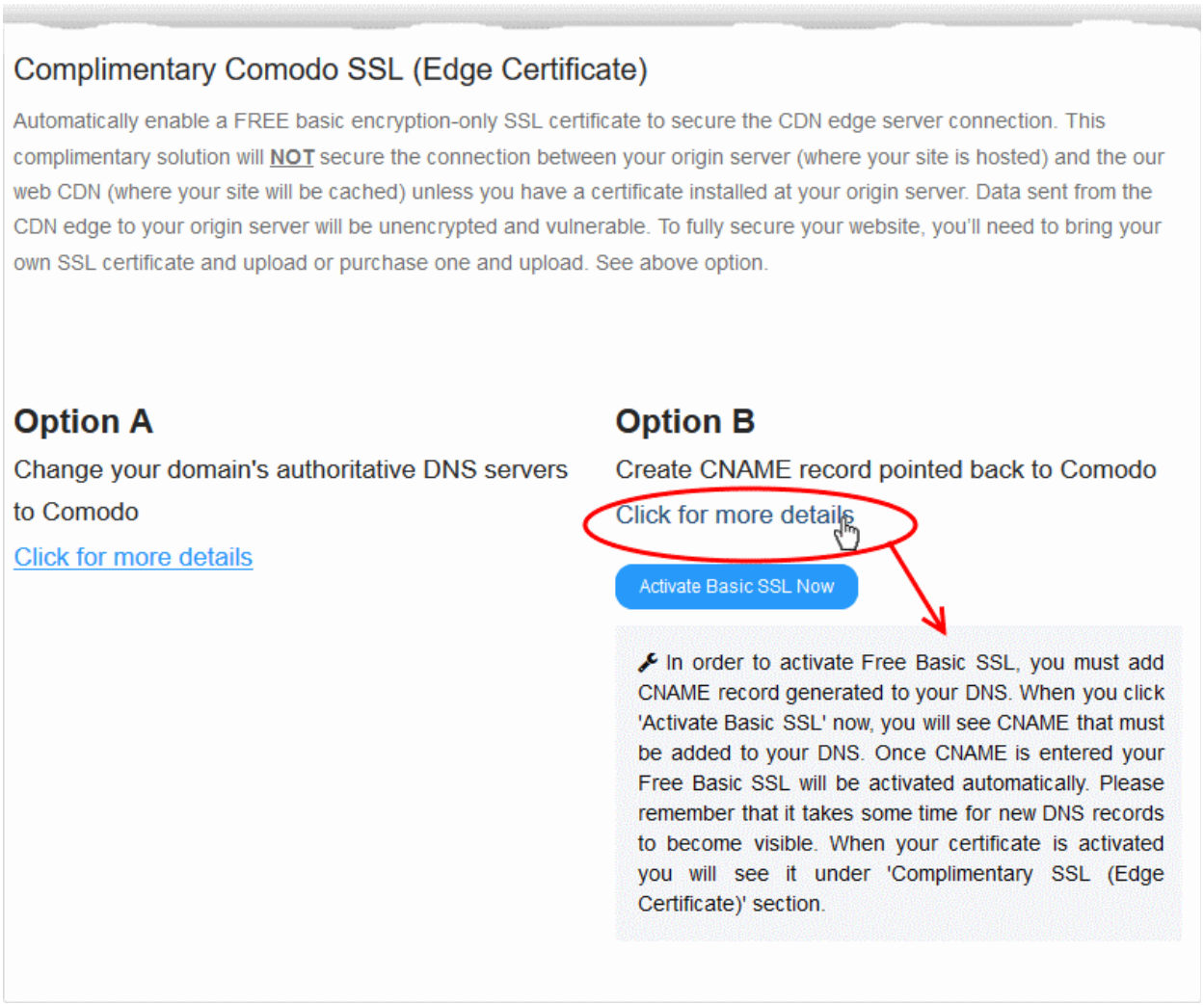
- Click the 'Activate Basic SSL Now' button
- The process will take a few minutes to complete.
- Once activated, you can see the certificate in 'Settings' > 'SSL', listed under 'Complimentary Comodo SSL (Edge Certificate)'.



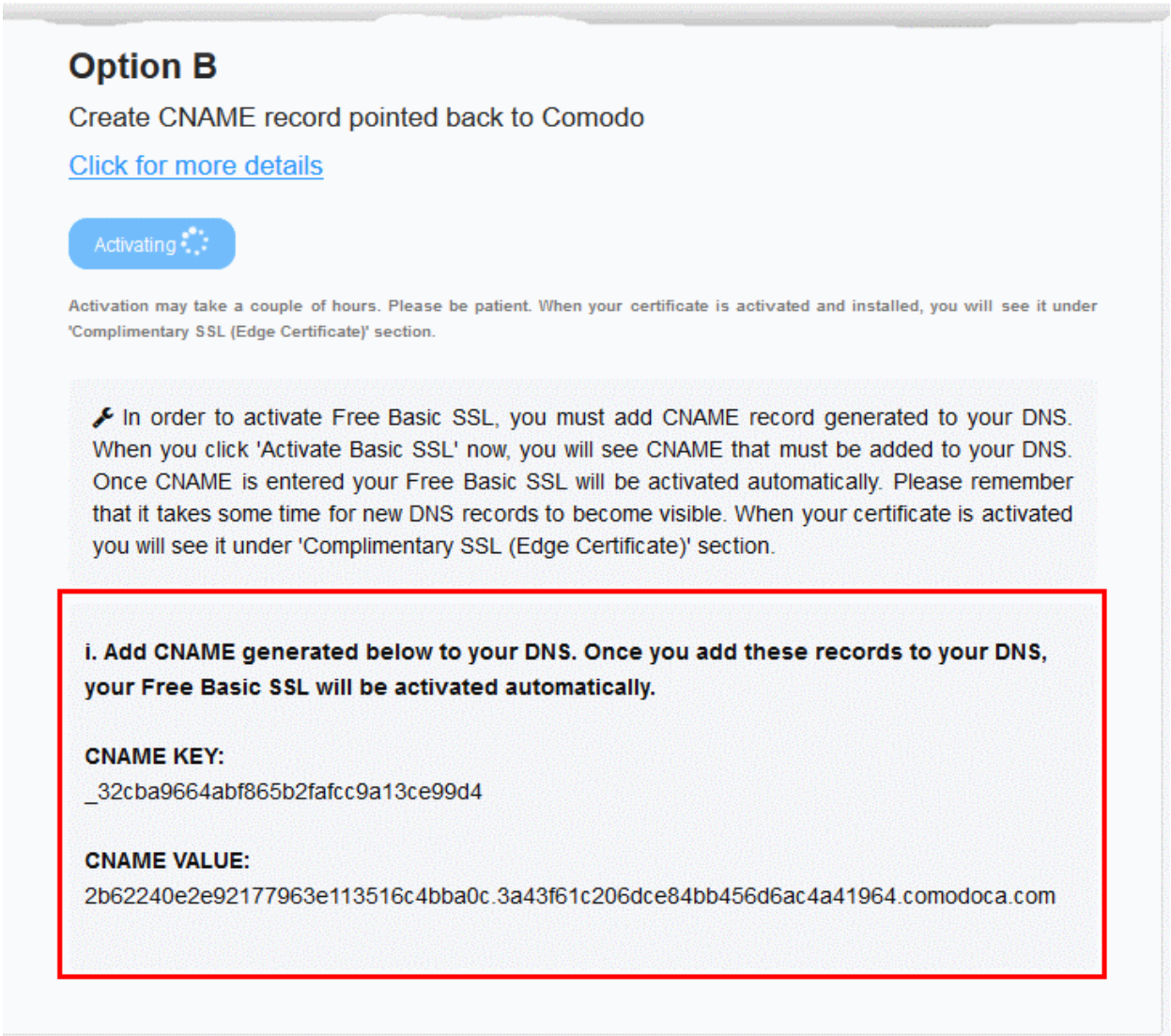
- The certificate is valid for one year and is set for auto-renewal.
- Note - This certificate encrypts the connection between the CDN servers, which host a copy of your site, and your website visitors.
- It does not encrypt the traffic between your web-server and the CDN edge servers.
- You need to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



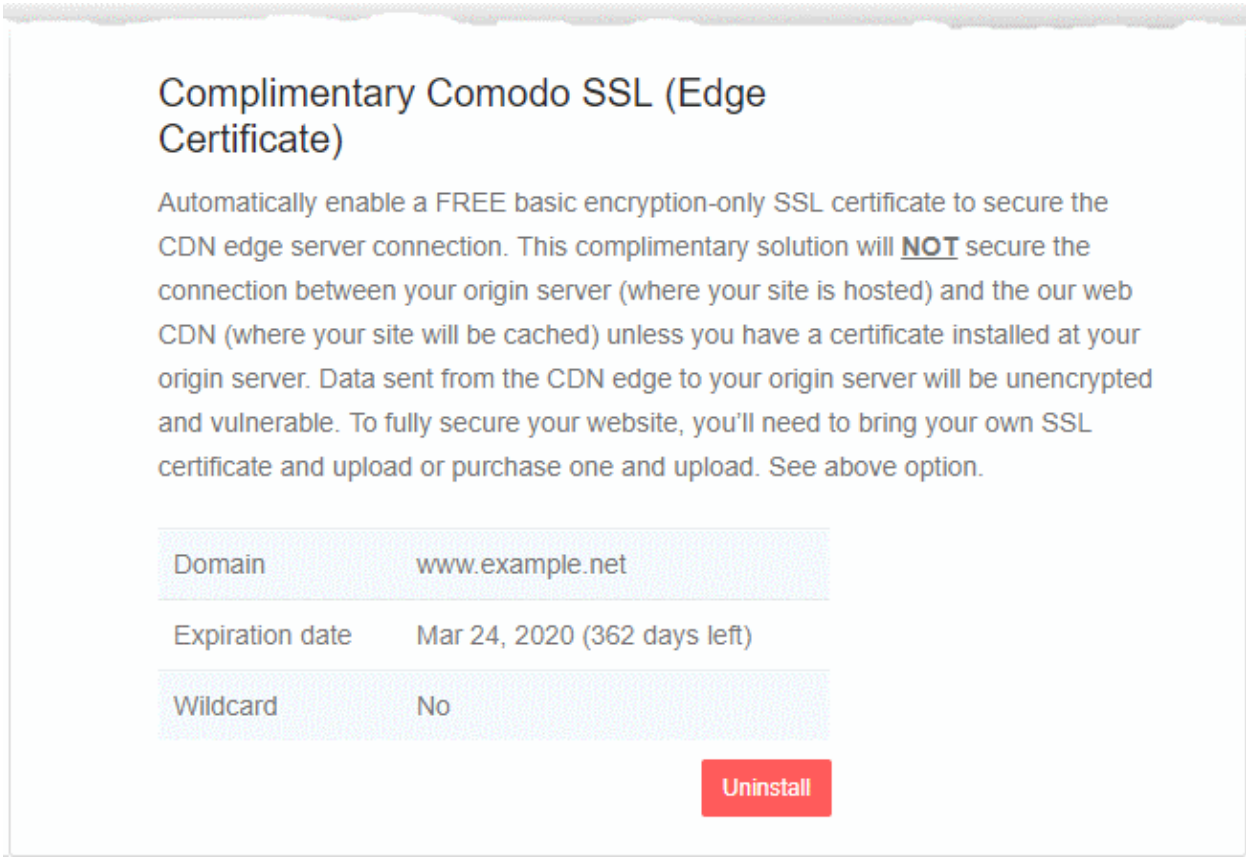
- Click the 'Activate Basic SSL Now' button:



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.

4.6 DNS Configuration

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

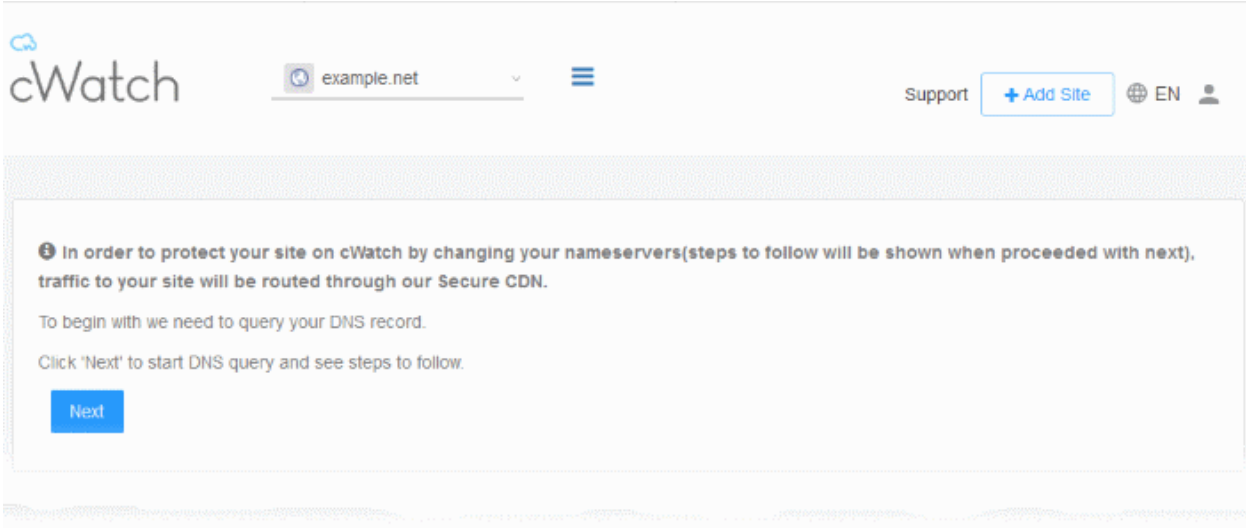
The following sections explain how to:

- **Configure DNS settings for your site**
- **Manage DNS Records for your site**

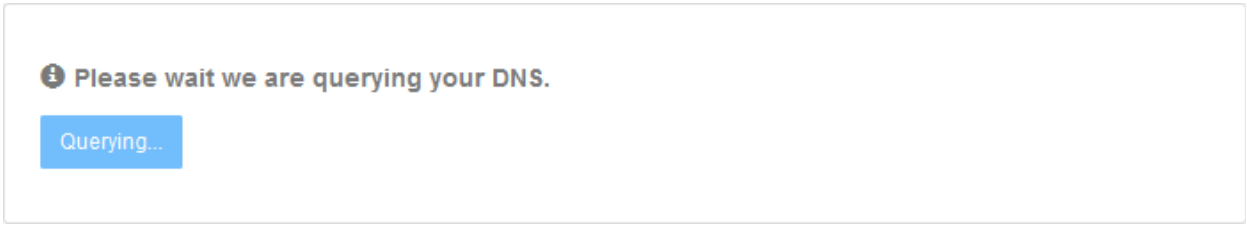
Configure DNS settings for your site

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

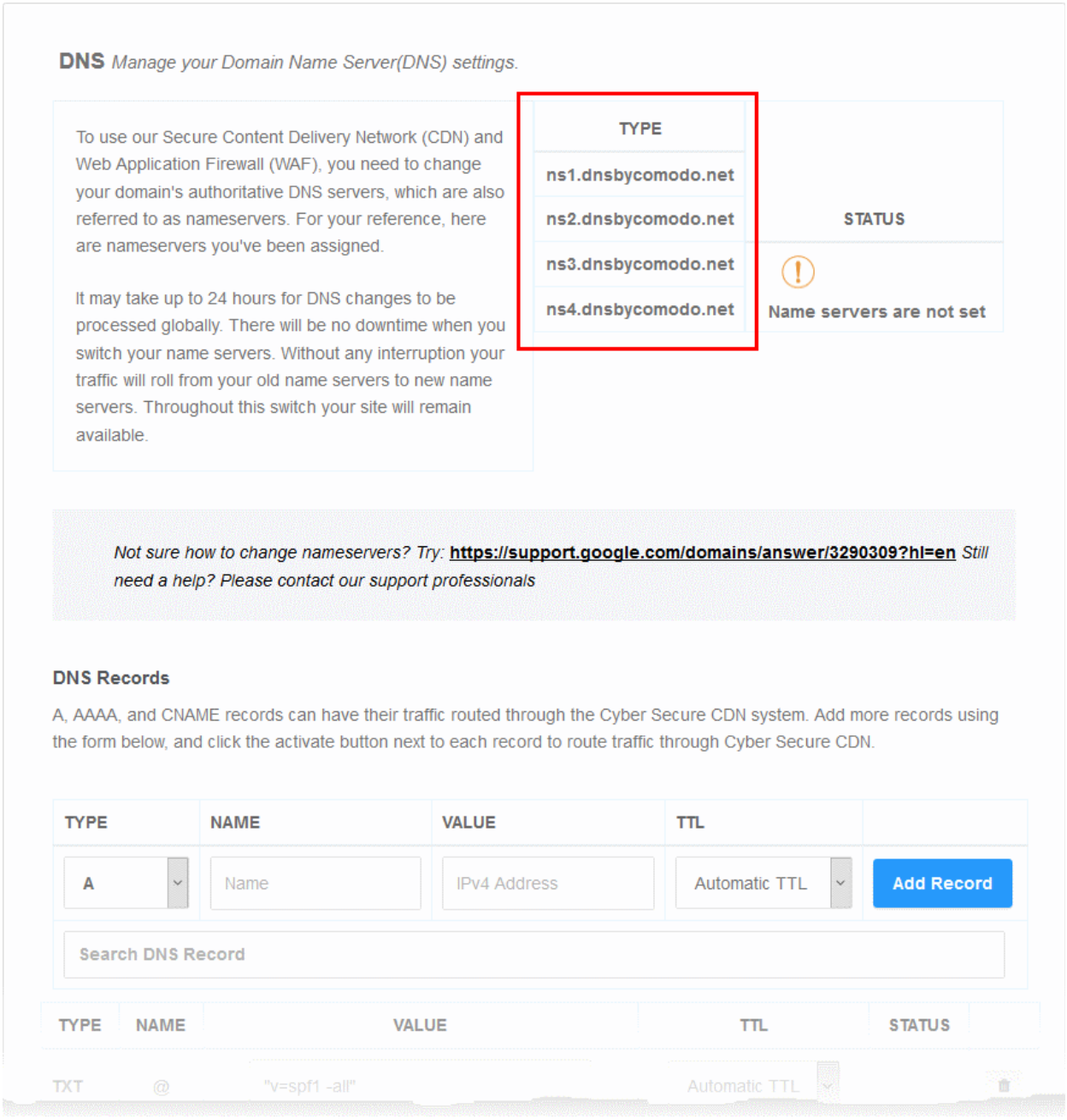
cWatch first queries your DNS servers to collect your existing records:



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



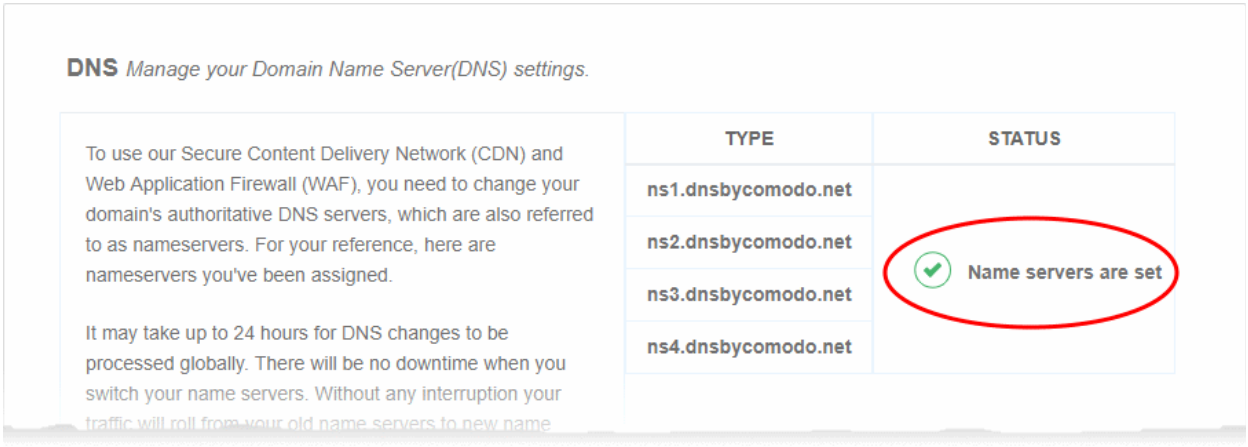
The DNS configuration page for the site will then load, complete with the site's name server (NS) details:



- 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
- 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 for your site

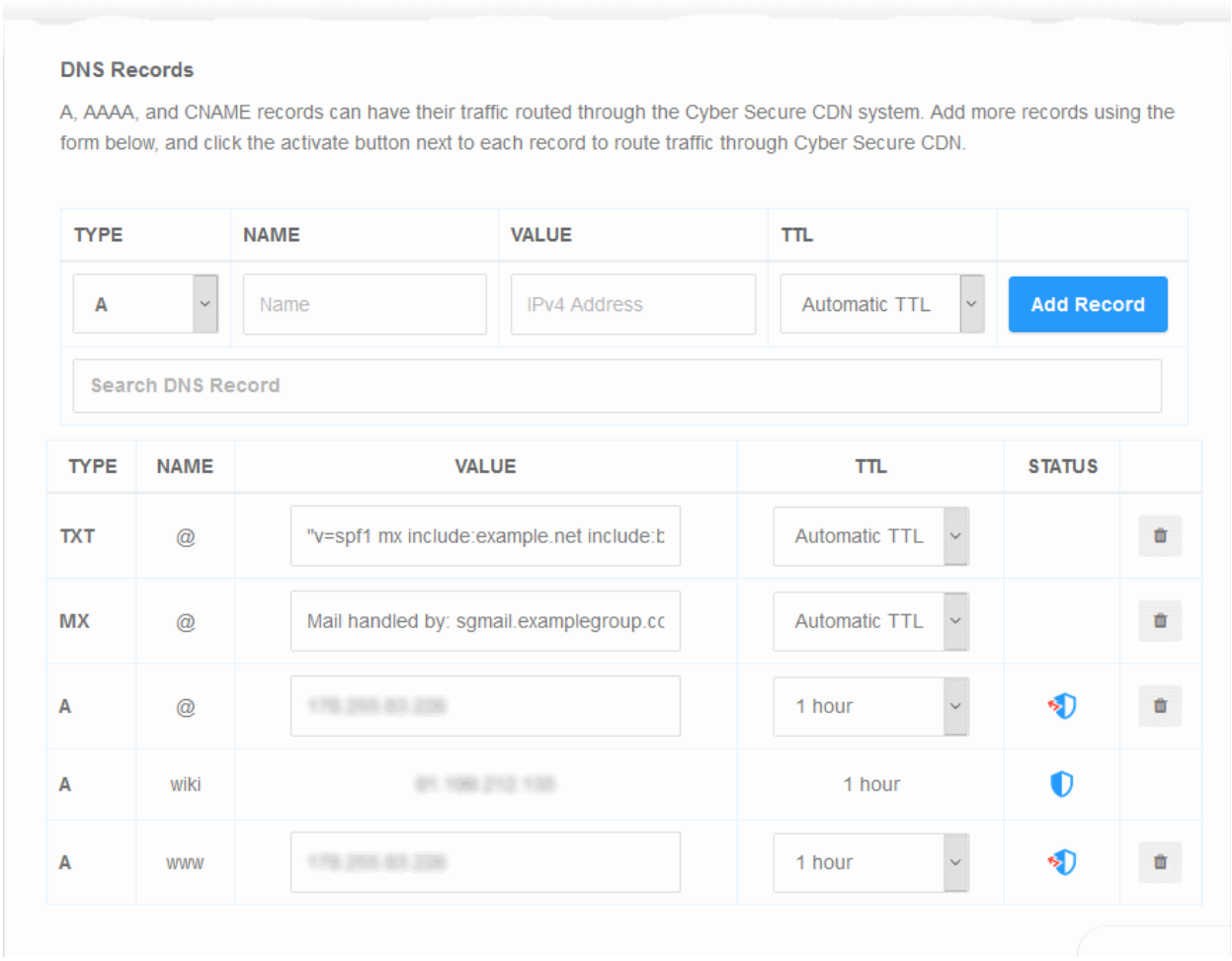
Note - you can only manage DNS records in cWatch if your nameservers are pointed to Comodo.

- 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
- 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

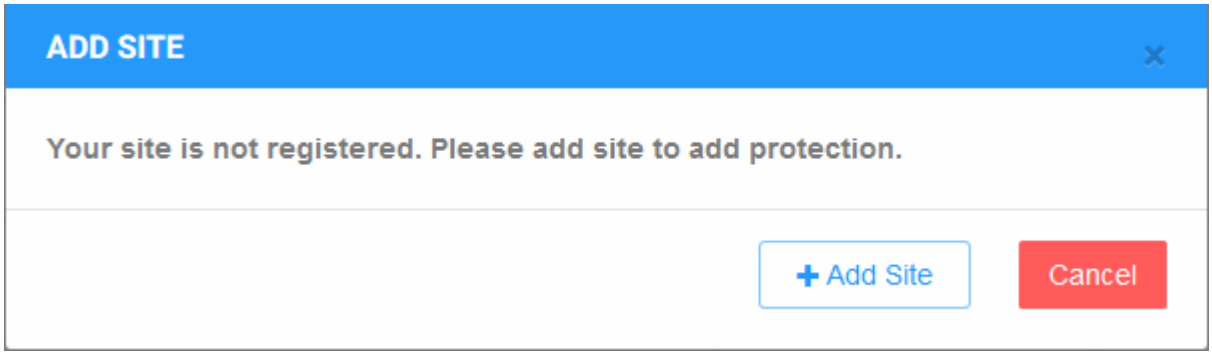
- Open the cWatch dashboard
- Select the target website from the menu at top-left
- Click the 'DNS' tab
- Scroll down to the 'DNS Records' pane
- Configure the following items:
  - Type - Select the kind of the DNS record from the drop-down
  - Name - Enter an appropriate label for the record
  - Value - 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.

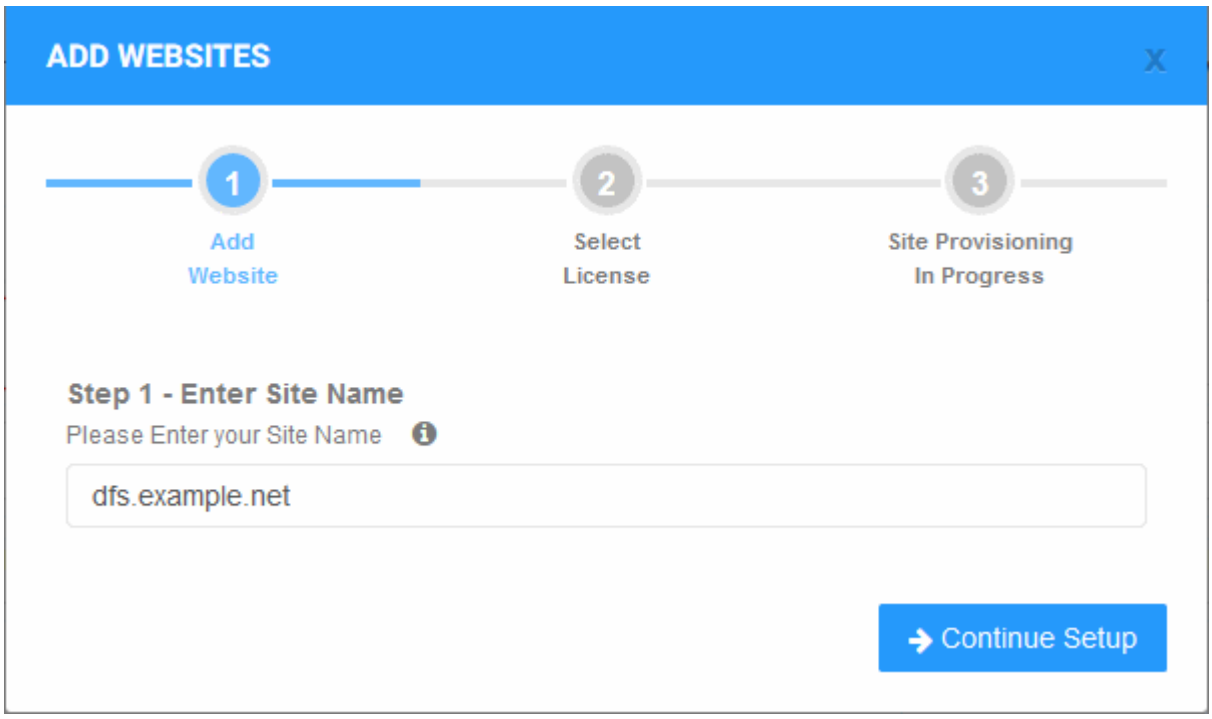
- See **https://support.google.com/domains/answer/3290309?hl=en** if you need more help to change nameservers.

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.

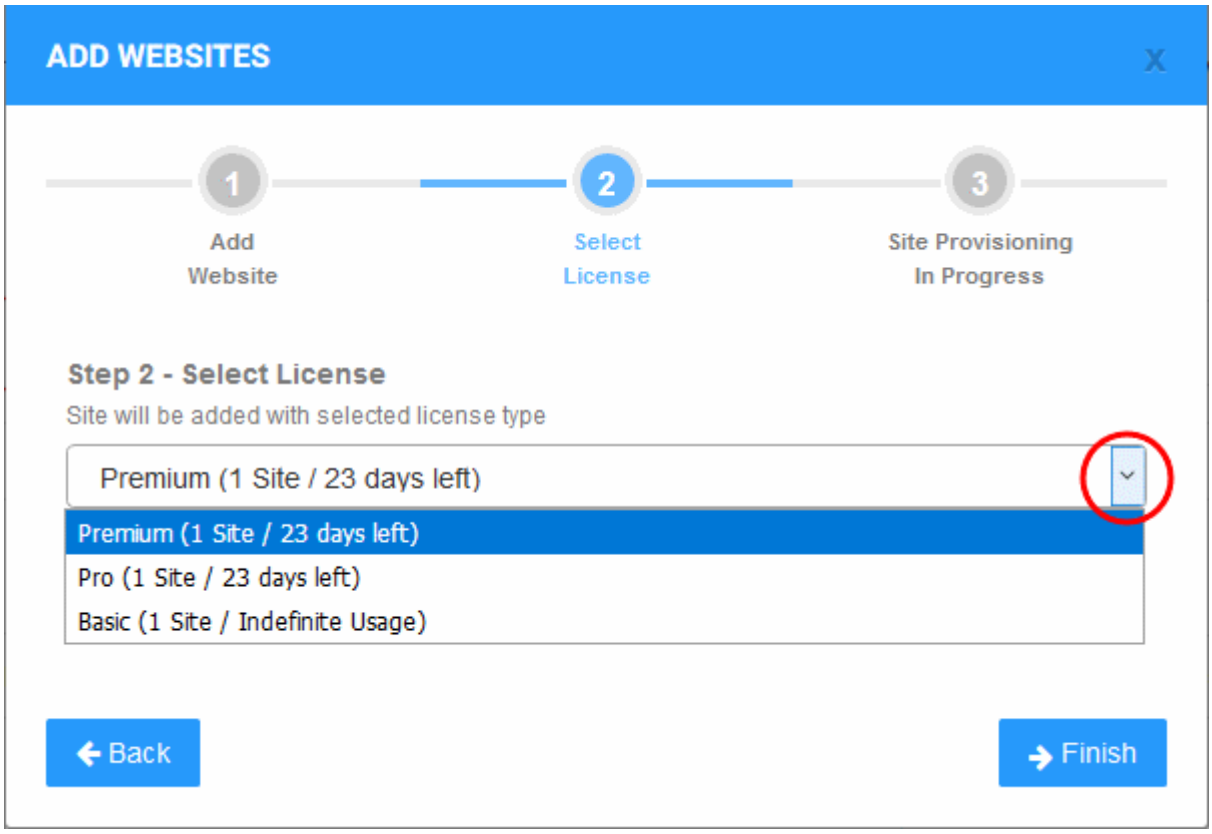


- Click 'Add Site' to start the 'Add Websites' wizard.

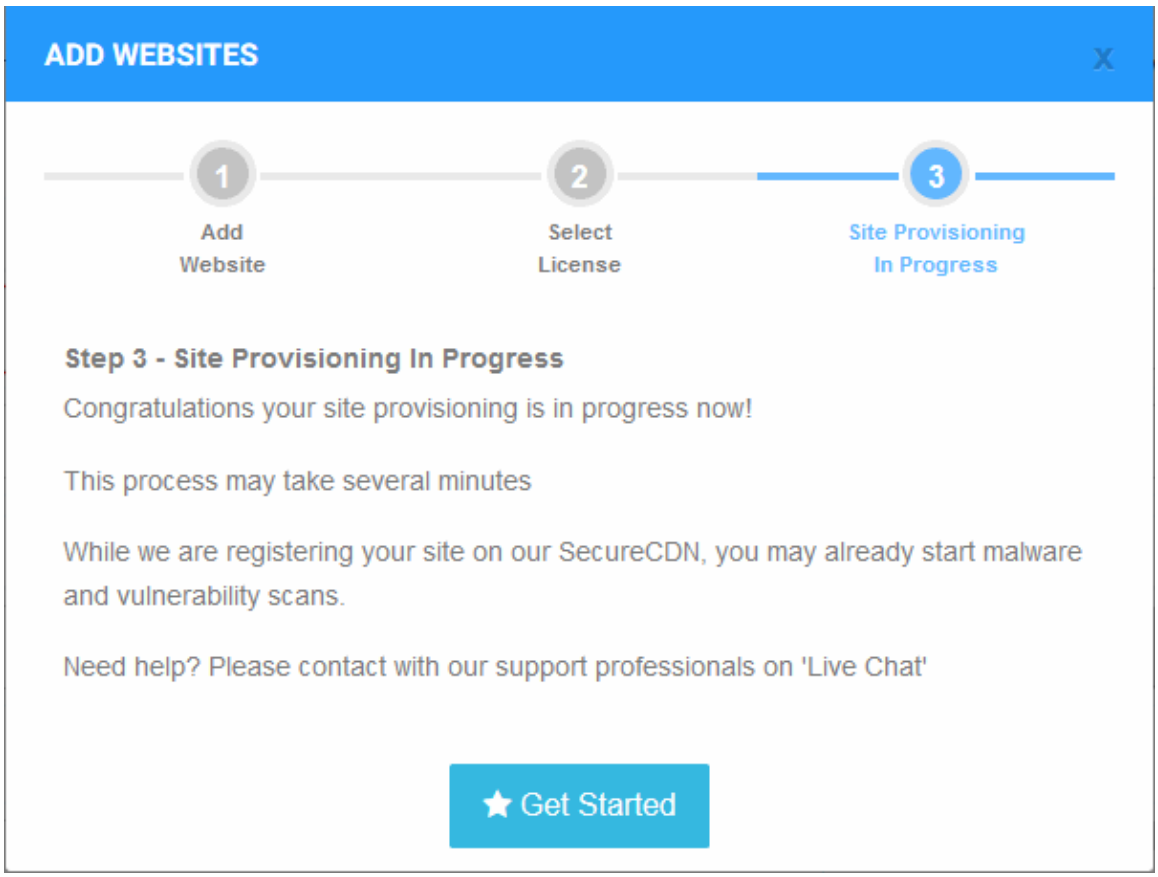


The website name is pre-populated.

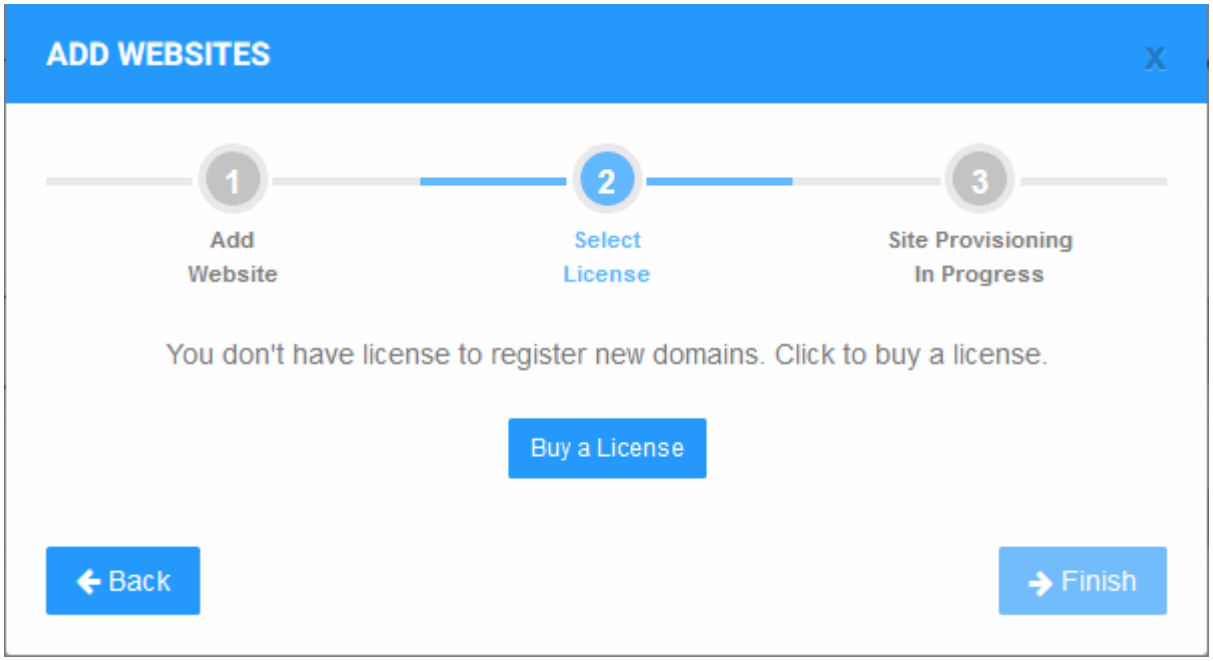
- Click 'Continue Setup' to move to the next step.
- The drop-down menu lists any unused licenses you have on your account. You can apply one of these licenses if available.
- Click 'Buy a license' if you don't have any existing licenses. **Click here** if you need help with the order form.



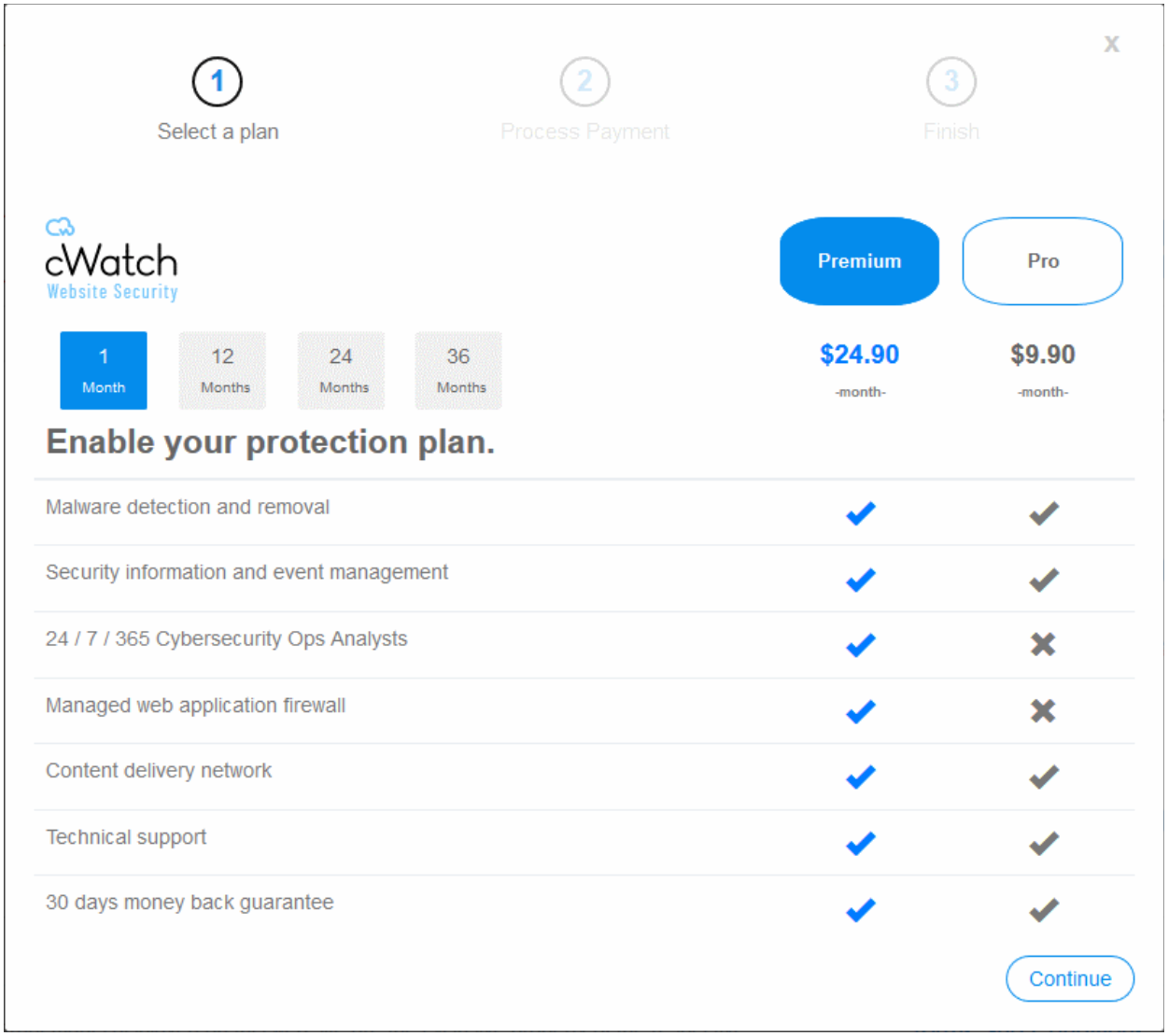
- Click 'Finish' to apply the license. The site will be registered.
- cWatch will validate your request then show the following confirmation message:



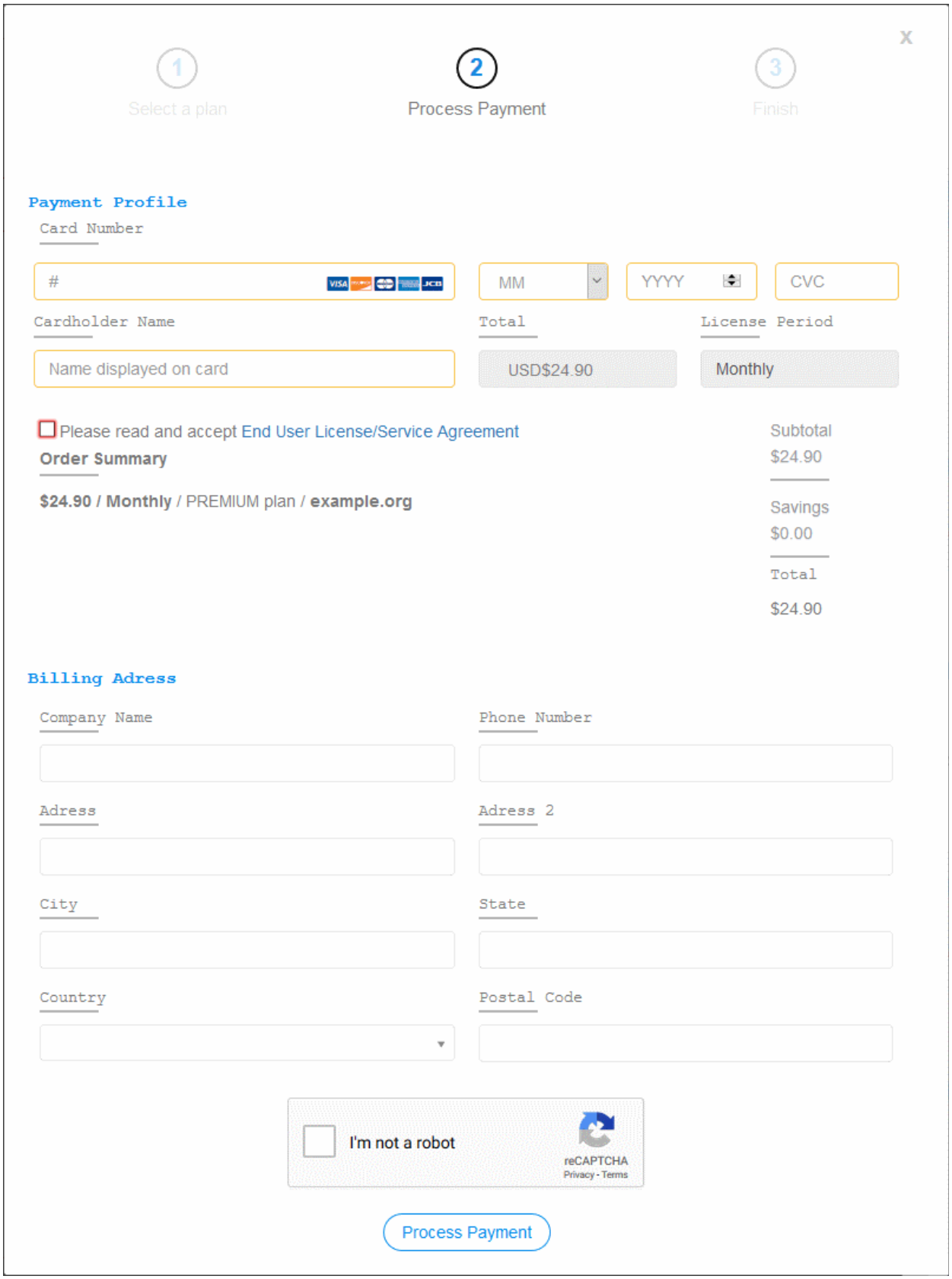
- Click 'Get Started' to activate cWatch protection.
- If you do not have any licenses available then you will be asked to purchase a license:



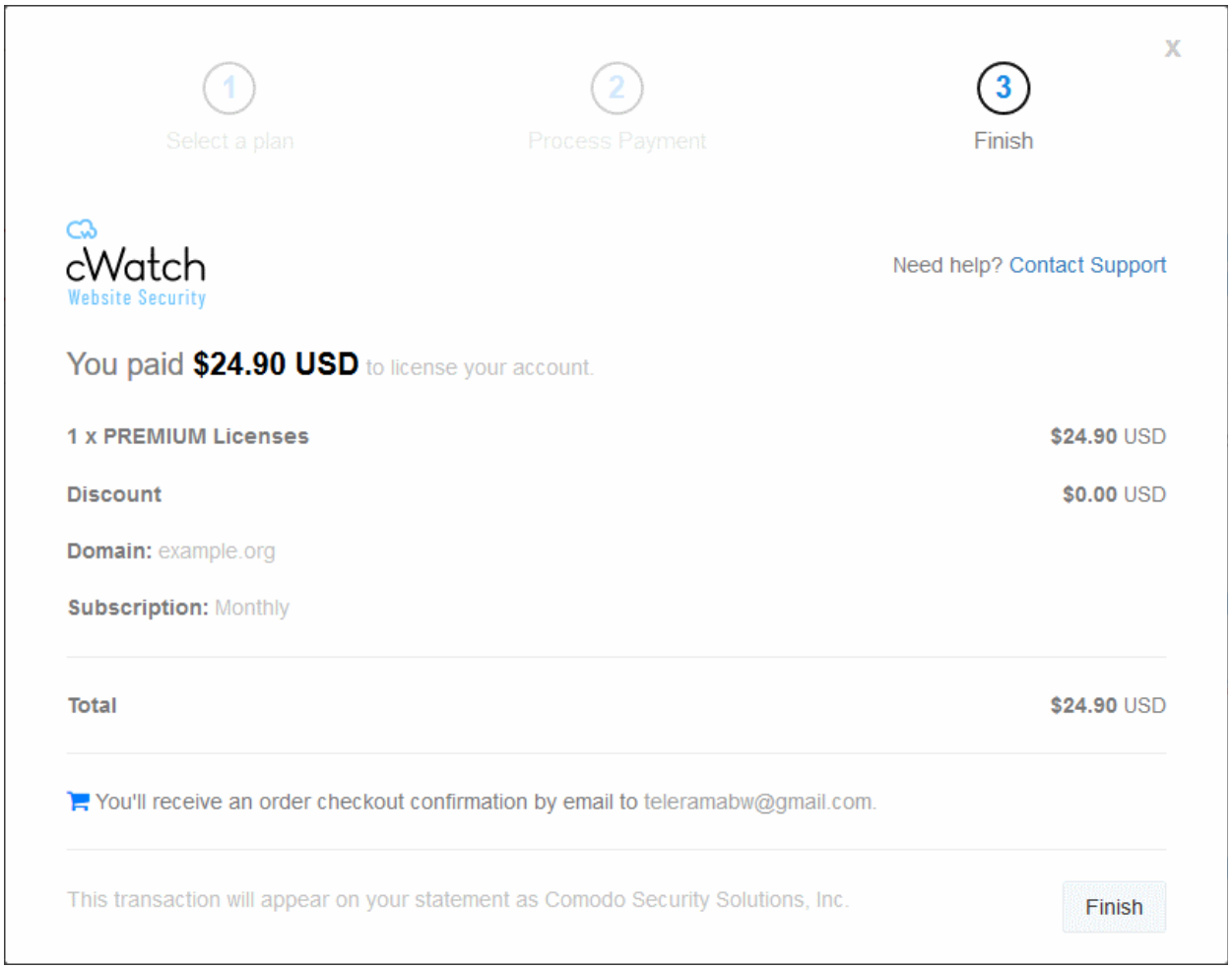
- Click 'Buy a License'.
- You will be taken to the license purchase page:



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



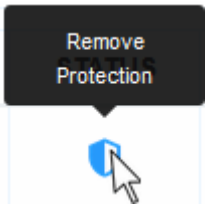
- Complete the payment details section
- Read the 'End User License/Subscriber Agreement' and tick the checkbox to agree
- Enter your billing address
- Complete the captcha verification and click 'Process Payment'



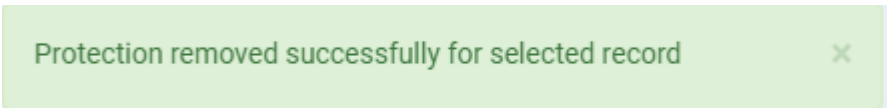
- The new license is added to your account and can be applied to the site in cWatch.
- Restart the process to add protection to the DNS record.

Remove protection from a site

- Click the shield icon beside the record:

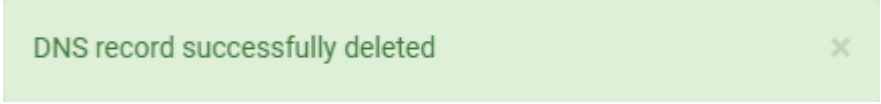


You will see the following confirmation message:



Remove a DNS record

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

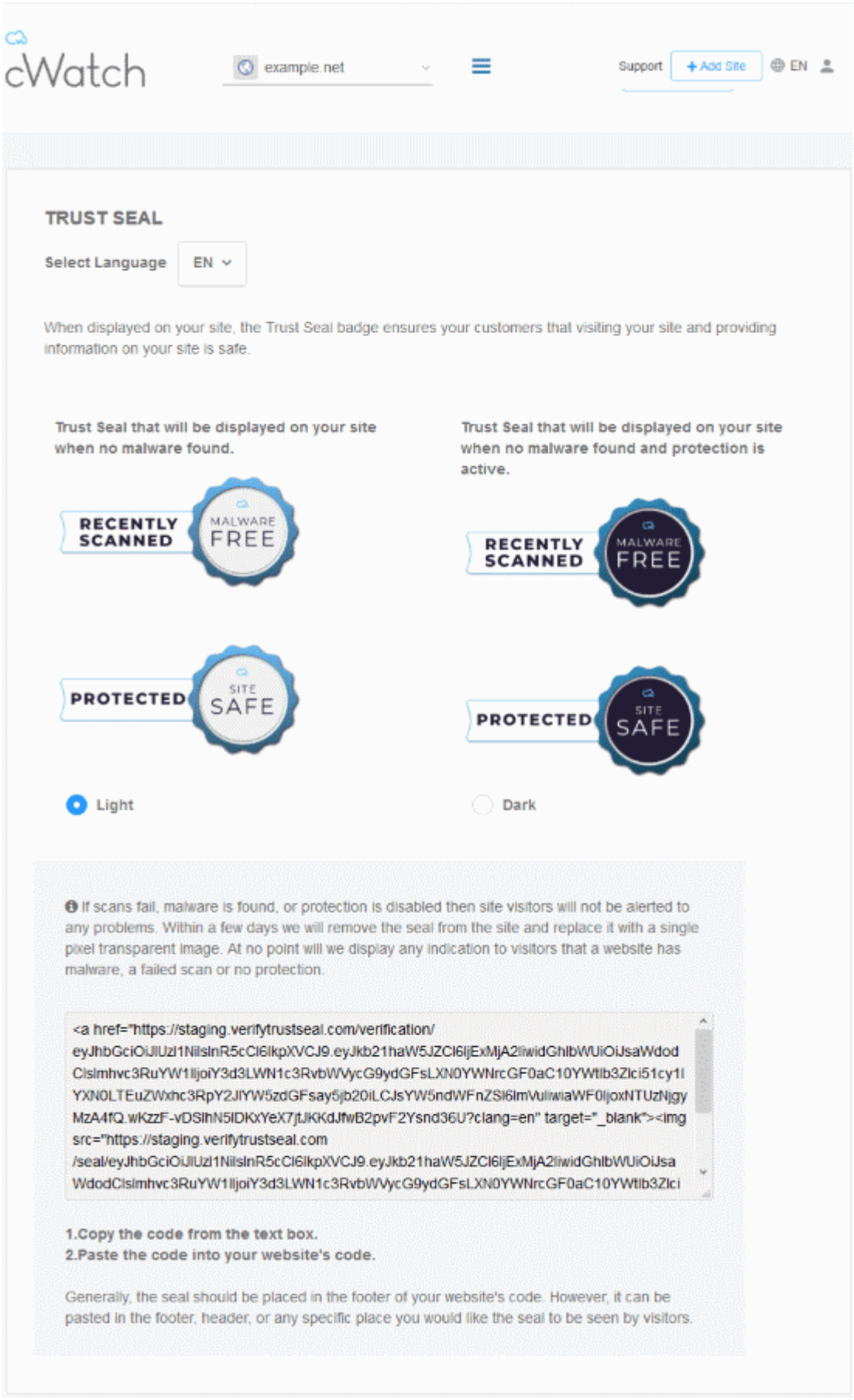


4.7 Add Trust Seal to your Websites

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

Add the trust seal to your website

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



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

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

Here are some sample scenarios:

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

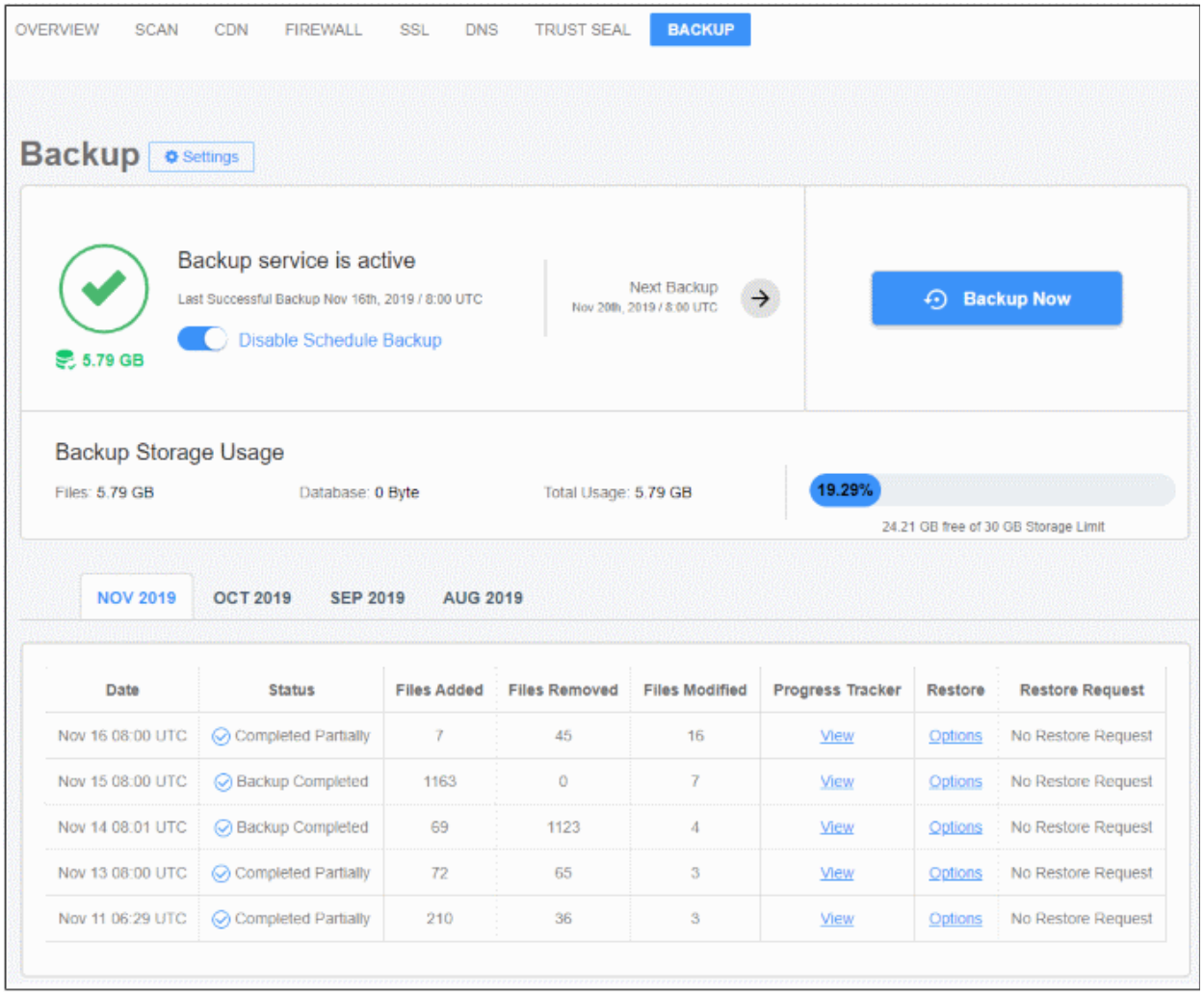
- No negative messaging is shown if your site fails a scan/appears on a blacklist. After a grace period, the seal will simply disappear, replaced by a transparent single-pixel image. The seal will reappear when the issues are fixed.
- Select the language which should be used in the trust seal
- Follow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

4.8 Back up your Website

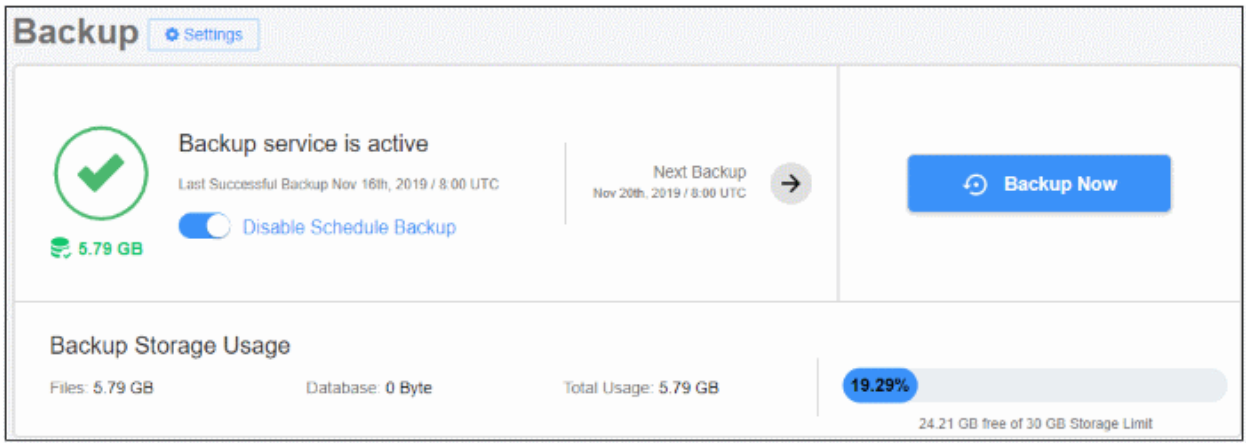
- cWatch backup is a robust disaster recovery solution which automatically creates a backup of your website at regular intervals. Using state of the art storage and security technologies, the service lets you quickly and easily restore your site in the event of catastrophic data loss.
- cWatch Backup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

Open the backup section

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



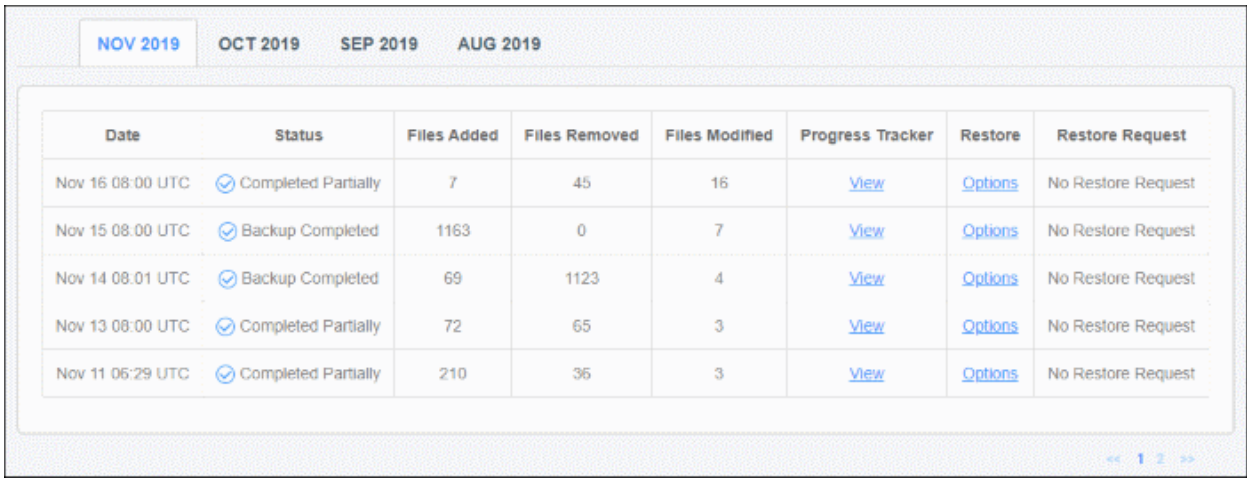
The top panel shows summary information about your latest backup, your current usage, and more:



- **Backup service is active / not active** – Indicates whether backup is enabled or disabled in **backup settings**.
- **Last Successful Backup** – Date and time of the most recent backup operation.
    - The figure below the check-mark shows the total size of the files you have in your backup.
- **Disable Schedule Backup** – Activate or deactivate automatic backups. See '**Configure Backup Settings**'

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

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



From this pane you can:

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

Settings

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

See the following sections for more on each:

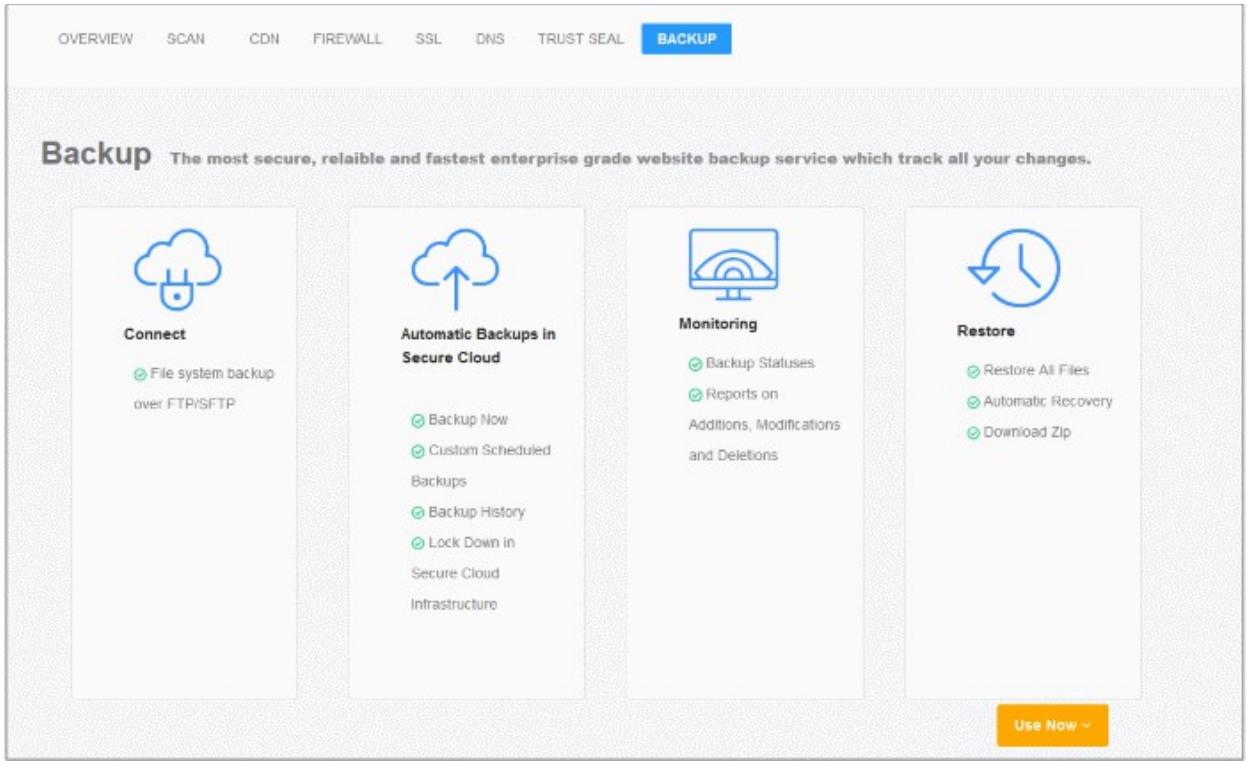
- **Purchase a Backup License**
- **Configure Backup Settings**
- **On-Demand Backup**
- **View Backup Records**
- **Restore and Download Website Files**

4.8.1 Purchase a Backup License

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

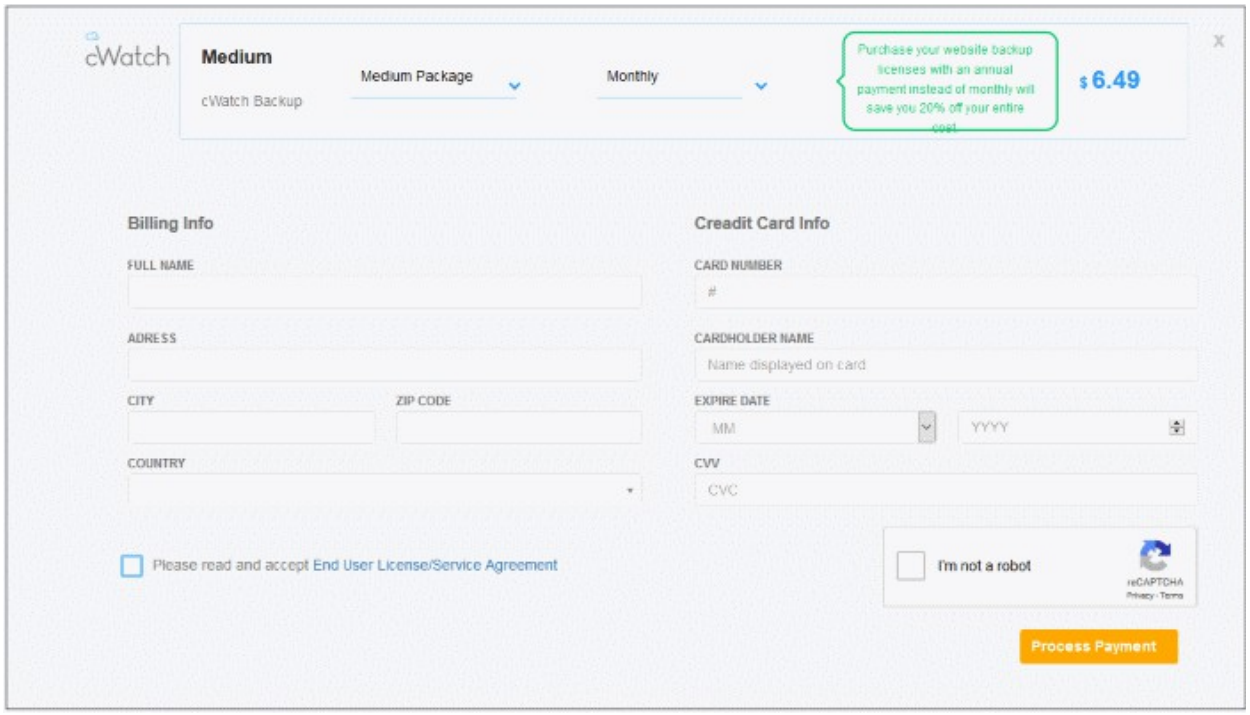
Open Backup section

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



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

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



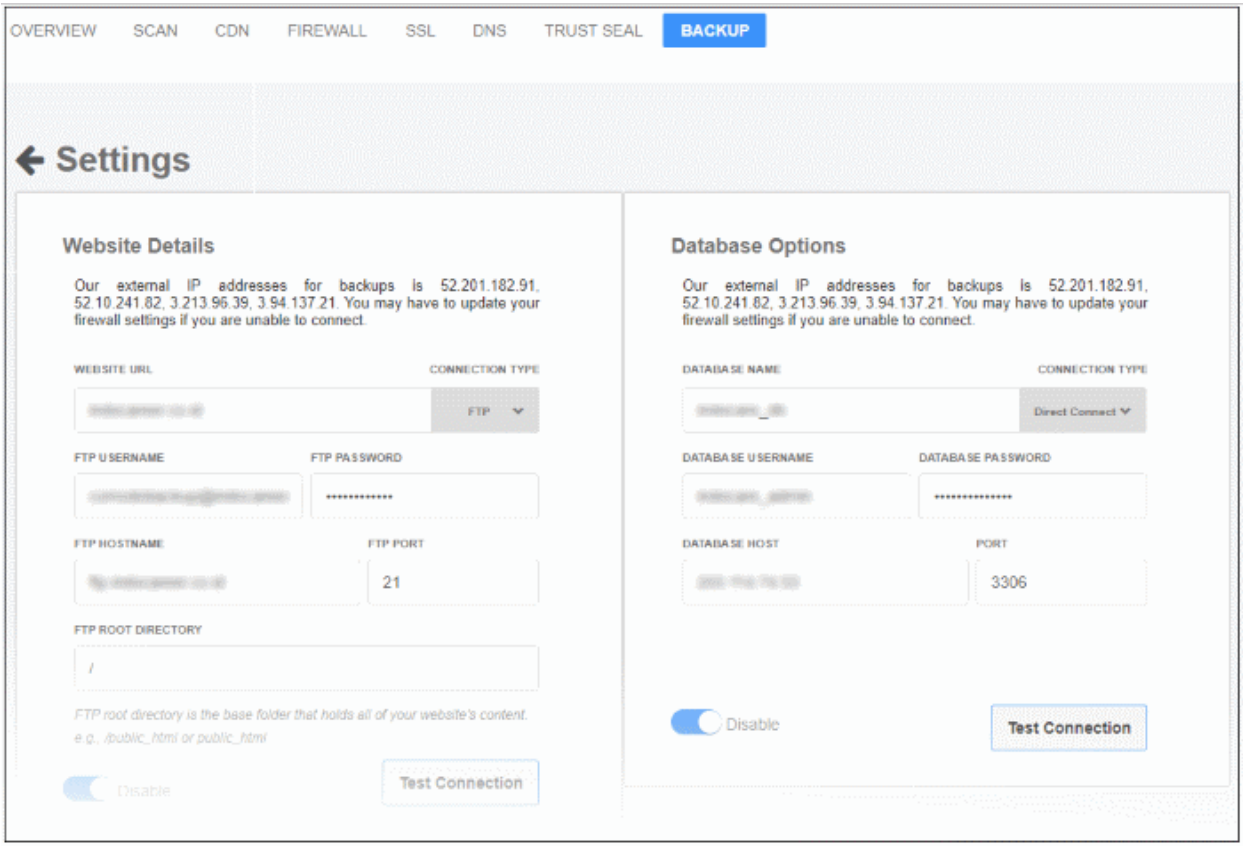
- Click 'Process Payment' to submit your order
- Repeat the process to purchase licenses for other sites on your account.
- We will notify you when your license is due for renewal, or when you are approaching your storage limit.
- Next, **configure your backup**

4.8.2 Configure Backup Settings

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

Open the backup settings page

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



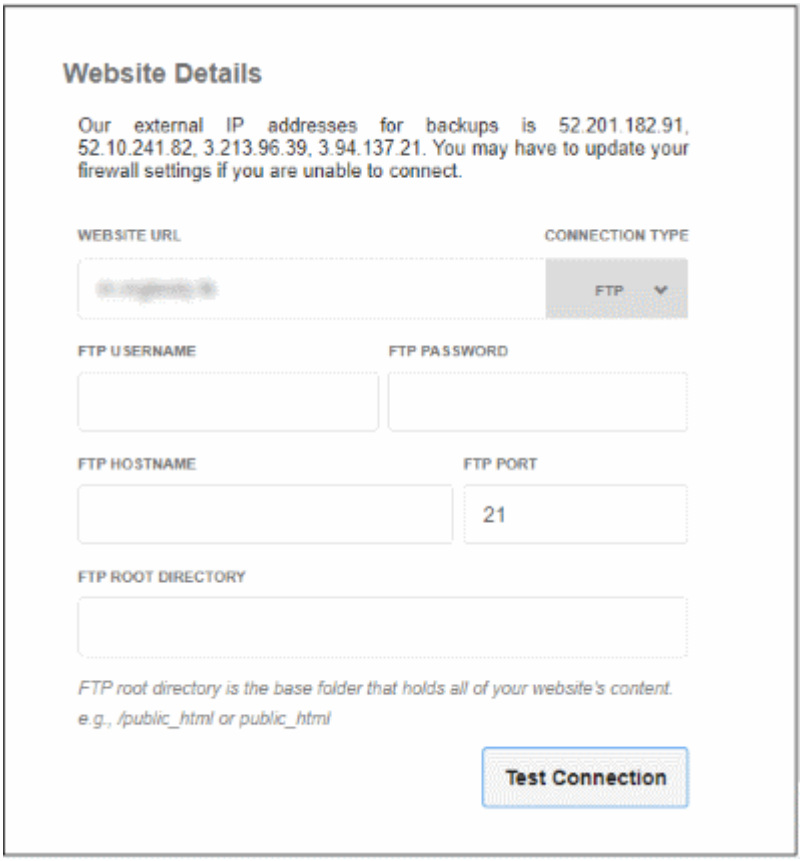
See the following for details about each of the settings:

- **Website Backup Settings**
- **Database Backup Settings**
- **Schedule your Backup**
- **Notification Settings**
- **Backup Exclusions**

Website Backup Settings

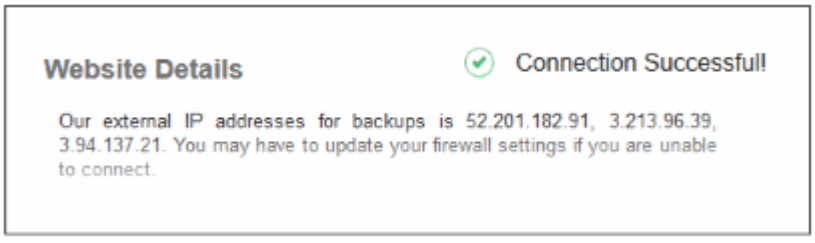
This section explains how to connect your site to the backup servers.

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



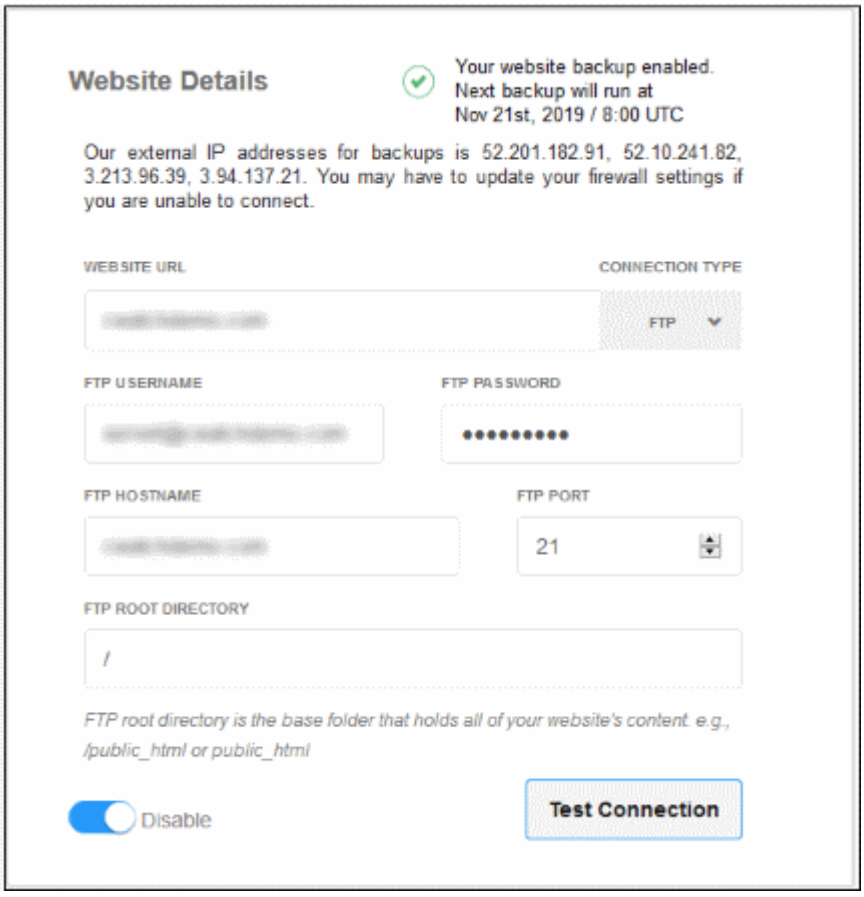
- **Website URL** – Enter the domain of your site. Do not include http:// or https:// at the start.
- **Connection Type** – Select one of the following:
  - **FTP** – Enter the username and password of your FTP server
  - **SSH-KEY** – Add the private key shown in the interface to your authorized keys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

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

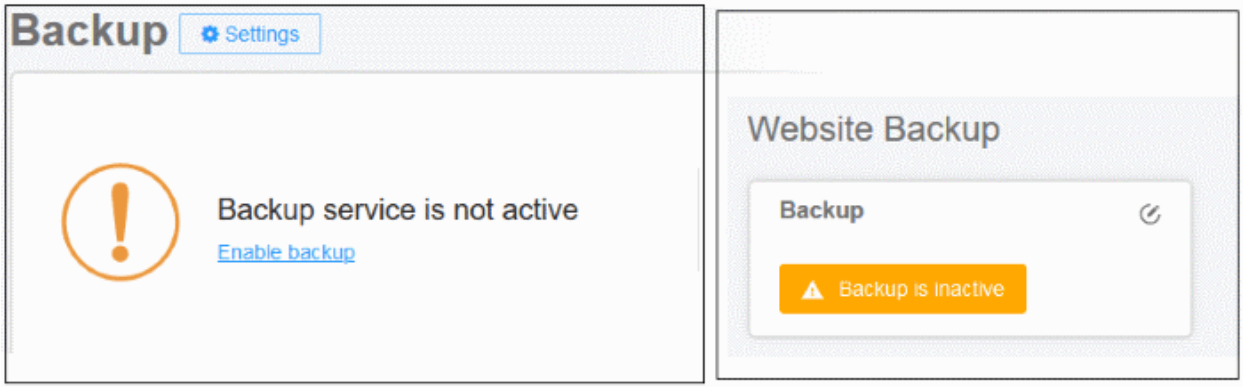


- Click 'Save'

The backup service is activated. You can enable or disable the service using the switch at the bottom.



Note – you will see an error message if you have a backup license, but the file and database backup settings are not configured:



- Click 'Enable backup' / 'Backup is inactive' to open the settings page.

Database Backup Settings

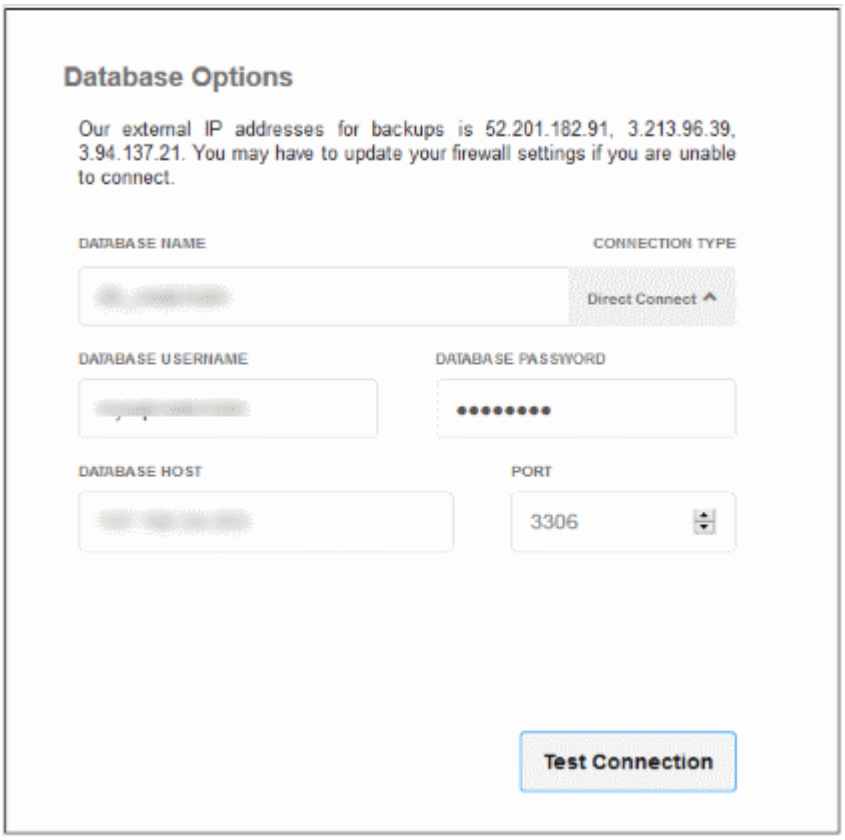
This settings is configured to back up your website database to cWatch servers

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

Database Options

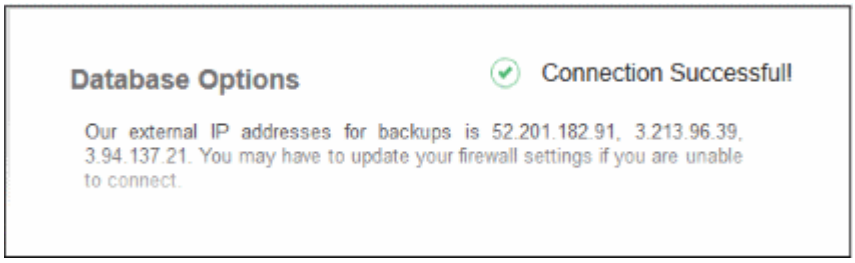
Your site databases are handled separately to the rest of the files on your site. Use this section to tell cWatch of the name, location and connection method of your database.

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



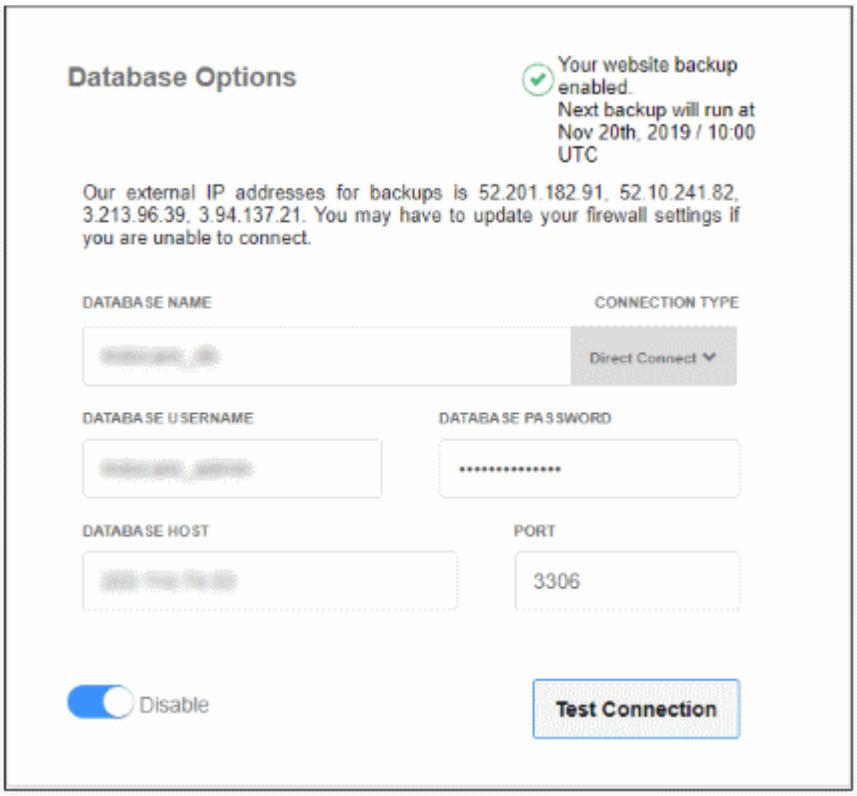
- **Database Name** – Your database's label
- **Connection Type** – Select one of the following:
  - **Direct Connect** – An AWS network connection from your database server to the cWatch server.
  - **SSH-KEY** - Add the private key shown in the interface to your authorized keys file (…/ssh/authorized_keys)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

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



- Click 'Save'

The database backup service is activated and you have the option to enable or disable it using the button at the bottom.

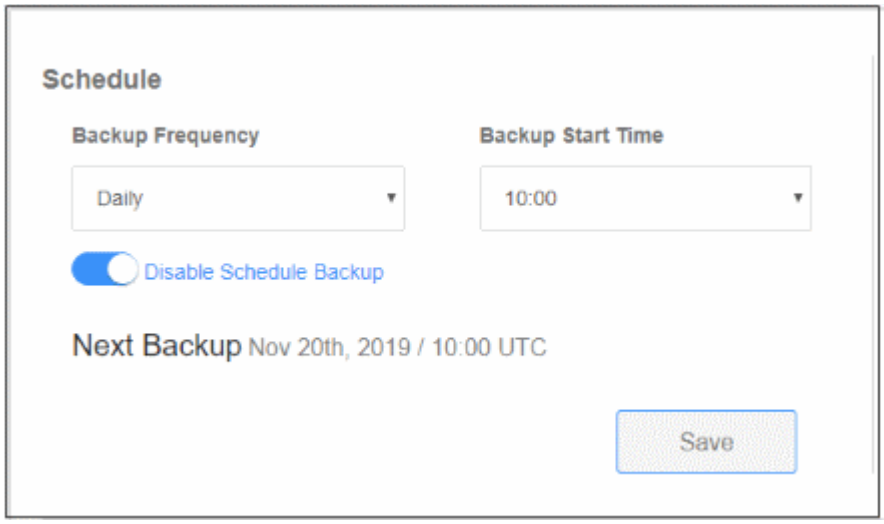


Backup service is not active message is shown in the backup and overview pages if you disable backup here. This message is also shown if you have a backup license but the file and database backup settings are not configured.

Schedule your Backup

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

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



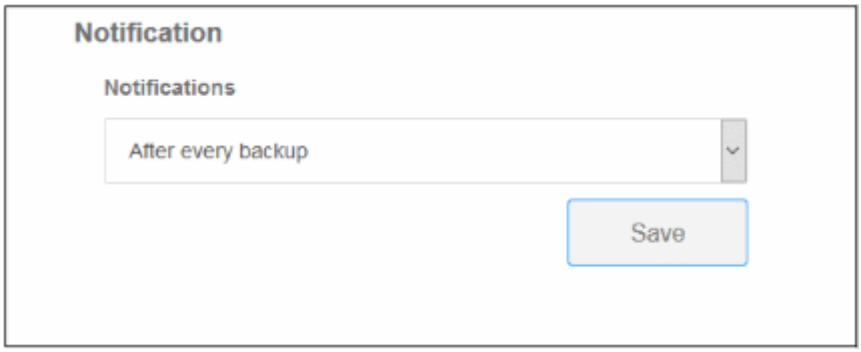
- **Backup Frequency** – Four options are available:
  - **Daily** - Backups start at the date/time shown in 'Next Backup', then run every day at the same time thereafter
  - **Every 2 days** - Backups start at the date/time shown in 'Next Backup', then run every other day thereafter.
  - **Weekly**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

- Click 'Save'

Notification Settings

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

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



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

Backup Exclusions

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

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

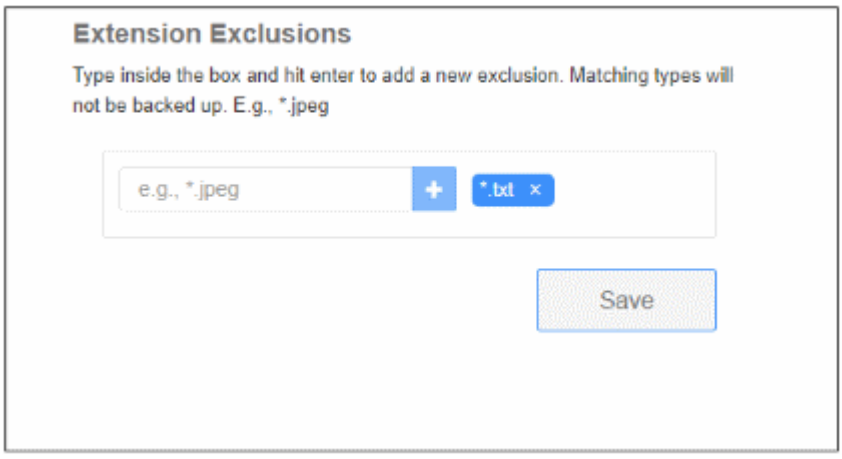
Directory Full Path

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

- Click 'Save'

Extension Exclusions

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



- Type the extension of the file that you want to exclude. You must prefix the extension with *.

- For example, *.txt
- Click '+'.
- Repeat the procedure to add more file extensions.

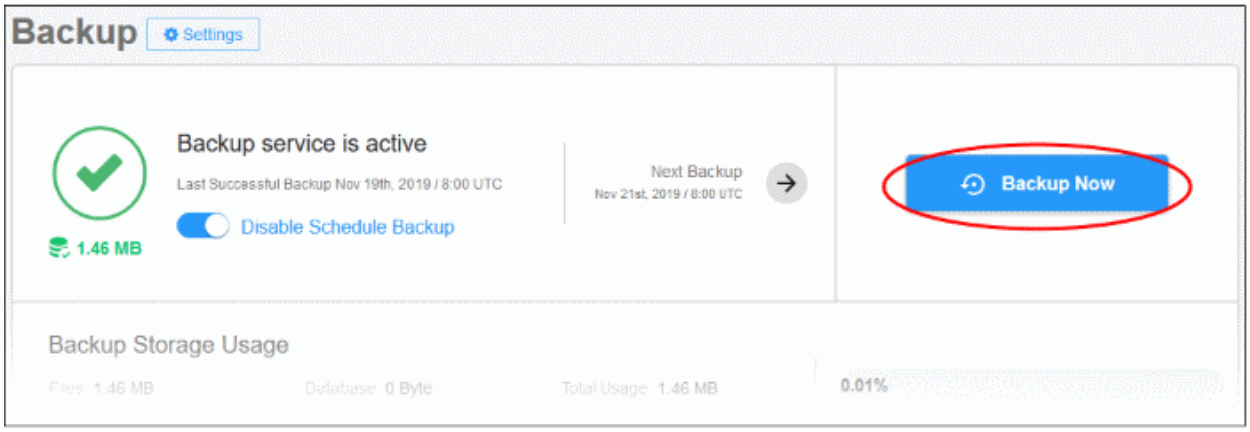
- Click 'Save'

4.8.3 On-Demand Backup

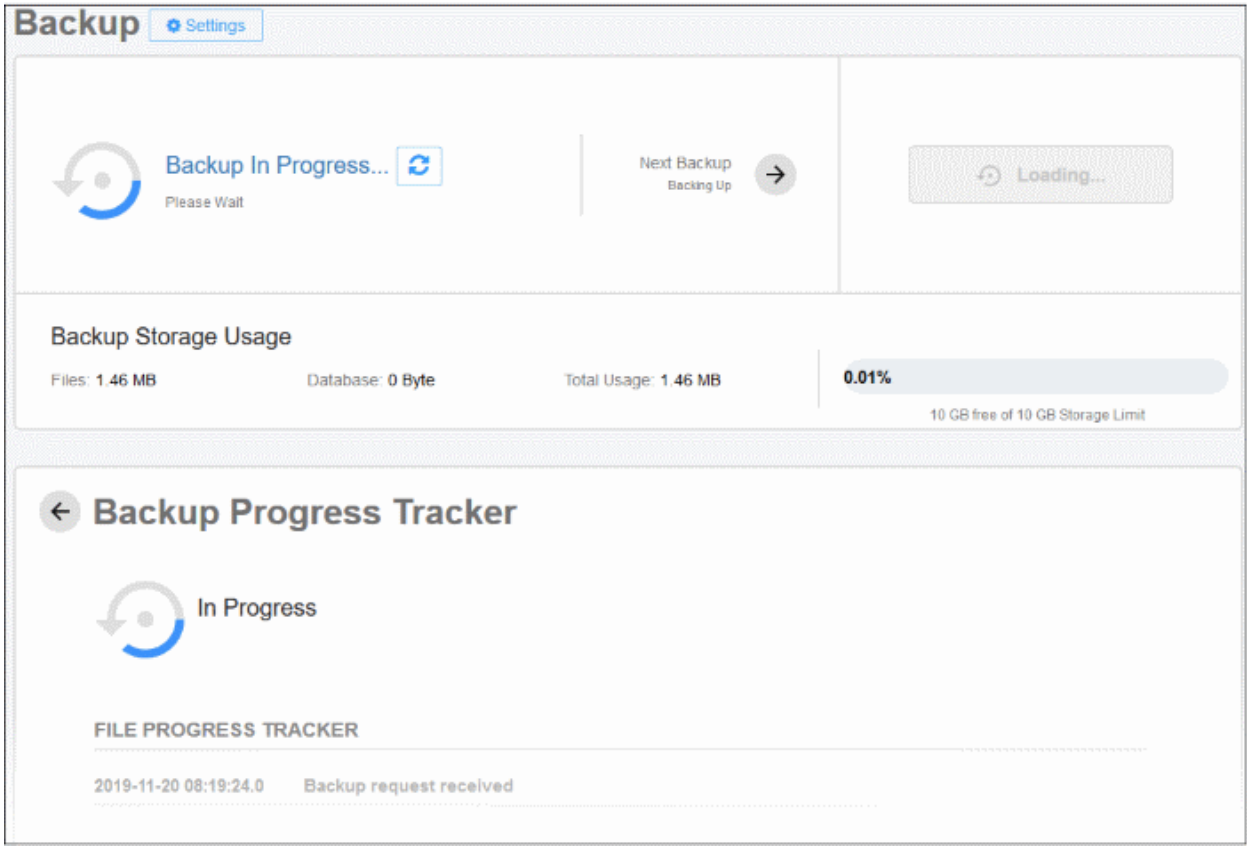
An on-demand backup is one that you run at any time as circumstances demand. For example, you might want to run an on-demand backup just prior to putting some website changes live.

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

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

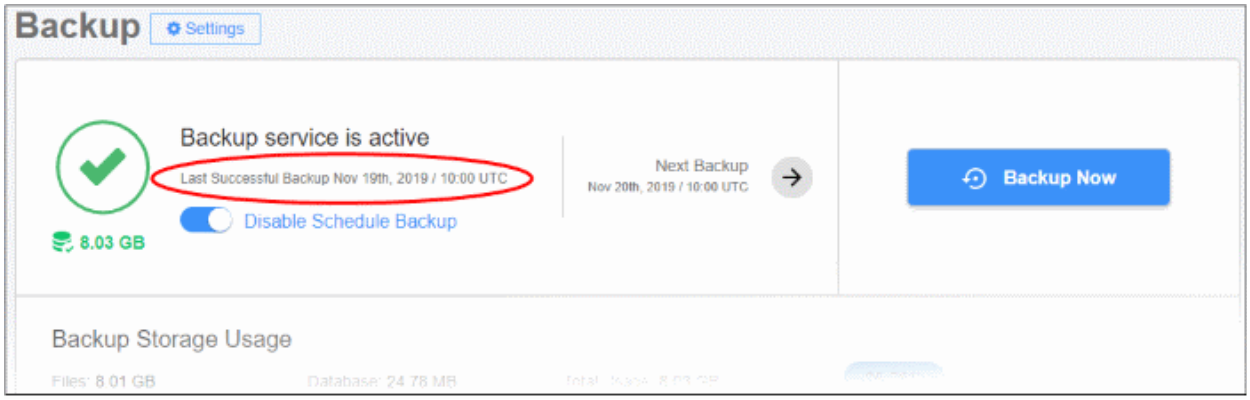


The progress of the backup is shown as follows:



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

The date of the most recent backup is updated when the operation finishes:

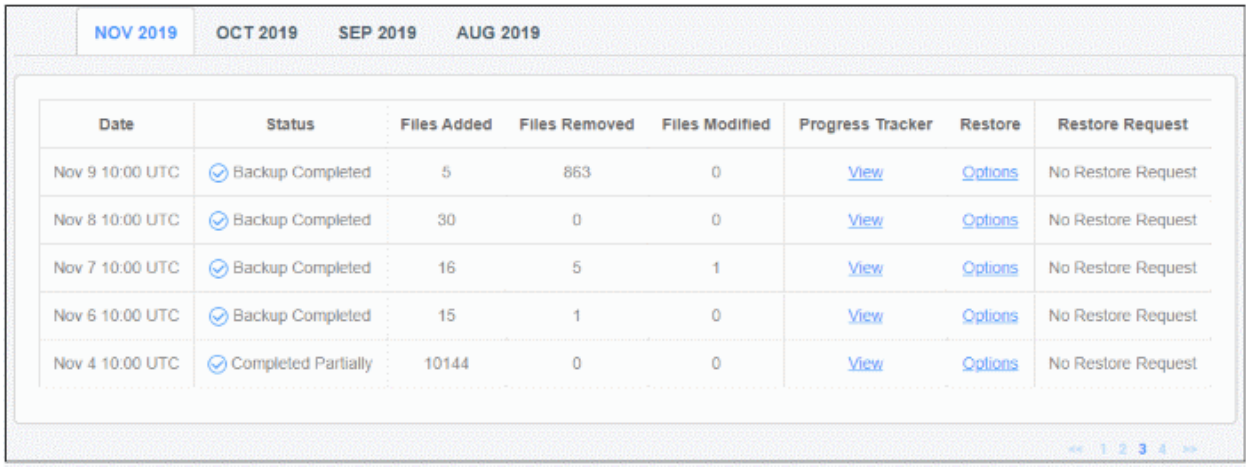


4.8.4 View Backup Records and File Statistics

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

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

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

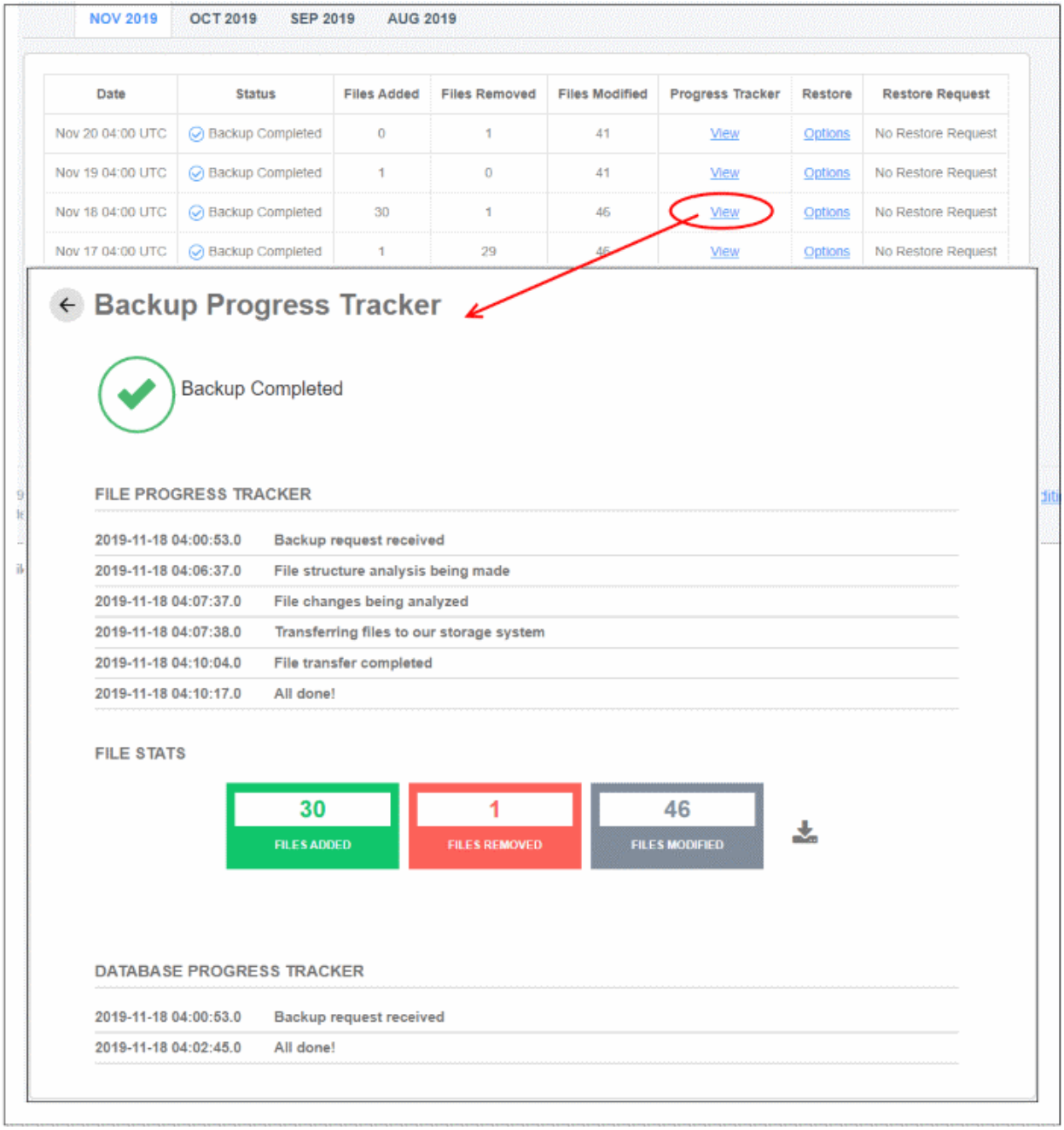


Backup Records - Table of Parameters	
Parameter	**Description**
Date	When the backup was run
Status	Whether or not the backup was successful. Possible values are: • **Backup Completed** – All items, files and database, were transferred successfully. • **File Backup Failed** – File copying did not succeed for some reason. For example, the internet connection failed. • **DB Backup Failed** – The database backup did not succeed for some reason. • **Completed Partially** – Some files weren't copied because they were deleted between the start and finish of the backup operation. • **Backup in Progress** – Backup is running.
Files Added	Number of new files added compared to the previous backup
Files Removed	Number of files removed compared to the previous backup
Files Modified	Number of files that were updated since the previous backup
Progress Tracker	View the exact names of files added, removed or edited. **Click here** for more details.
Restore	Restore your website using the files/database in this record. See '**Restore and Download Website Files**'
Restore Request	Details are shown here if your web site was restored using the backup on this row. Click 'View' to view the restore details. See '**Restore and Download Website Files**'

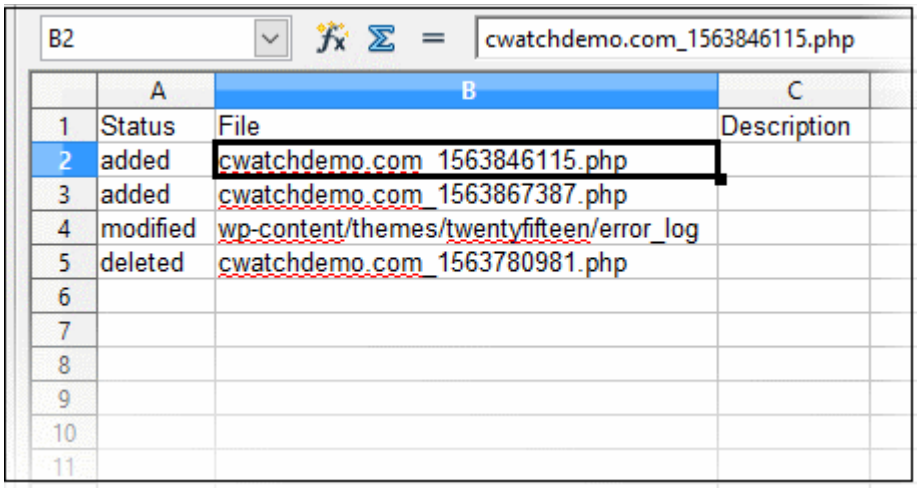
View File Statistics

The backup progress tracker pane shows how many files were added, removed or modified during a backup operation. You can also download the record to view the exact files that were involved.

- Click 'View' in a backup record



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



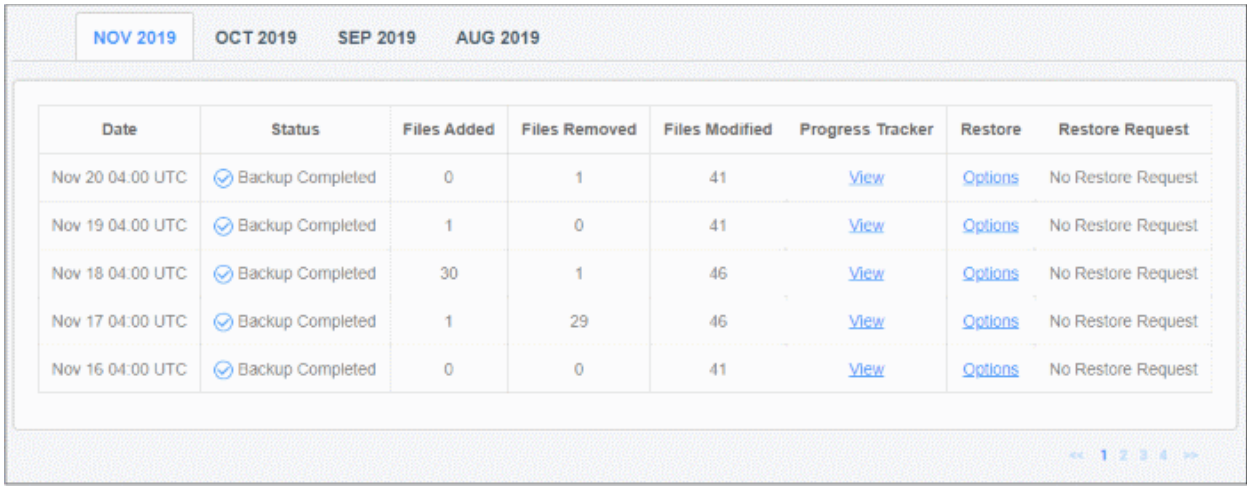
4.8.5 Restore and Download Website Files

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

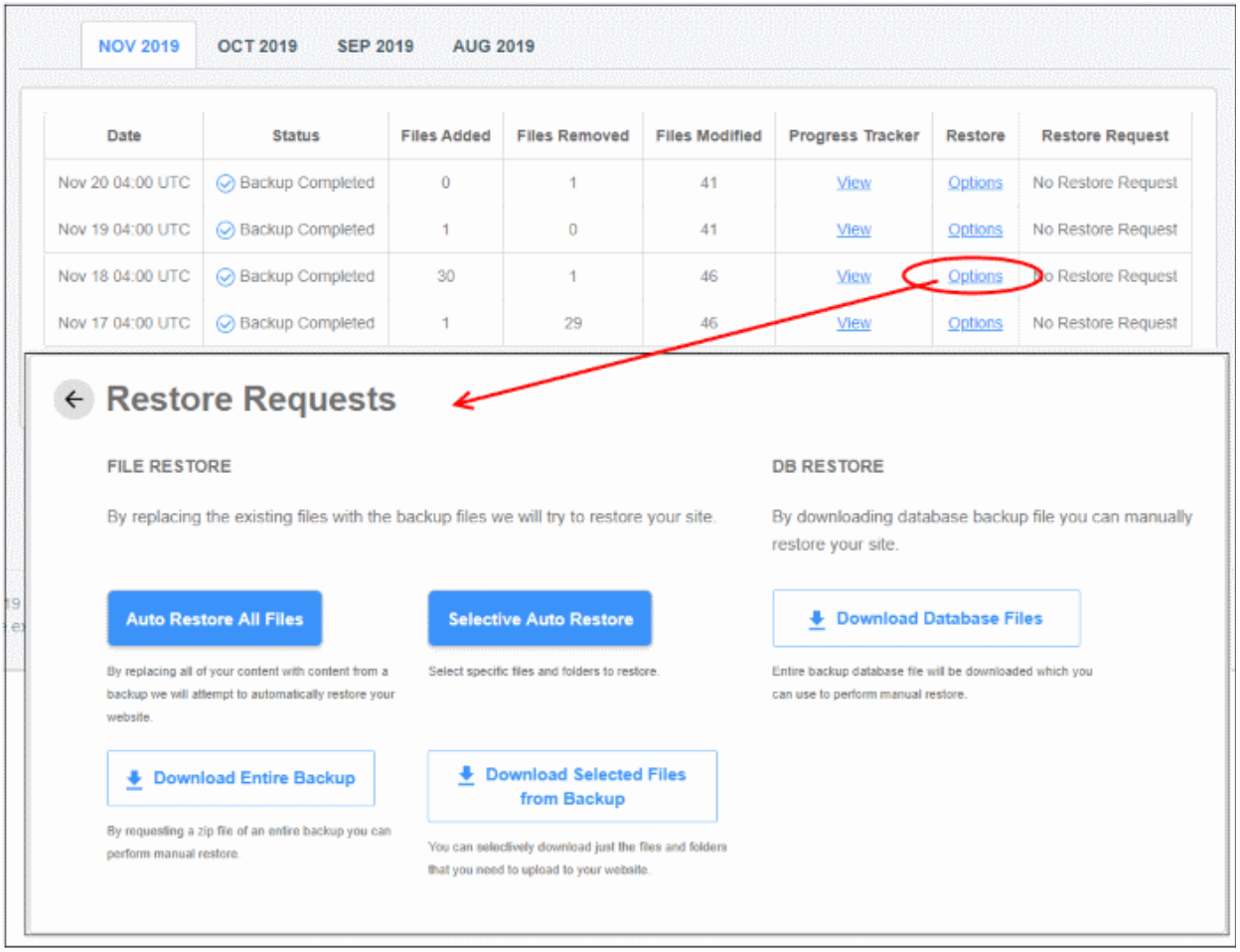
The options above offer you flexibility when restoring a website. For example, you can restore your site to the 'last-known-working' version, while keeping a database which has your most recent transactions.

Run a restore operation

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



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

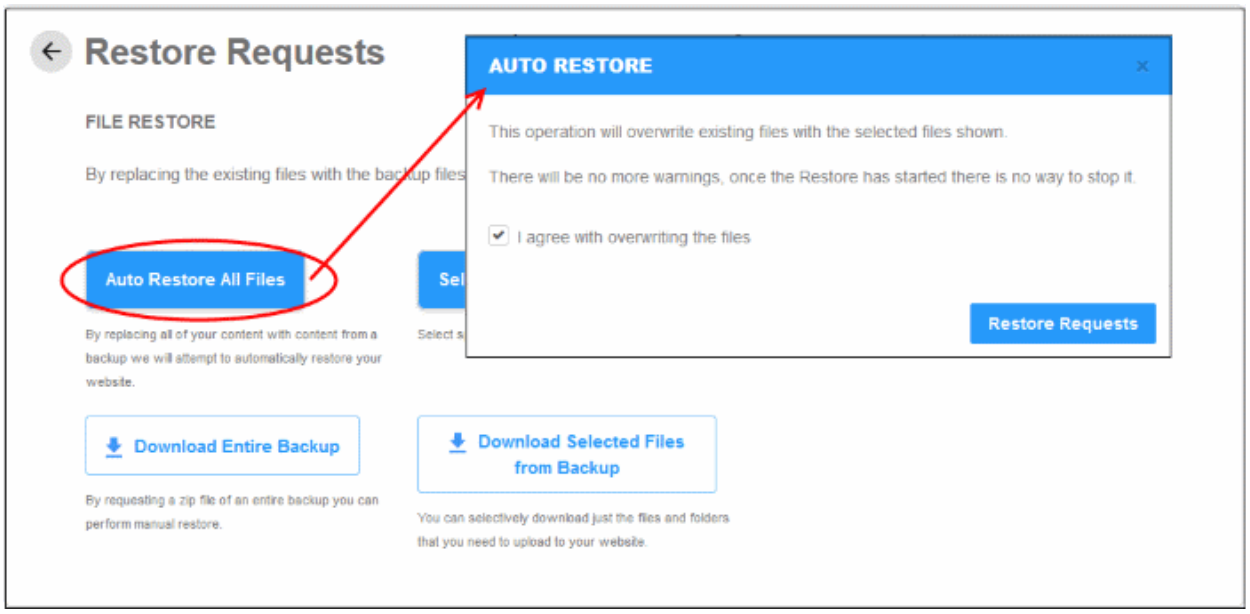


- File Restore:
  - **Auto Restore all Files** - Start the restore process. Files in the destination will be replaced by those in the backup.
  - **Selective Auto Restore** – Restore specific files and folders.
  - **Download Entire Backup** - Download a .zip file of the backup. You can use this to manually restore files, or to run a partial restore, or to simply retrieve some lost / older versions of files.
  - **Download Selected Files from Backup** – Retrieve specific files from the backup. This is a simple download of files, rather than restoring them to their original location.
- DB Restore:
  - **Download Database Files** - Download a .zip file which contains all database records. You can manually unzip and restore the database as required.

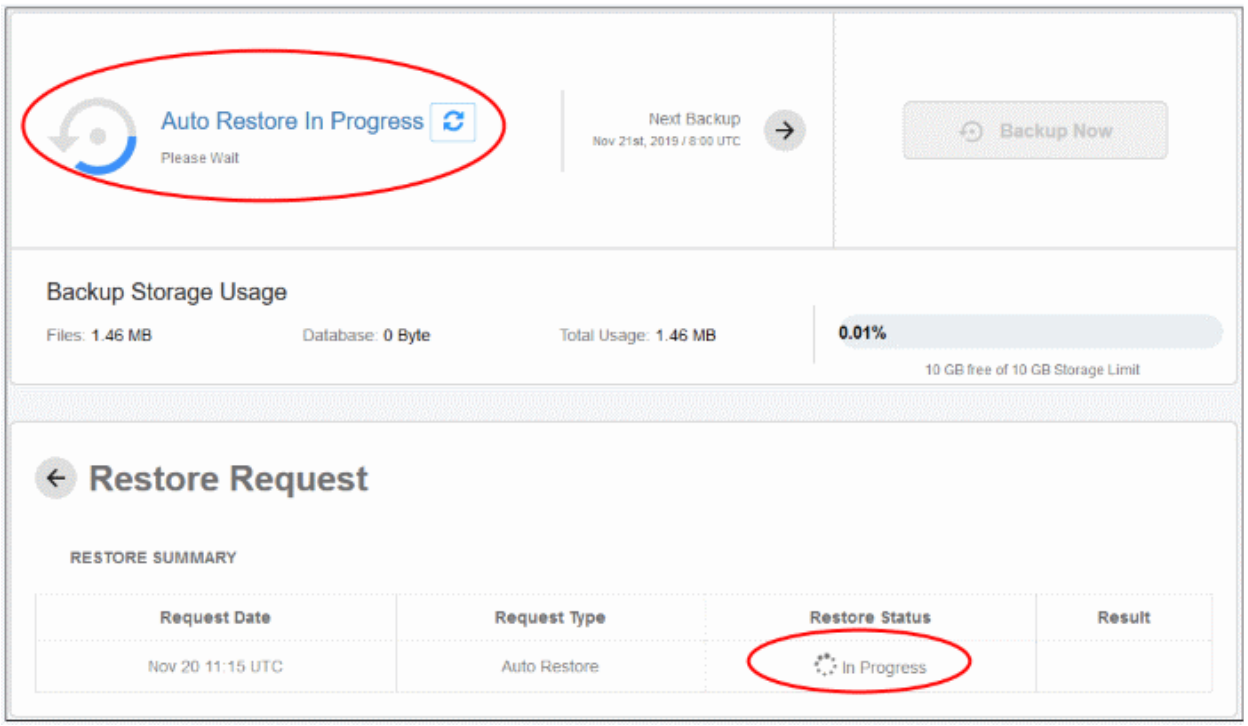
The rest of this section is just screenshots to illustrate the processes above.

Auto Restore all Files

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



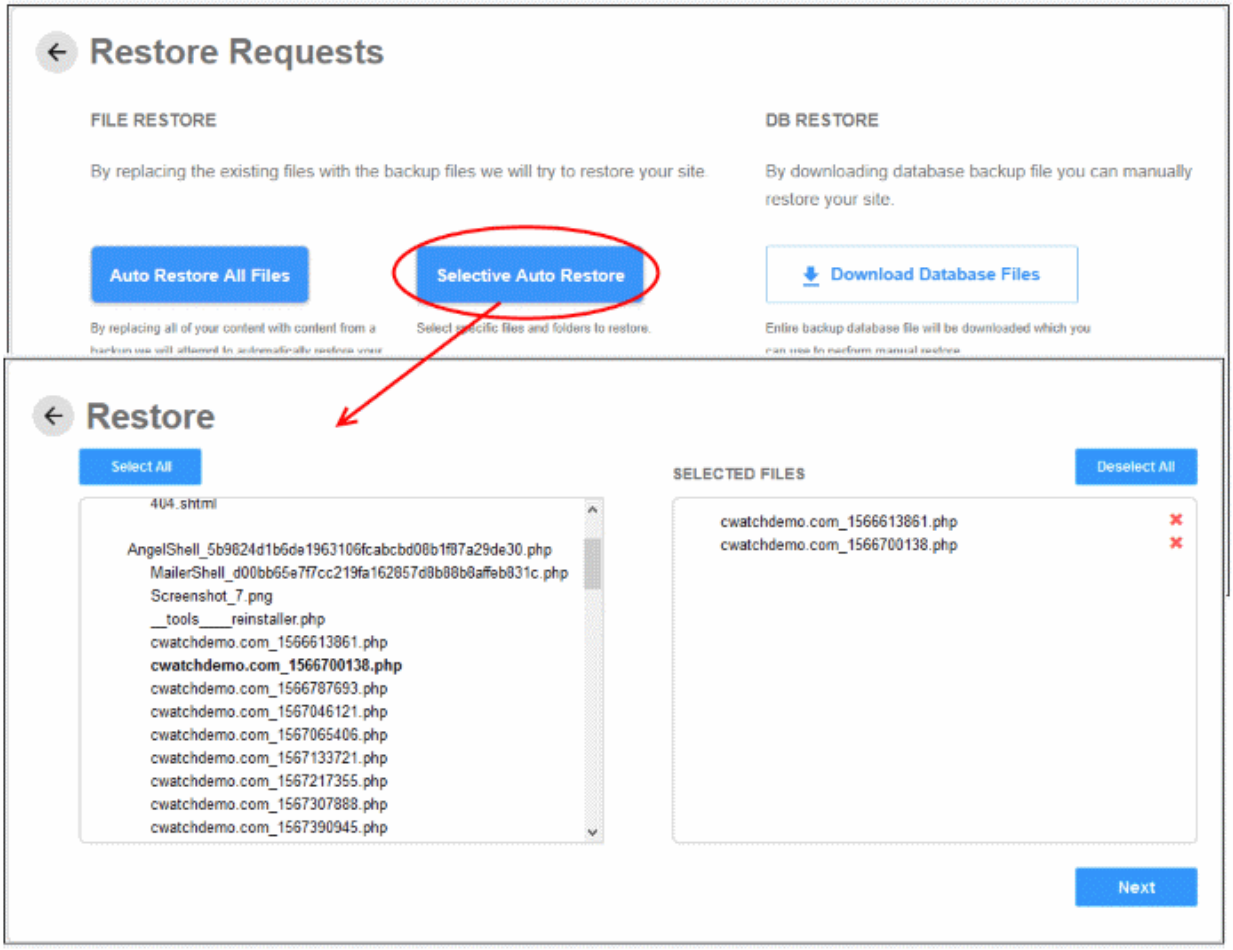
- Agree to overwriting files and click 'Restore'
- You will see the following confirmation:



- Results are shown at the end of the operation:

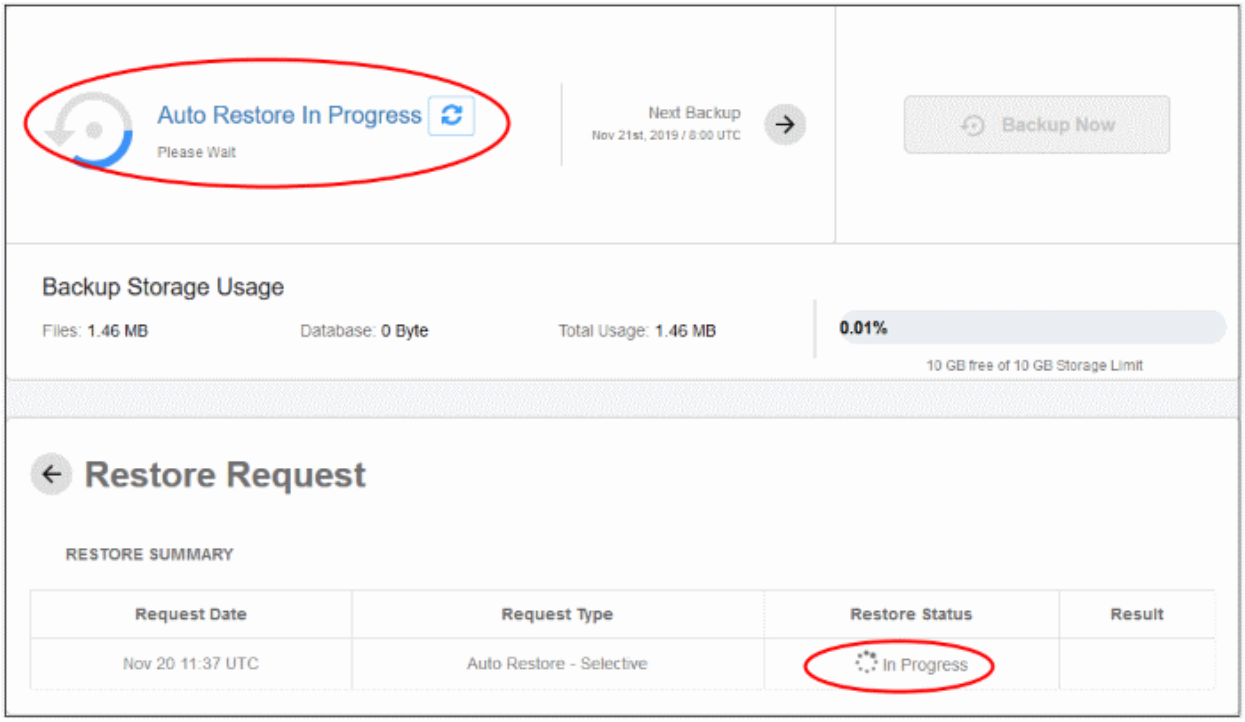
Selective Auto Restore

- Click 'Options' in the row of the backup you want to use
- Click 'Selective Auto Restore':

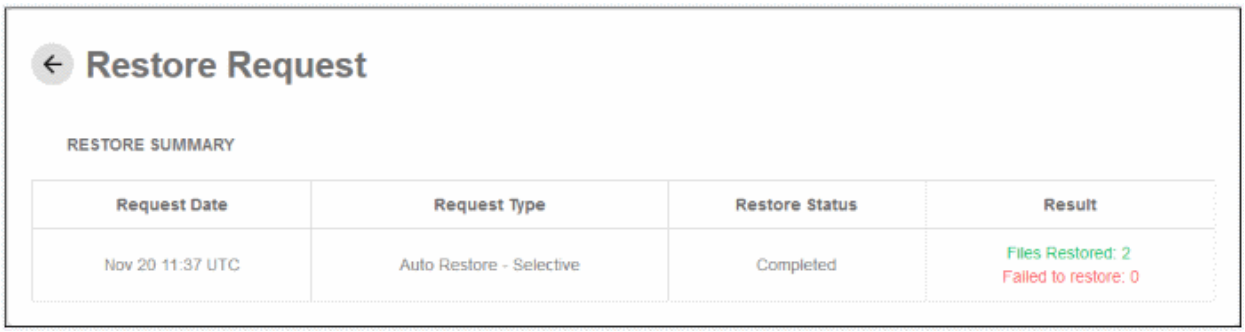


- Select the backed up file(s) on the left and click 'Next'

- Check the selected files detail on the left, agree to overwrite the files and click 'Restore'.
- You will see the following confirmation:

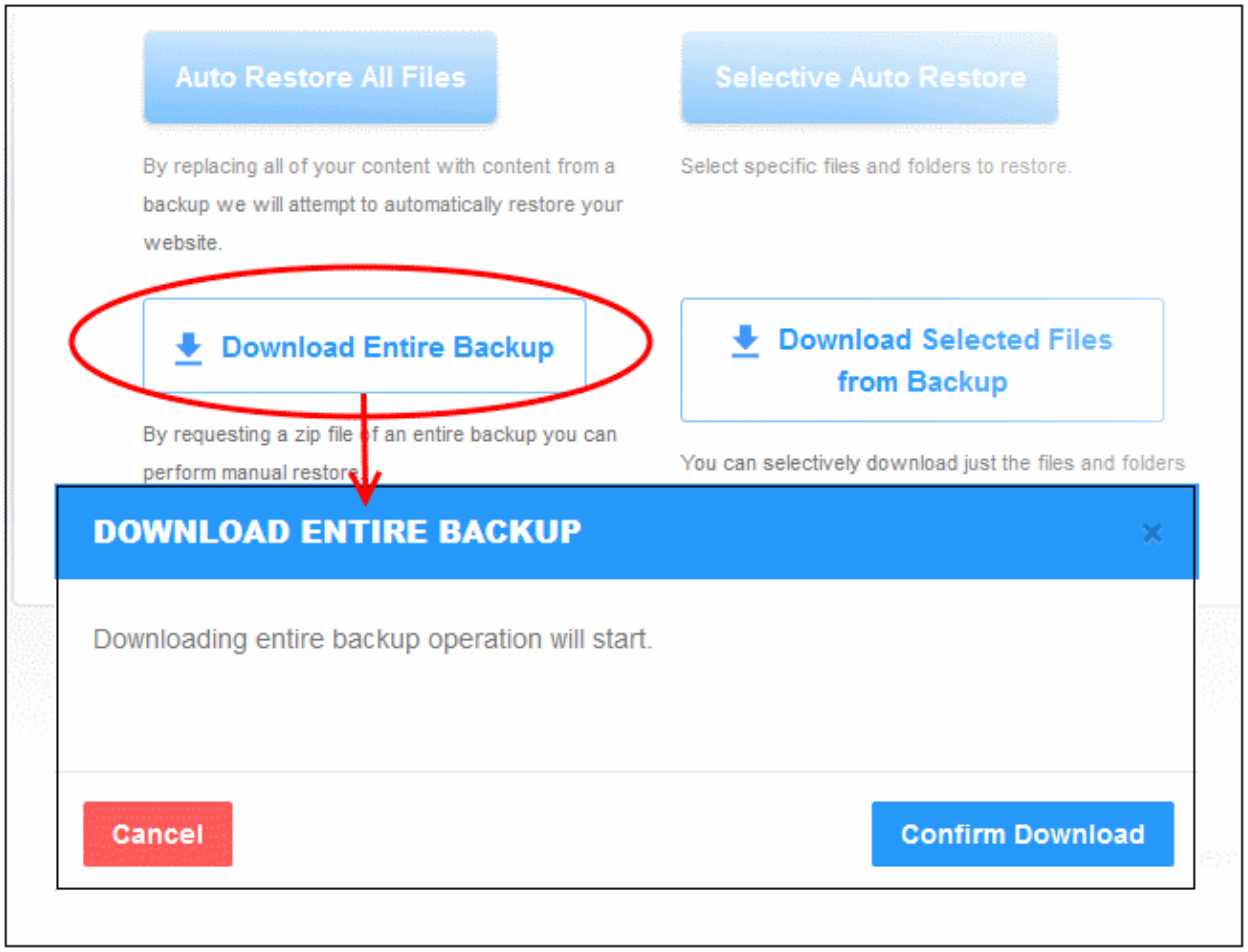


- Results are shown at the end of the operation:

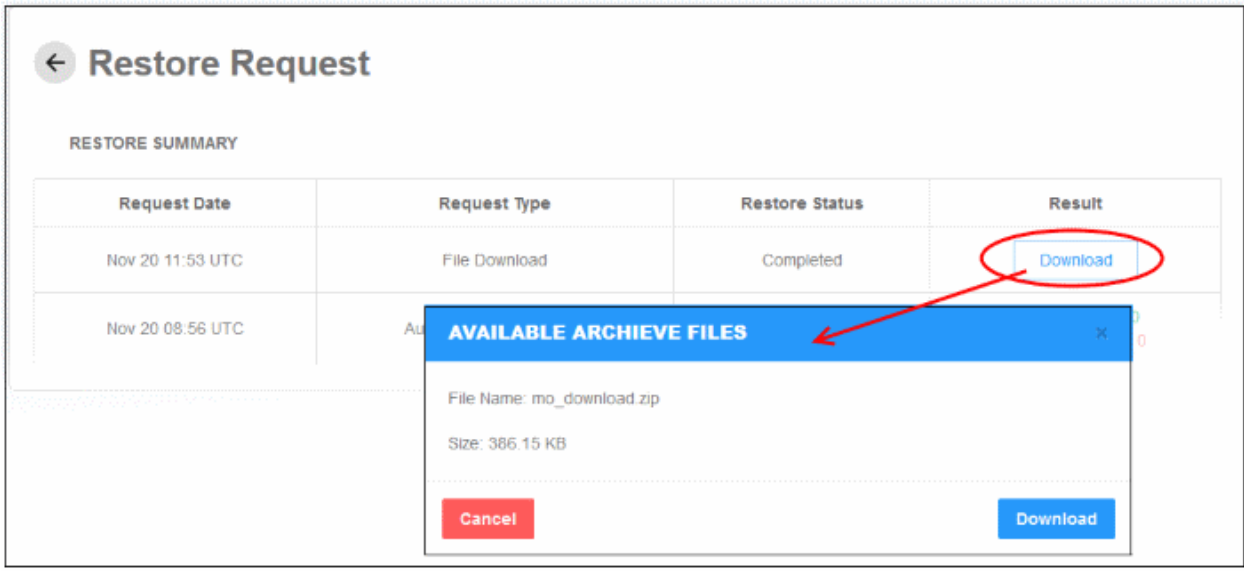


Download Entire Backup

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



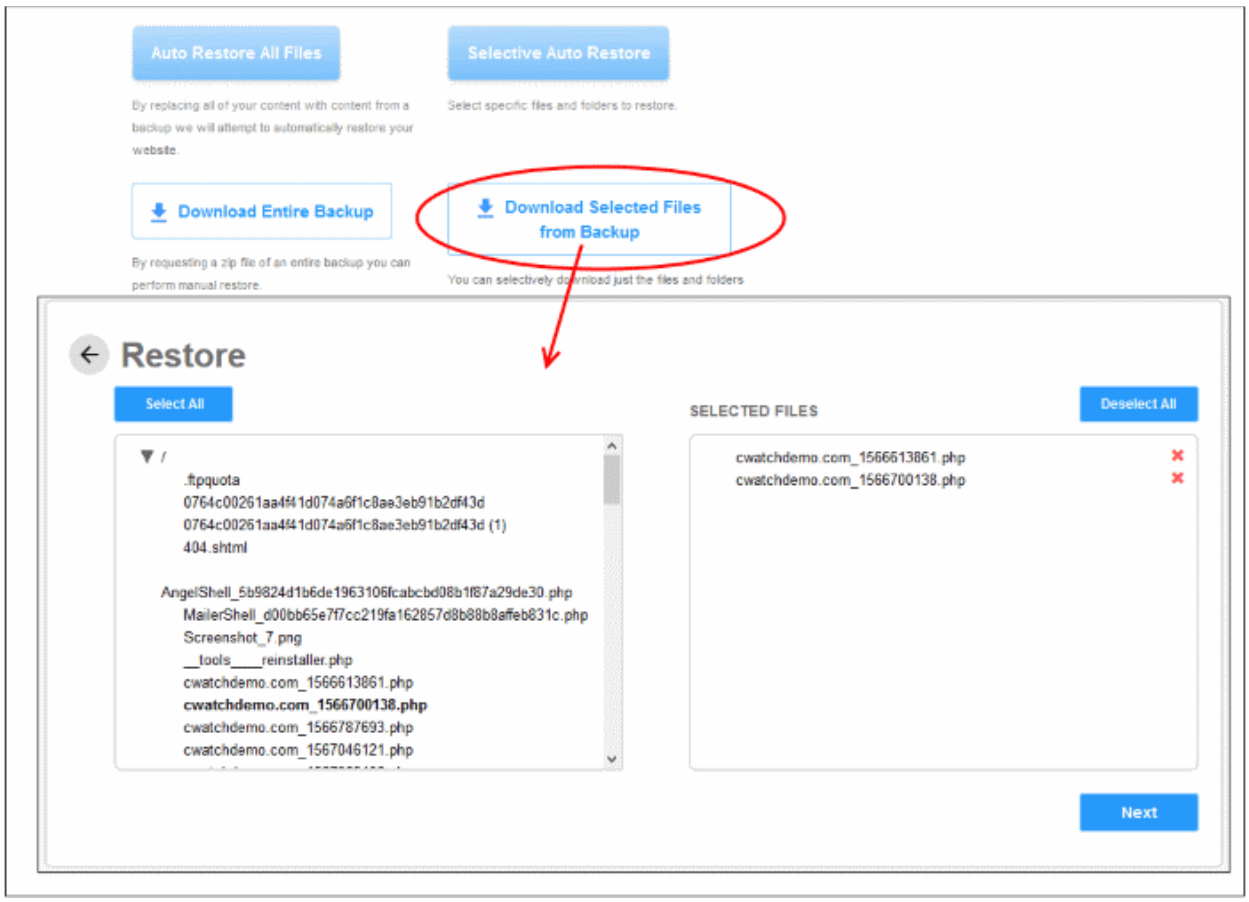
- cWatch will retrieve your files and create a zip file of them. This process may take a few seconds.
- Once complete, click 'Download' in the 'Result' column:



- Click 'Download' to save the zip file

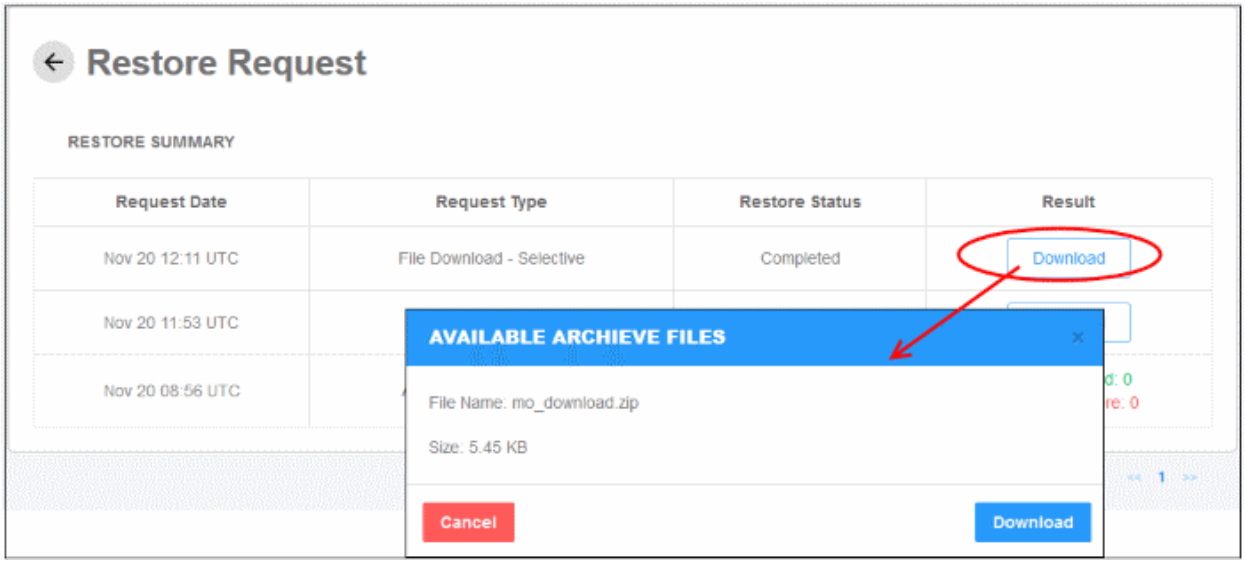
Download Selected Files from Backup

- Click 'Options' in the row of the backup you want to use
- Click 'Download Selected Files from Backup'



- Select the backed up file(s) on the left and click 'Next'

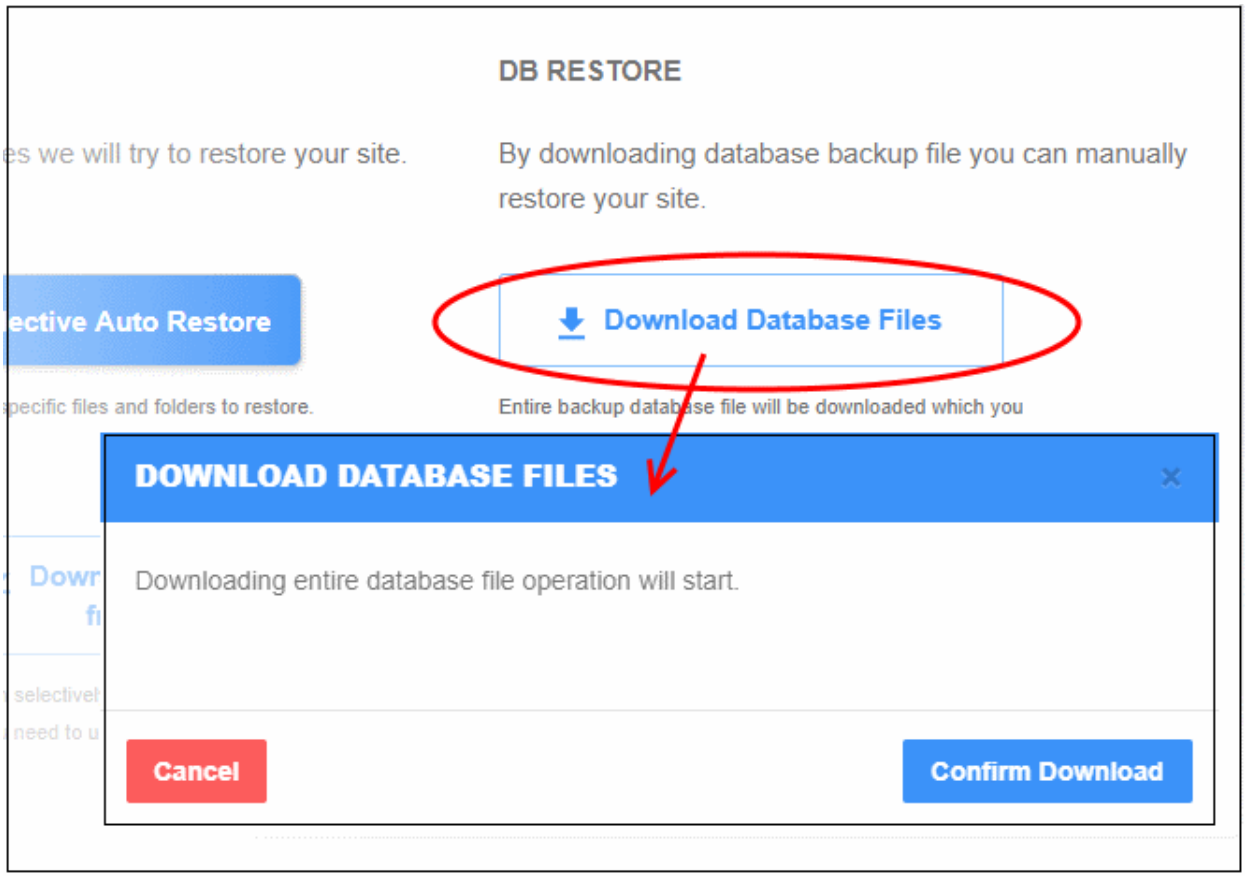
- Check the selected files detail on the left and click 'Download'.
- cWatch will retrieve your files and create a zip file of them. This process may take a few seconds.
- Once complete, click 'Download' in the 'Result' column:



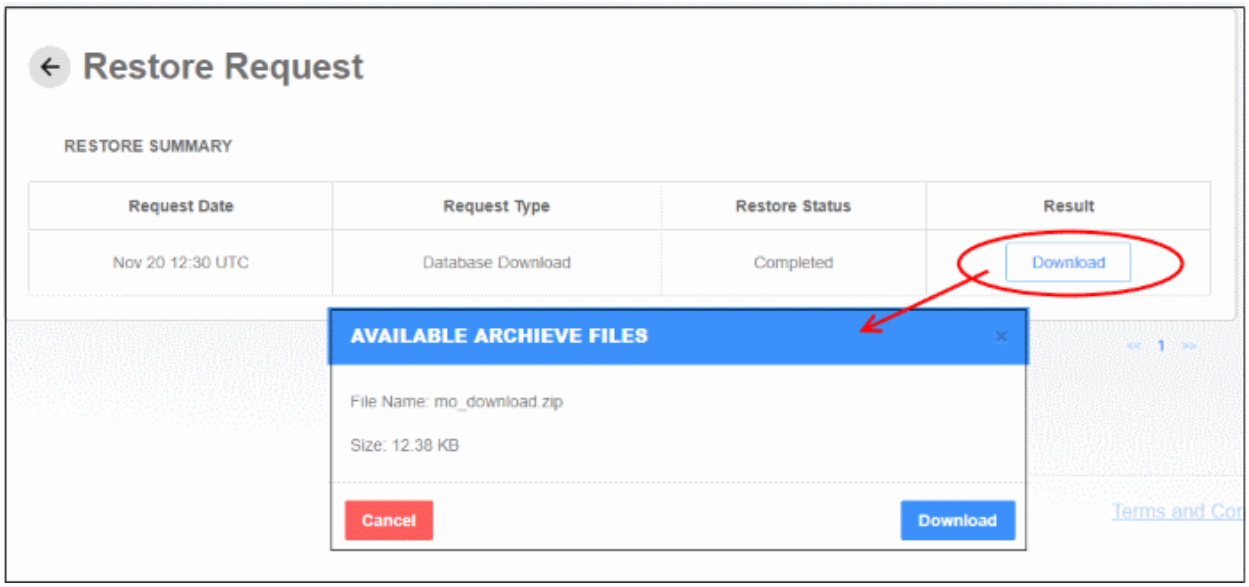
- Click 'Download' to save the zip file

Database Restore

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



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



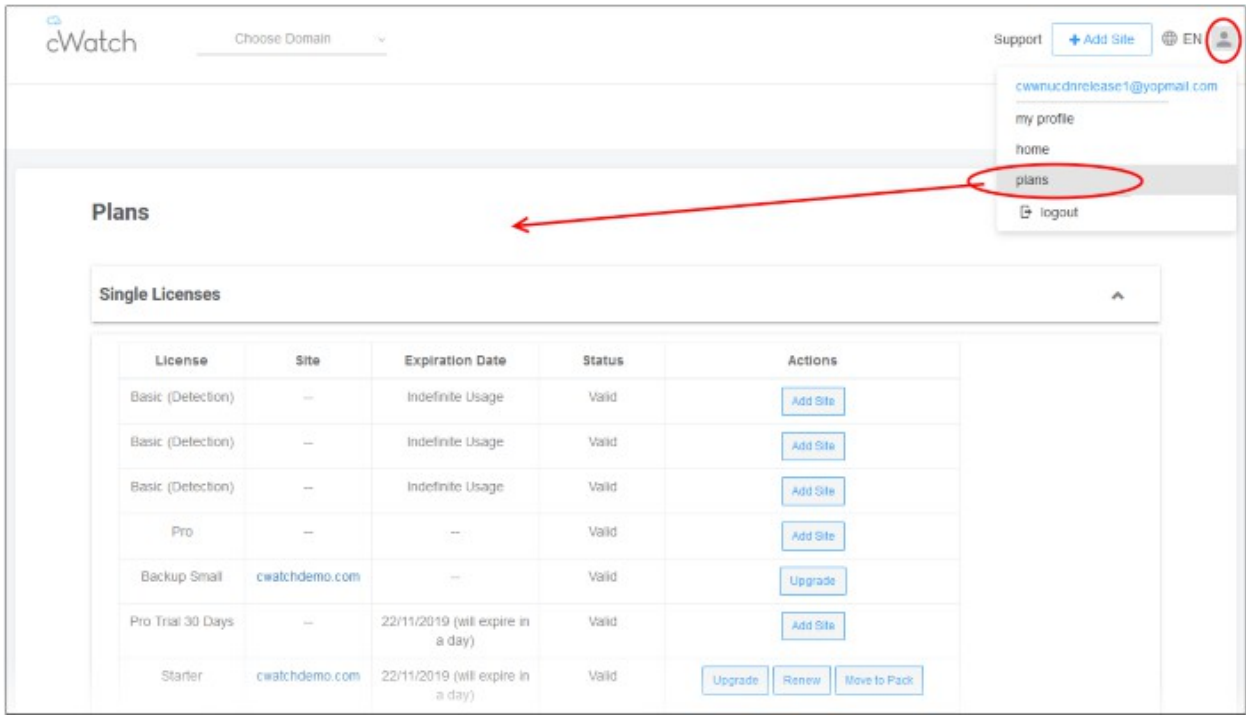
- Click 'Download' to save the zip file

5 View and Upgrade Licenses for Domains

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

Manage Licenses

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



- Single Licenses – Single licenses can be used for one domain
- Multi Pack Licenses – Each license can be used for 5 or 10 sites, depending on the license. Applies to customers that subscribed via a Comodo partner.

Plans - Column Descriptions	
Column Header	**Description**
License	The subscription type
Site	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 the license on a domain**

From this interface you can:

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

Upgrade license for a domain

You may want to upgrade your cWatch license if:

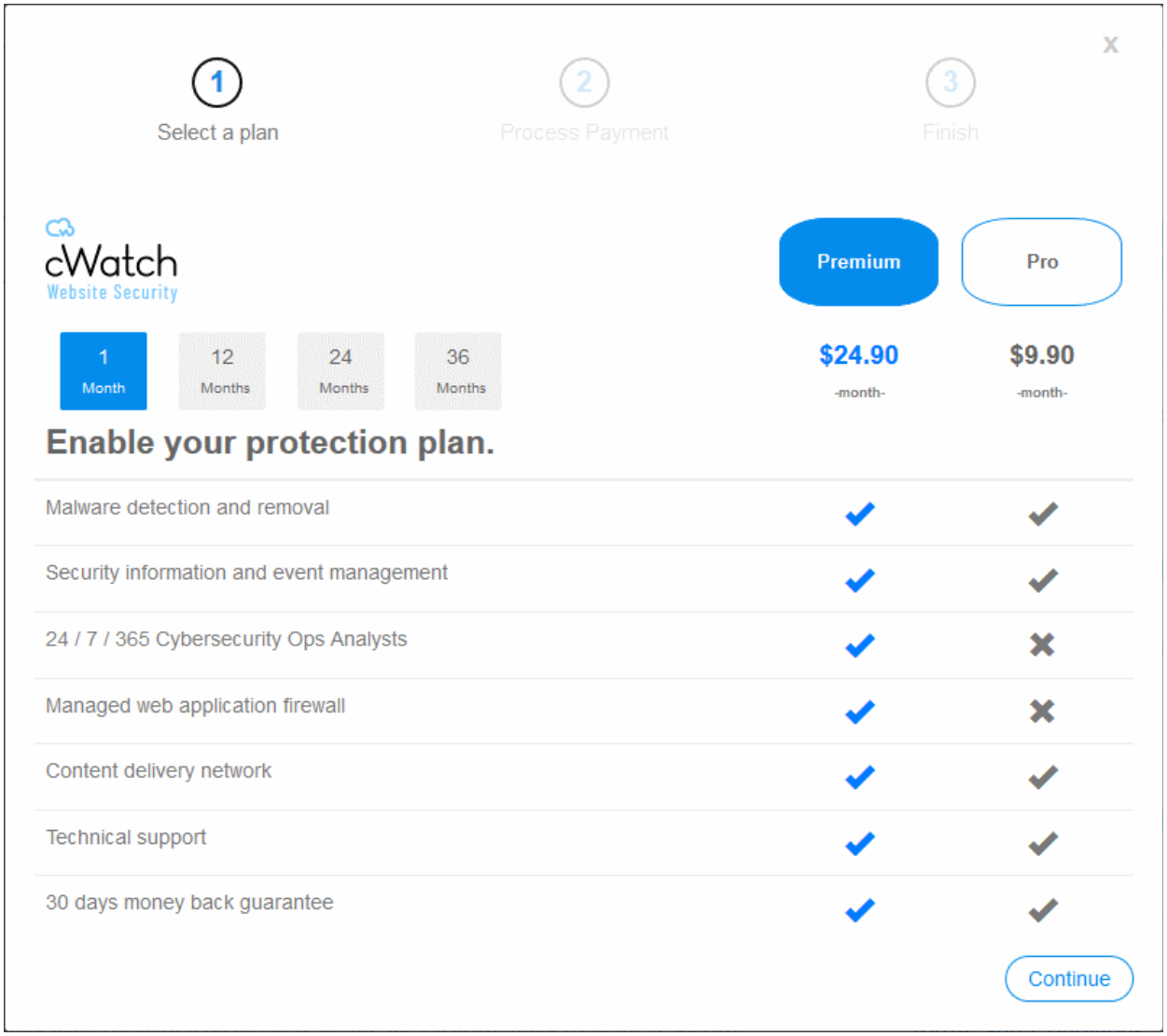
- You want to enable the superior protection features afforded by a Pro or Premium license
- You want to add sub-domains for a website

Upgrade license

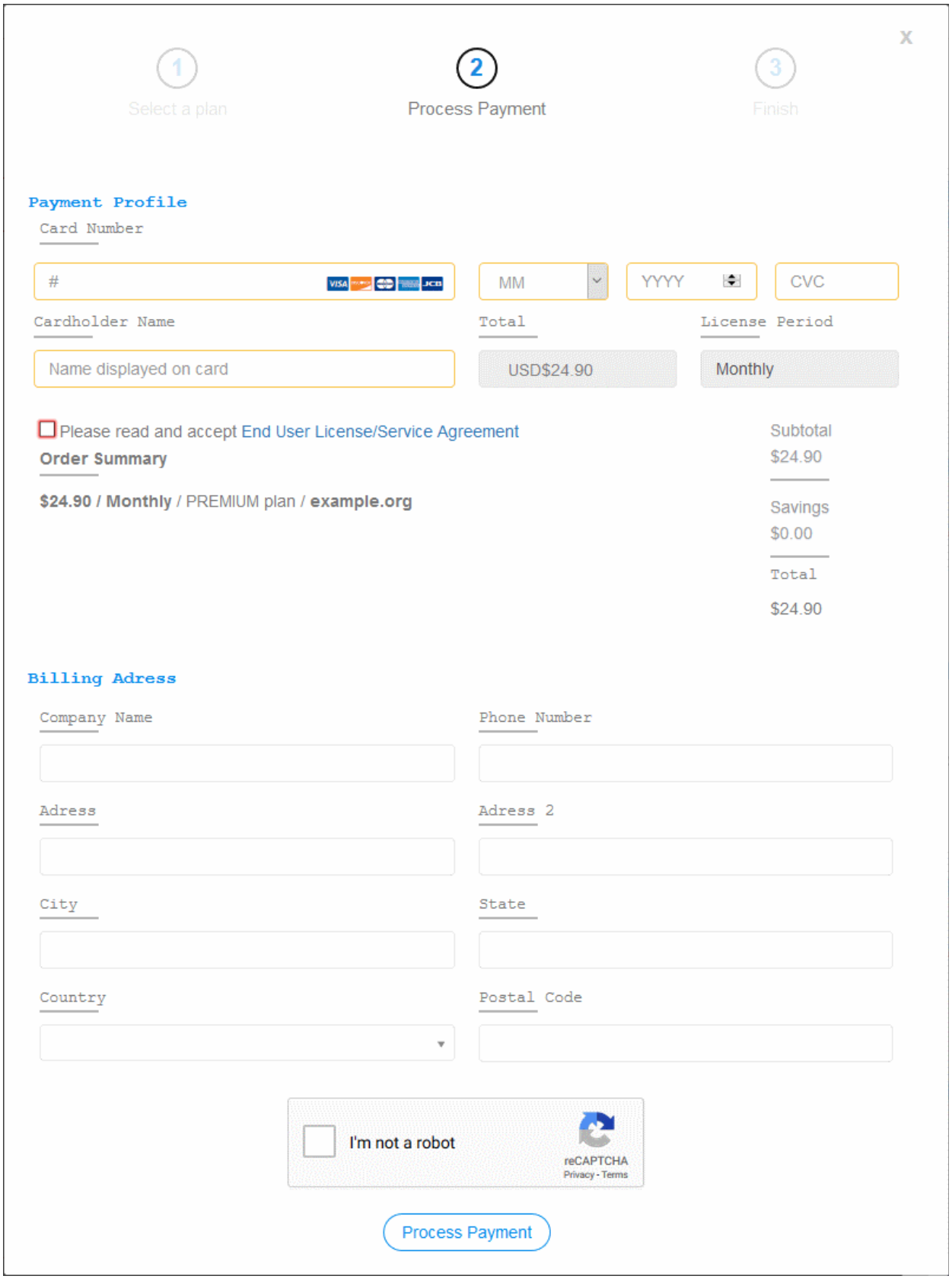
- Click the user icon at top-right
- Select 'Plans' from the drop-down
- The plans screen shows a list of available, unused licenses
- Click 'Upgrade' in the row of the target website
- Select the license you want to associate with the domain then click 'Yes' in the confirmation screen.

The license will be applied to the domain.

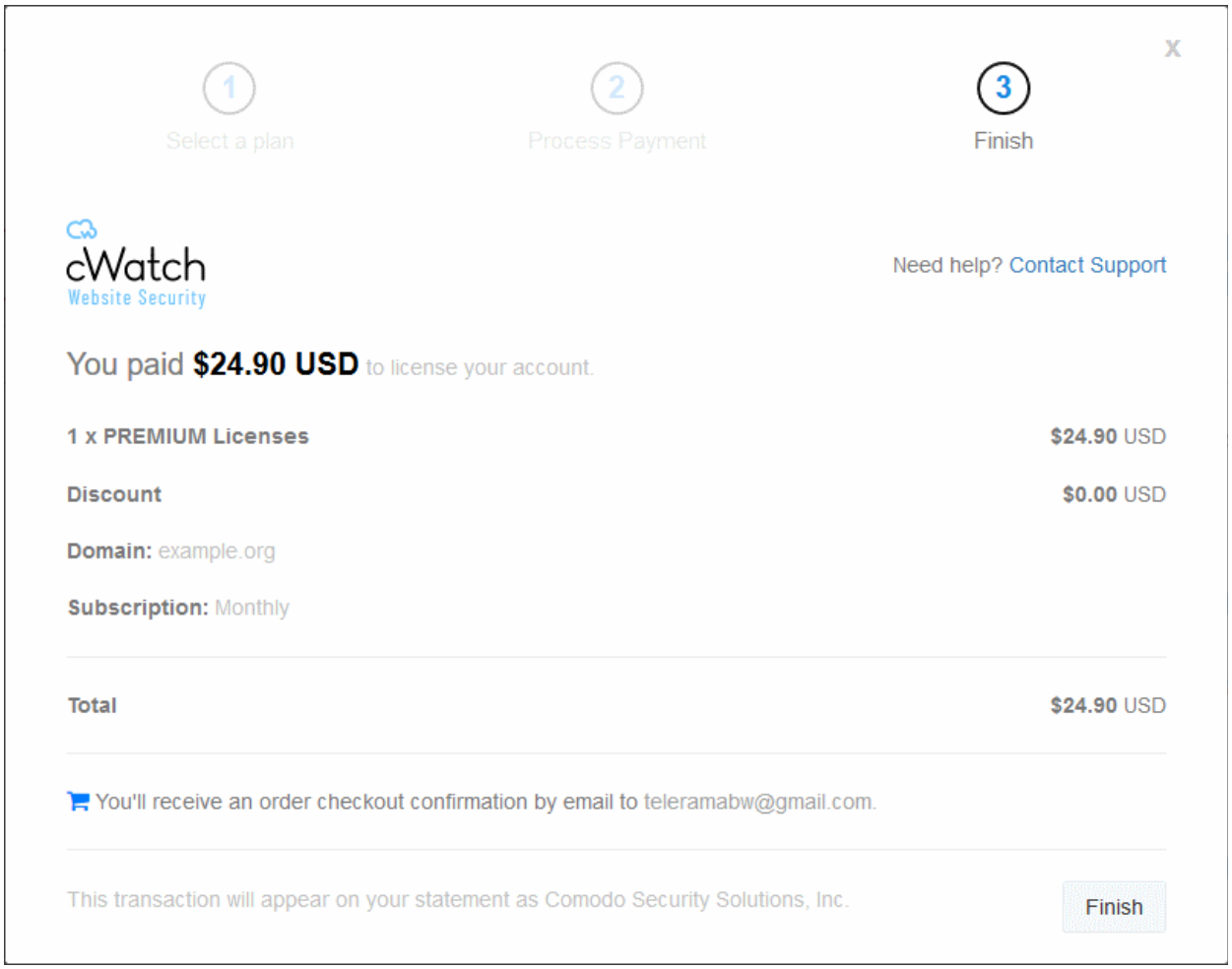
- If you do not have any licenses available then you will be taken to the license purchase page:



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



- Click 'Finish' at the payment confirmation screen:

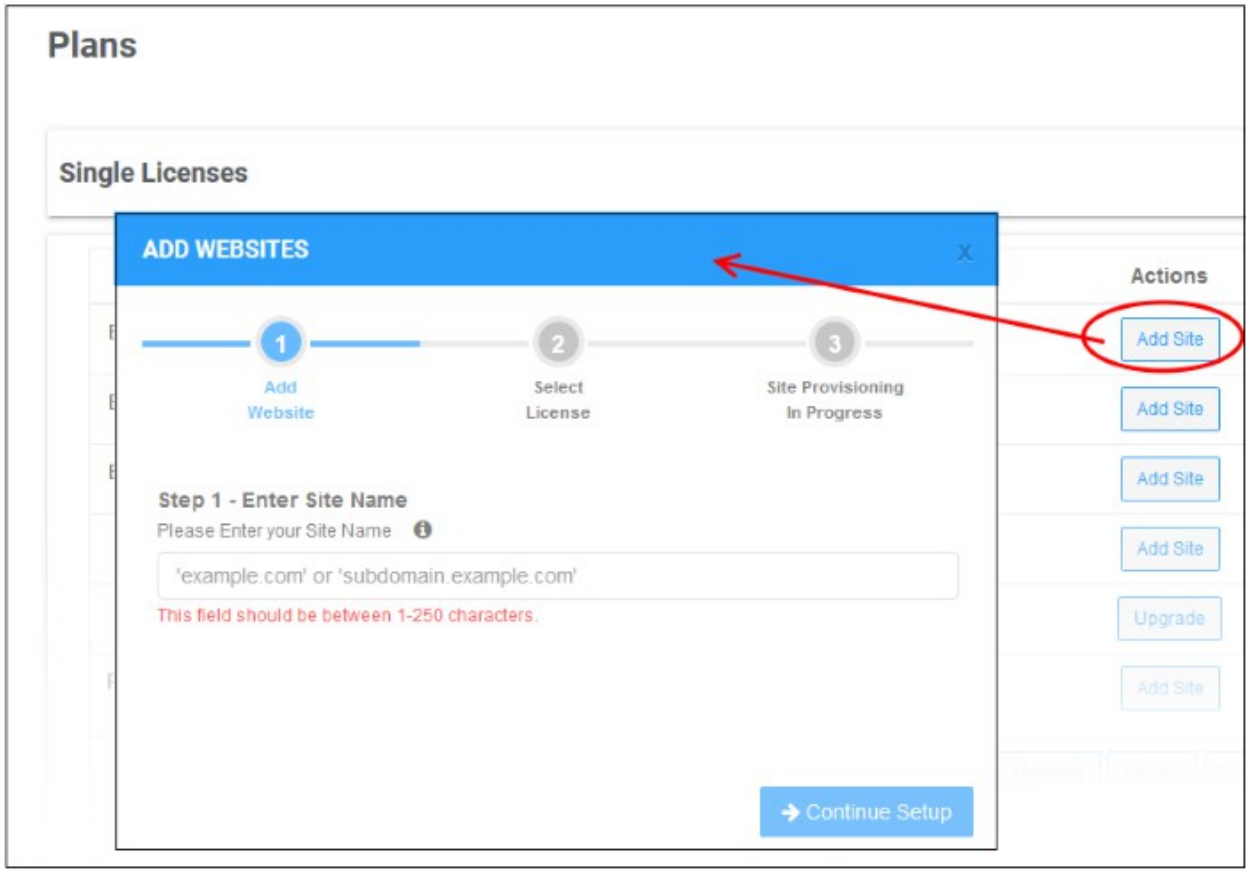


- You can now go back to the license upgrade process as described earlier.

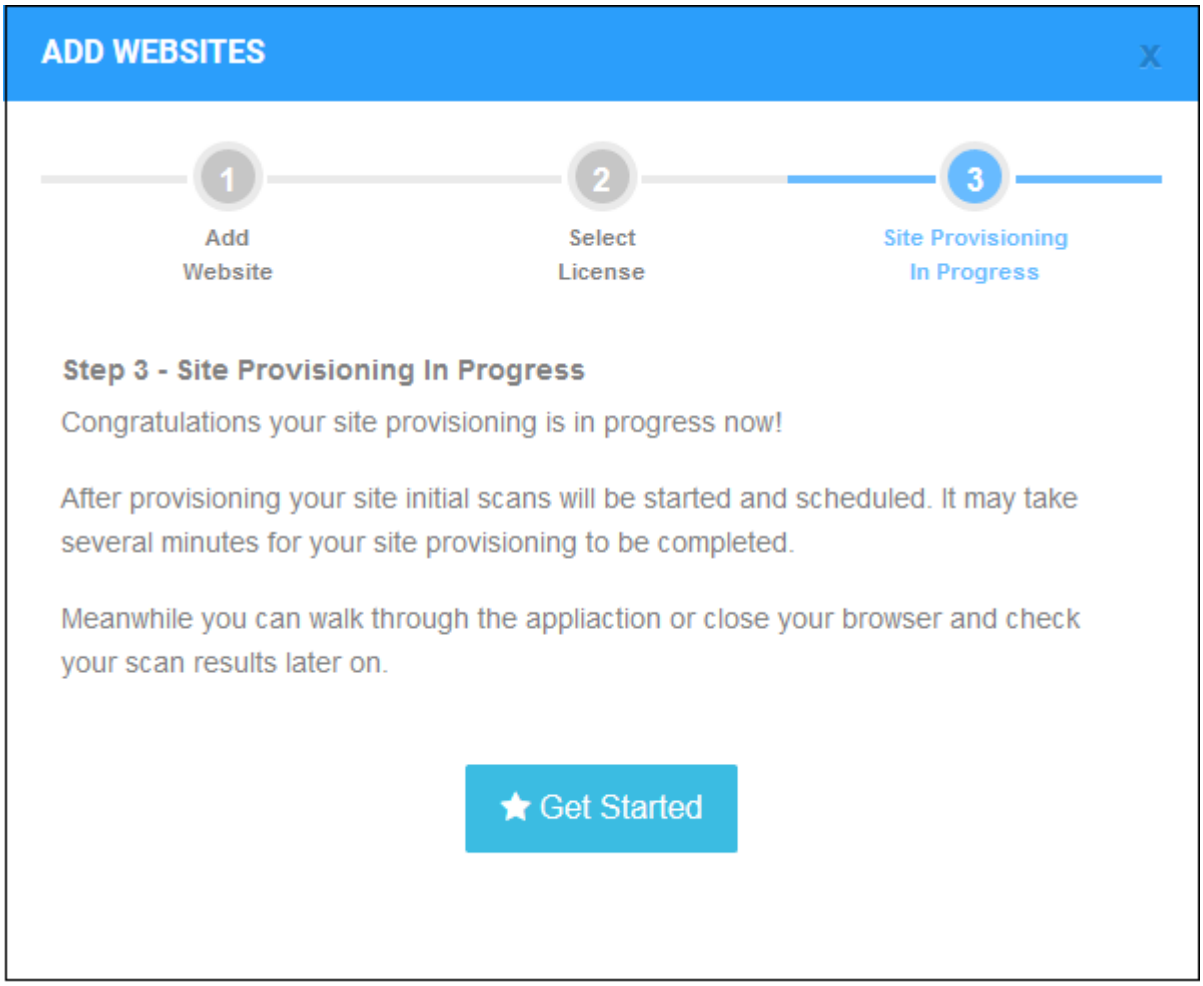
Add a new domain to an unused license

You can protect a new website by associating it with an existing license.

- Click the user icon at top-right
- 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:

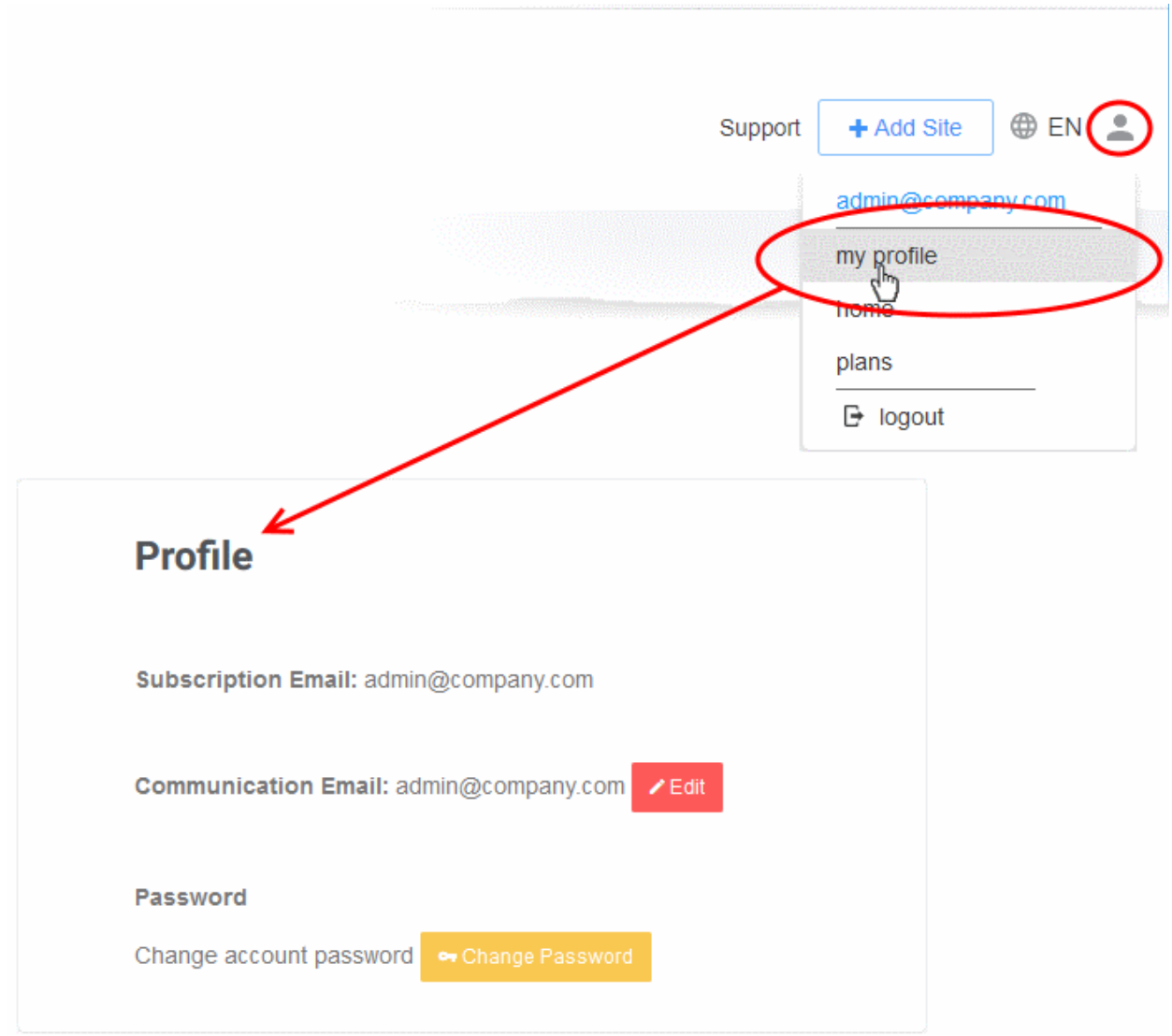
- Next up is to enable cWatch protection on the site.
- Click 'Get Started' to open the 'Overview' page for the site
- The overview page lets you configure malware and vulnerability scans, firewall rules, CDN settings, and more.
- This is covered in more detail in the **Website Overview** section.

6 Manage Your Profile

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

Manage your profile

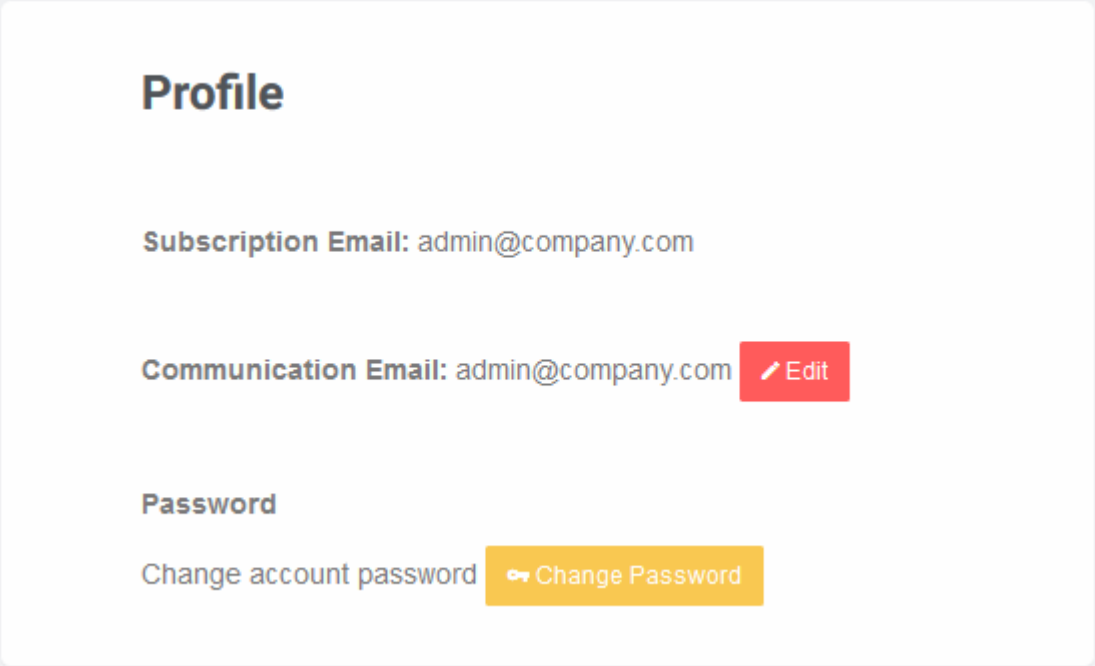
- Click the user icon at top-right
- Select 'My Profile' from the drop-down



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

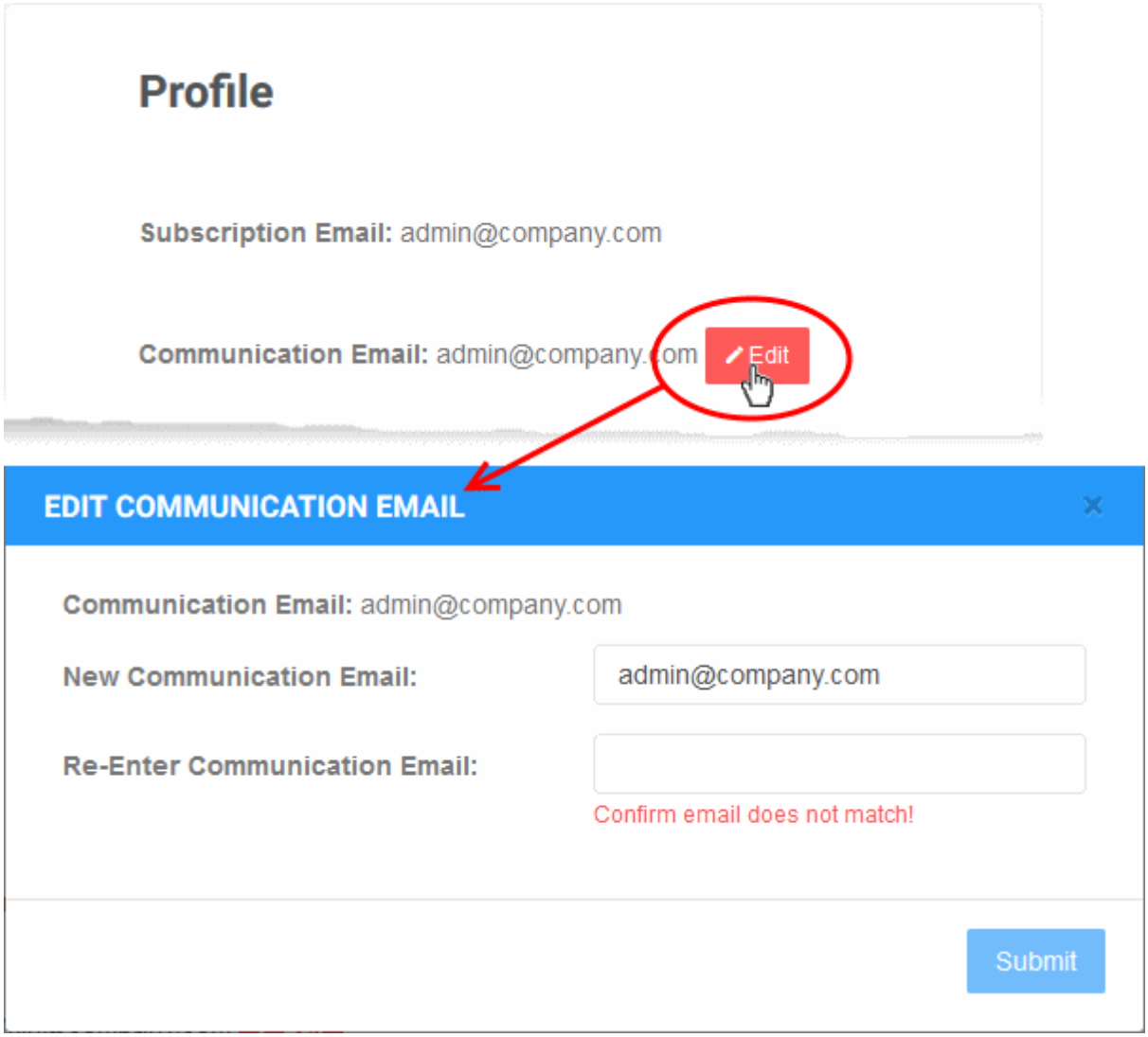
Edit your profile

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



- **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.

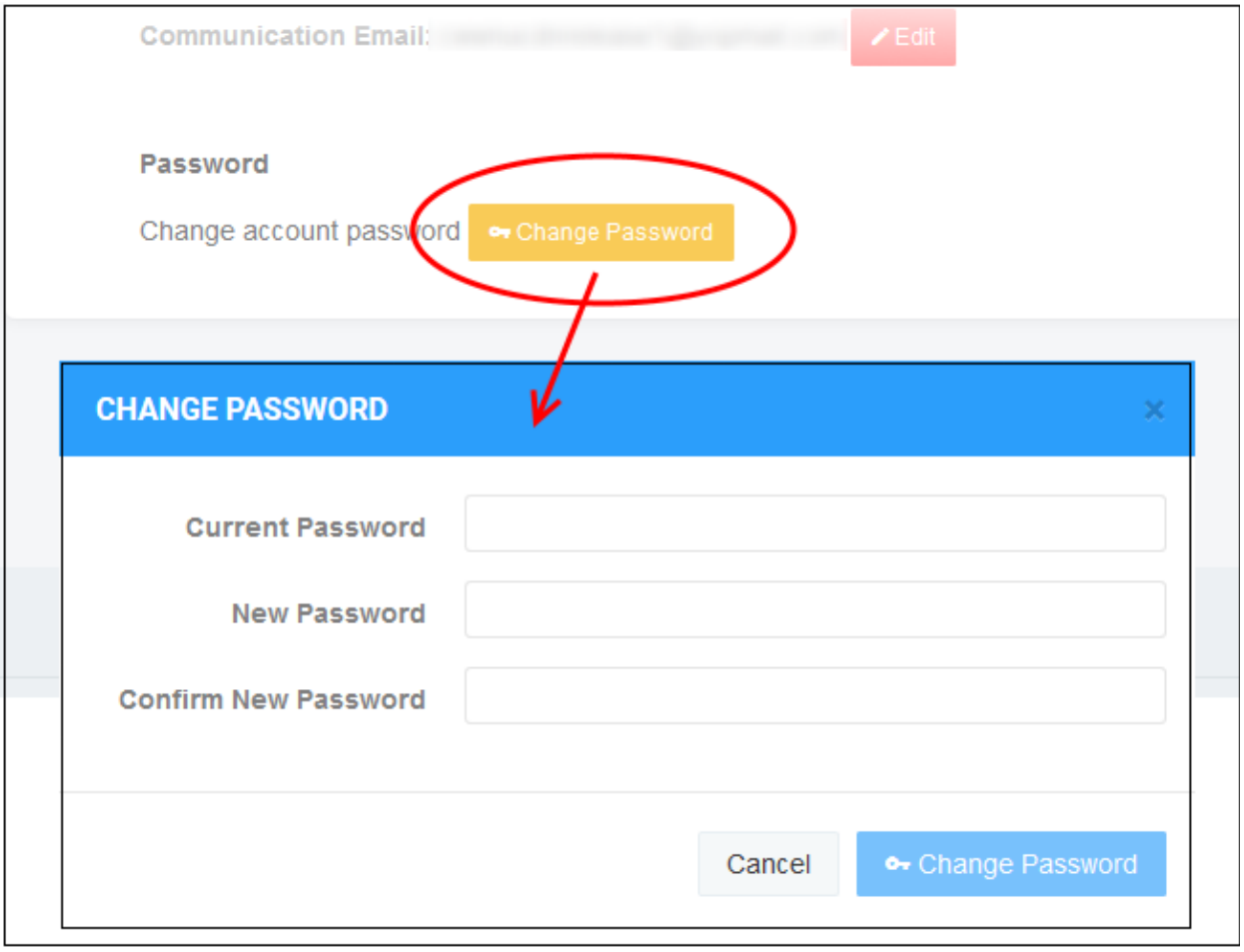
      You will get system emails for the following:
        - Account Creation
        - Purchase cWatch Web
        - Malware Found
        - When license is expired
        - When a license is distributed for the first time
        - When a license is distributed by partner
        - When license is expired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

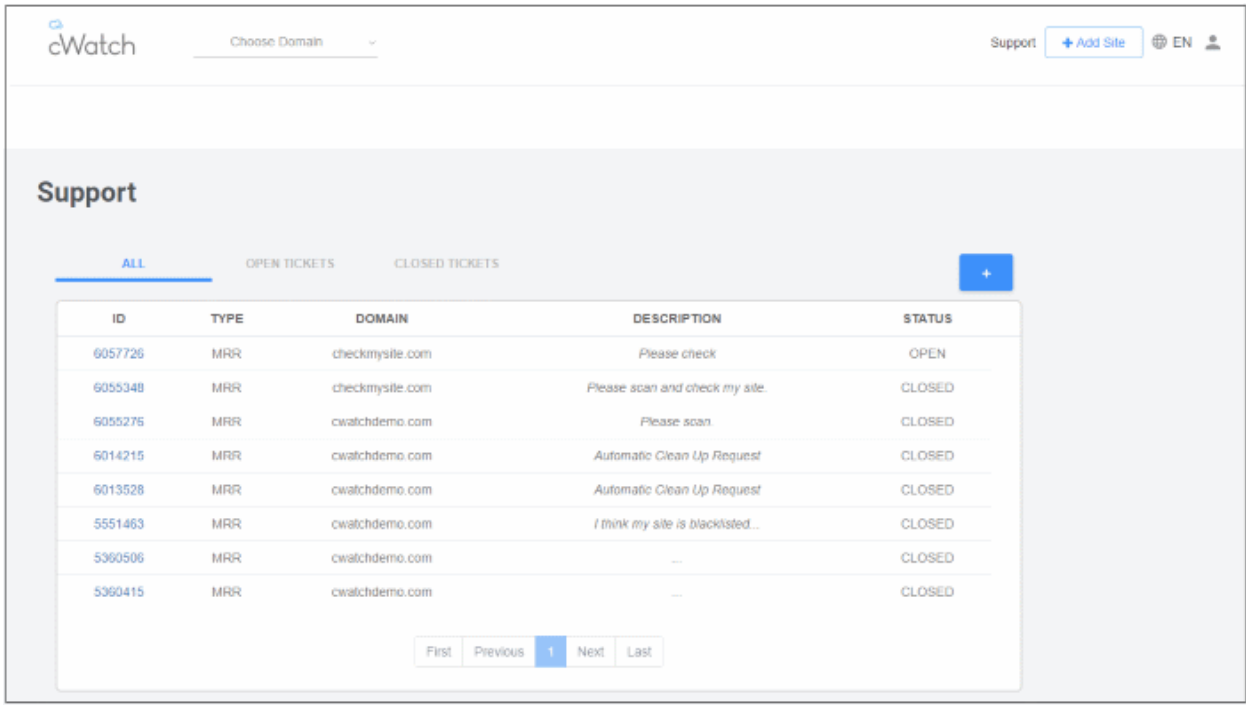


- Confirm your existing password and create a new password
- Click 'Change Password'

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

7 Get Support

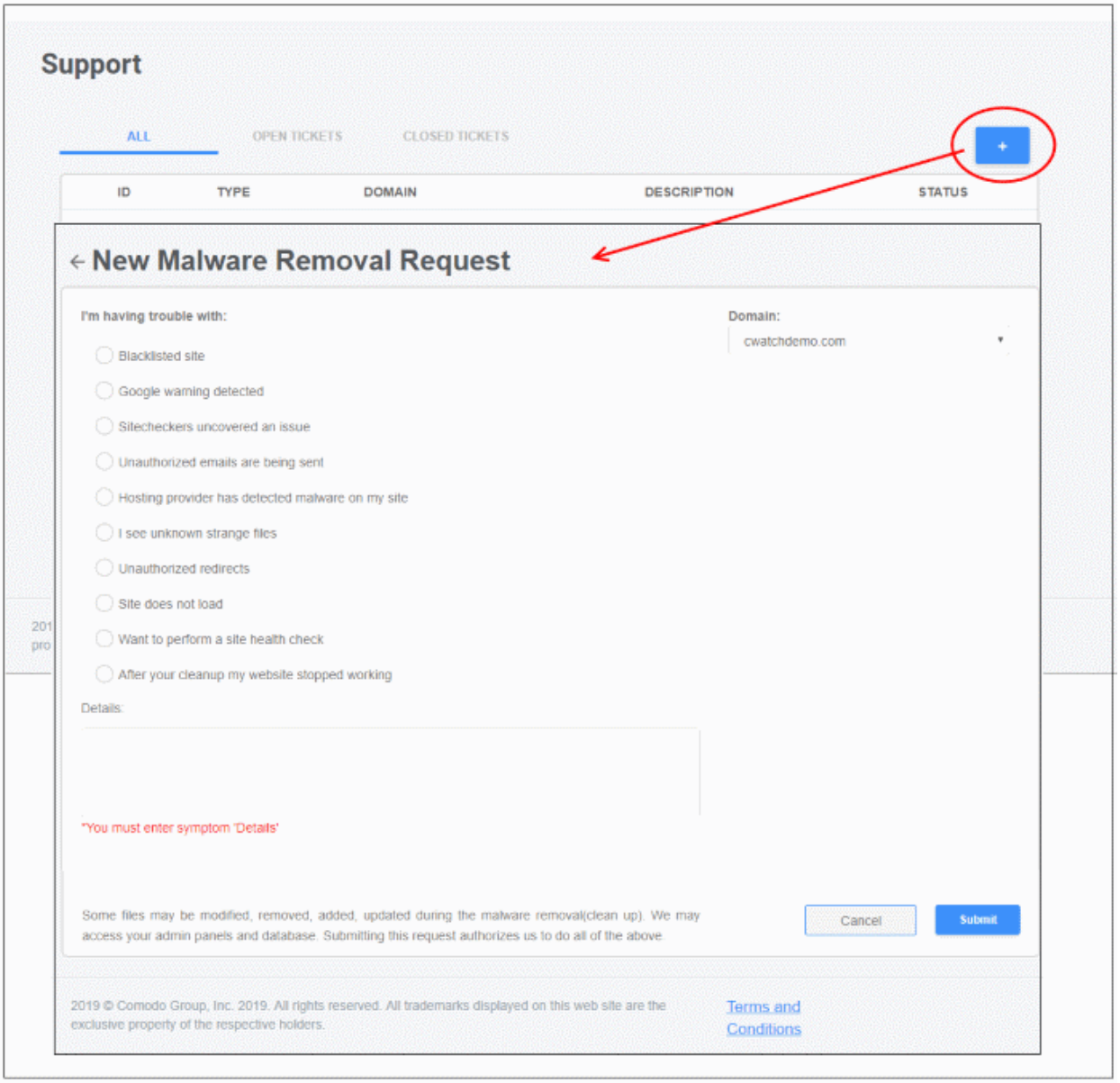
- The support page shows all malware clean-up requests you have submitted
- You can also create a new request from this interface
- Click 'Support' at top-right:



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

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

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



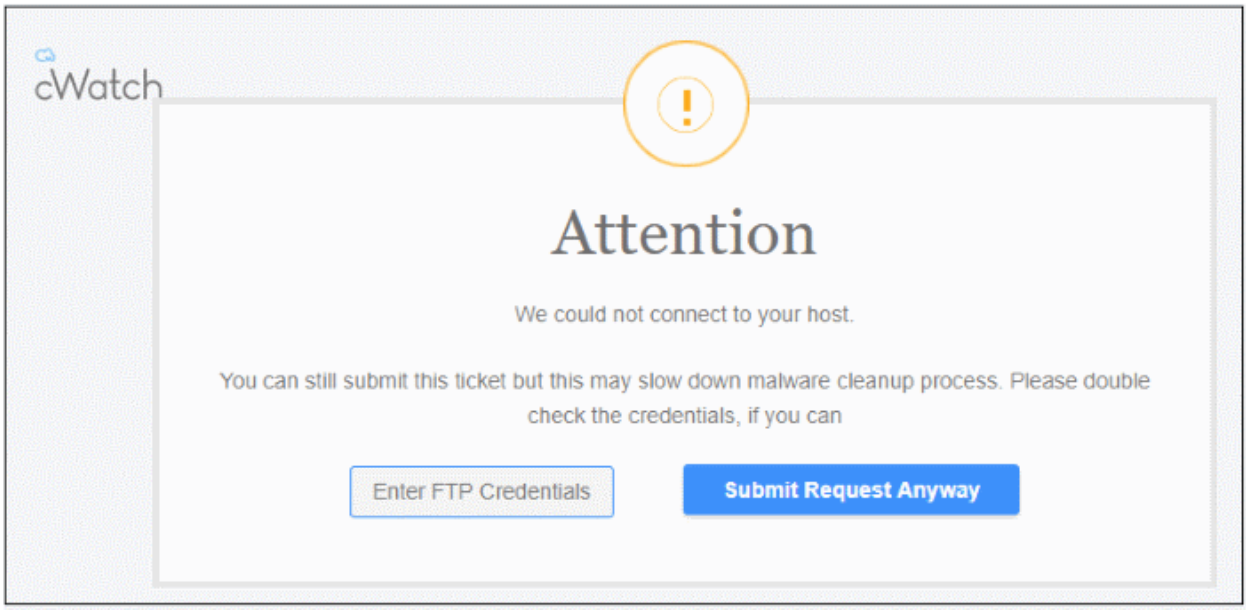
- **Domain** – Your websites will be listed in the drop-down. Select the website for which you want to create a ticket.
- Select the issue(s), provide short notes about the problem in the details box and click 'Submit'
- A ticket will created and listed in the table. Our technician will attend to the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

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

- Enter your site's FTP details and click 'Submit'

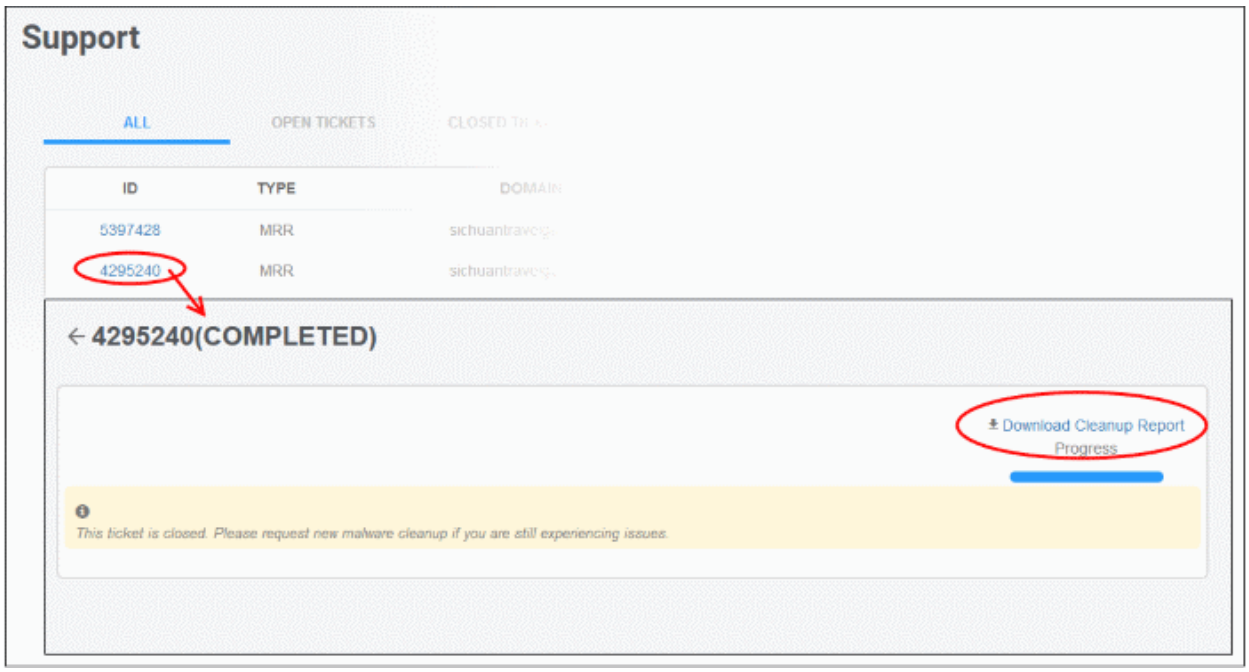
- You can configure the FTP settings in the malware page, or upload the agent manually. See '**Automatic Configuration**' and '**Manual Configuration**' for help with malware scanner configuration.

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



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

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



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

cWatch

Malware Cleanup report for [redacted]

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

Summary

The malware scan for your domain [redacted] was completed successfully and we found a total of **3** files to be suspicious in nature. The breakdown is as follows:

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

Details

Cured:

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

Deleted:

File Path	Action Taken
./.b601f3e7.ico	File deleted

Comment:

End of report

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

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

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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