

**COMODO**  
Creating Trust Online®



# Comodo cWatch Web Security

## cWatch Web - Plesk Extension Administrator Guide

Guide Version 1.0.011718

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

## Table of Contents

1 Introduction to cWatch Web for Plesk Extension.....	3
2 Install cWatch Extension.....	4
3 Advanced Configuration.....	7
3.1 FTP Settings.....	7
3.2 Log Settings.....	7
4 Manage Customers and Websites.....	8
4.1 Admin Interface.....	8
4.1.1 Basic Configuration.....	9
4.1.2 View Logs.....	10
4.2 Customer Interface.....	12
4.2.1 Activate / Upgrade Website License for a Customer.....	16
4.2.2 Scan and Clean customer websites.....	19
4.2.3 Login to a Customer Account and Manage their Websites.....	23
5 Uninstall cWatch Extension.....	26
6 Membership Plans.....	28
7 Manage your CAM Account.....	29
About Comodo Security Solutions.....	30

# 1 Introduction to cWatch Web for Plesk Extension

cWatch Web for Plesk lets partners and their customers enable 24/7 malware protection on licensed websites.

Home > Extensions

## cWatch

Configuration Logs

Show 10 entries Search:

Date	Command	Status	Action
2019-01-14 07:34:52	POST login	Success	Details
2019-01-14 06:53:42	GET domain/10385/settings/scanner	Success	Details
2019-01-14 06:53:41	GET domain/10384/settings/scanner	Success	Details
2019-01-14 06:53:41	GET domain/10385/malwareremoval?pageSize=100&pageNumber=1	Success	Details
2019-01-14 06:53:40	GET customer/site/listBySite?siteName=host01.cwwplesk.pp.ua&email=cwatchweb@gmail.com	Success	Details
2019-01-14 06:53:40	GET domain/10387/settings/scanner	Success	Details
2019-01-14 06:53:40	GET domain/10384/malwareremoval?pageSize=100&pageNumber=1	Success	Details
2019-01-14 06:53:39	GET customer/site/listBySite?siteName=cwwplesk.pp.ua&email=cwatchweb@gmail.com	Success	Details
2019-01-14 06:53:39	GET domain/10385/settings/scanner	Success	Details
2019-01-14 06:53:39	GET domain/10387/malwareremoval?pageSize=100&pageNumber=1	Success	Details

Showing 1 to 10 of 4,852 entries 1 2 3 4 5 ... 486

Clear All Logs

This guide explains how partners can add/configure the cWatch Plesk extension and manage customer websites.

## Guide Structure:

- [Introduction to cWatch Web for Plesk Extension](#)
- [Install cWatch Extension](#)
- [Advanced Configuration](#)
  - [FTP Settings](#)
  - [Log Settings](#)
- [Manage Customers and Websites](#)
  - [Admin Interface](#)
    - [Basic Configuration](#)
    - [View Logs](#)
  - [Customer Interface](#)
    - [Activate / Upgrade Website License for a Customer](#)
    - [Scan and Clean customer websites](#)
    - [Login to a Customer Account and Manage their Websites](#)
- [Uninstall cWatch Extension](#)

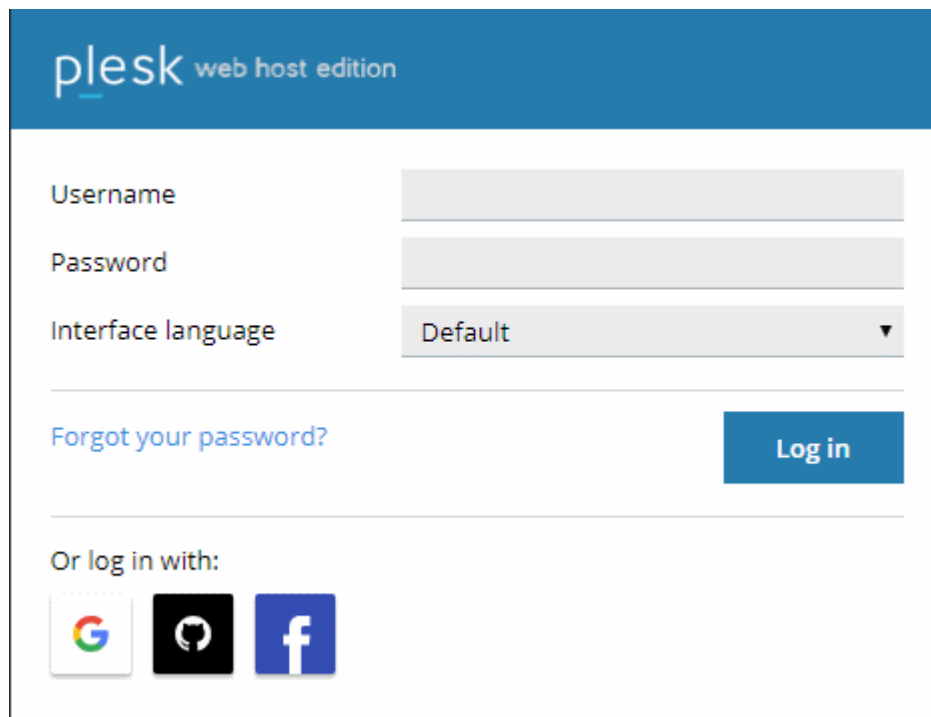
- [Membership Plans](#)
- [Manage your CAM Account](#)

## 2 Install cWatch Extension

**Prerequisite** - Save the cWatch zip file provided by our sales rep on the server running Plesk.

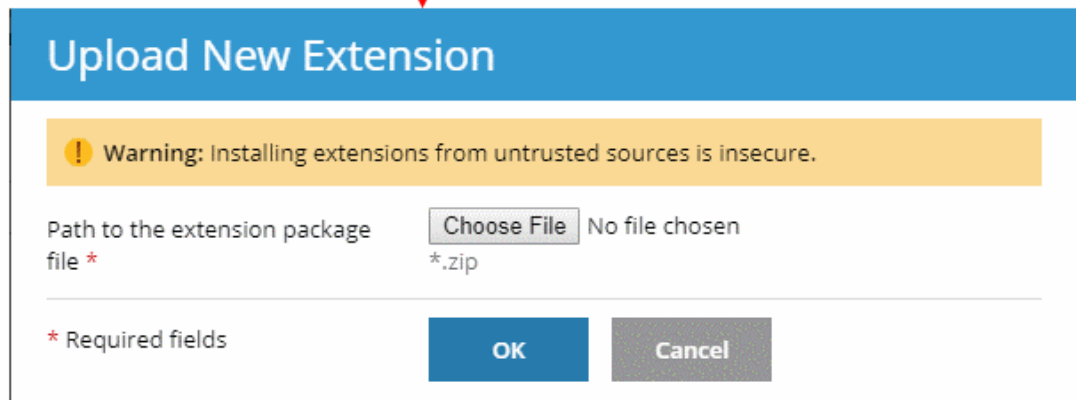
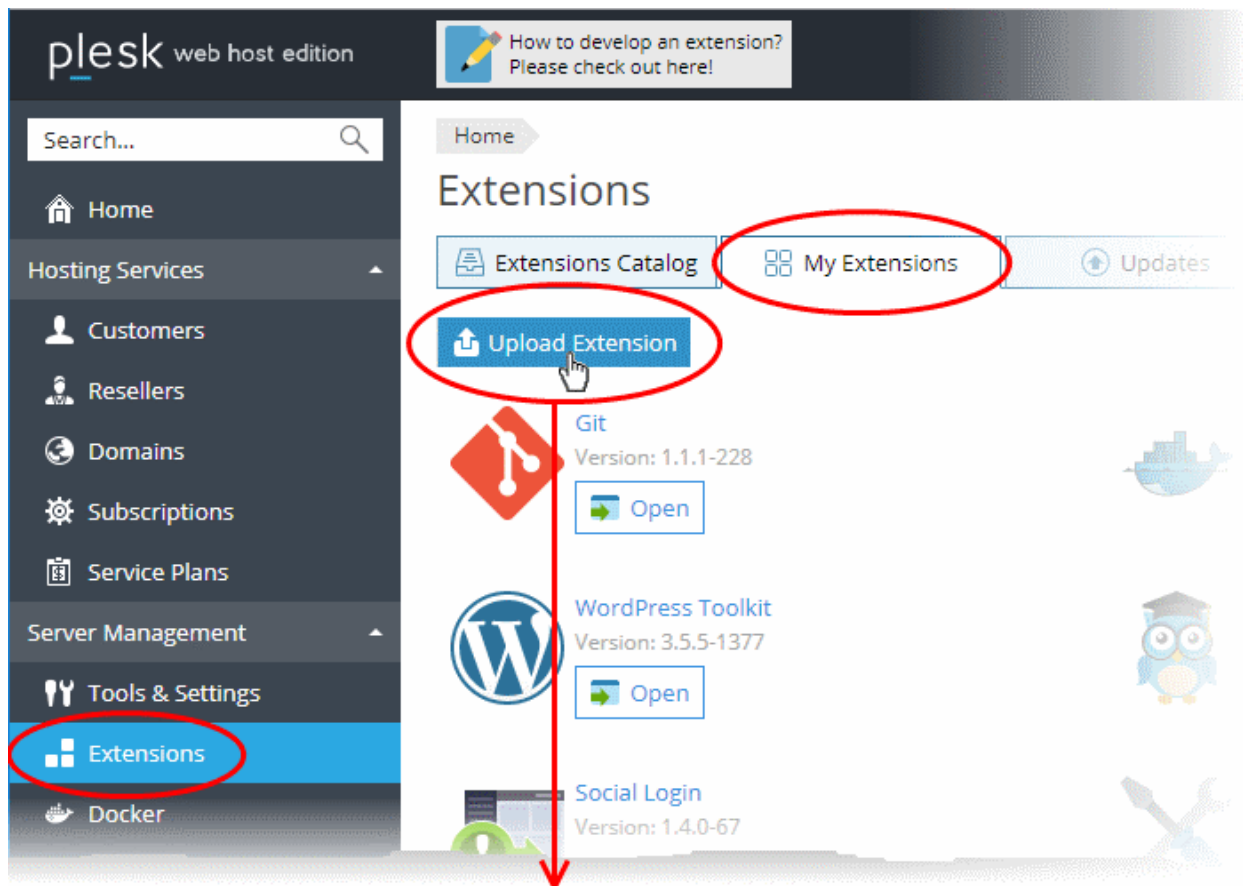
### Add the cWatch extension

- Login to your Plesk account

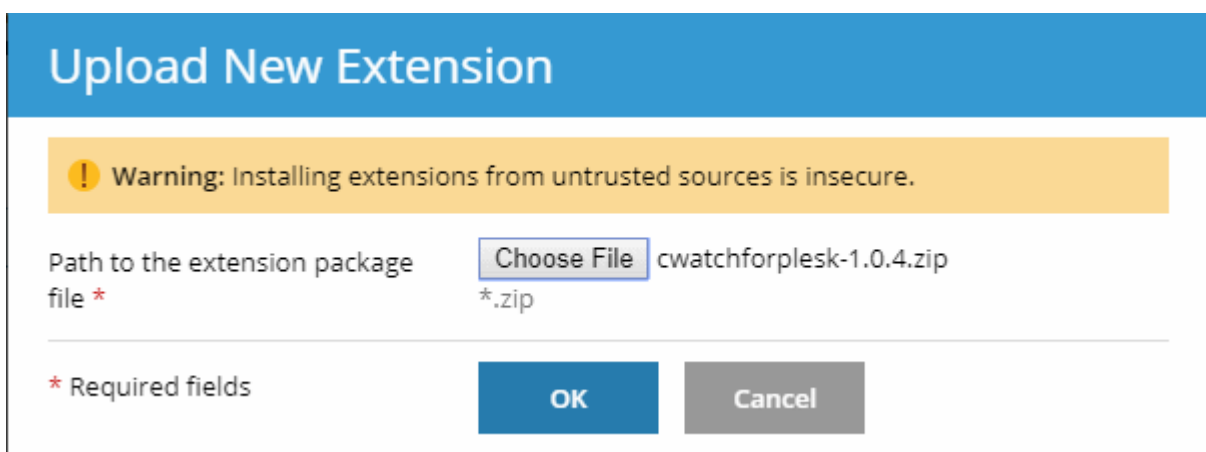


The screenshot shows the Plesk web host edition login interface. At the top, there is a blue header with the Plesk logo and the text 'web host edition'. Below the header, there are three input fields: 'Username', 'Password', and 'Interface language'. The 'Interface language' field is a dropdown menu currently set to 'Default'. Below these fields, there is a link for 'Forgot your password?' and a blue 'Log in' button. At the bottom, there is a section titled 'Or log in with:' with three social media icons: Google, GitHub, and Facebook.

- Click 'Extensions' under 'Server Management' on the left
- Select the 'My Extensions' tab
- Click the 'Upload Extension' button at top-left:



- Click 'Choose File' and browse to the cWatch for Plesk extension zip file



- Click 'OK'

The cWatch extension is now added to your Plesk control panel. The next step is to configure the extension to collect logs from your customer websites and run malware scans.

## Configure the cWatch extension

- Login to your Plesk account
- Click 'Extensions' on the left
- Select the 'My Extensions' tab

The extensions added to your Plesk control panel are shown as tiles.

- Click 'Open' in the cWatch tile

The screenshot displays the Plesk web host edition interface. On the left sidebar, the 'Extensions' menu item is highlighted and circled in red. The main content area shows the 'Extensions' page with the 'My Extensions' tab selected and circled in red. Below the tabs, there is an 'Upload Extension' button and a grid of extension tiles. The 'cWatch' tile (Version: 1.0.4-1) has its 'Open' button circled in red. A red arrow points from this button to the configuration page shown below. The configuration page for 'cWatch' has two tabs: 'Configuration' (selected) and 'Logs'. Under 'API Configuration', there are three input fields: 'Partner Portal API URL \*' (http://cwatchpartnerports), 'Partner Portal API Username \*' (admin@cwatchpartner.co), and 'Partner Portal API Password \*'. Below these fields are 'Save Changes' and 'Test Connection' buttons.

- Click the 'Configuration' tab (if it is not already open)
- Enter the URL and login credentials of your partner portal API implementation in the respective fields
- Click 'Test Connection' to check whether the extension can connect to your partner portal
- Click 'Save Changes'

The cWatch extension is now and will be available to your customers. The extension can fetch logs from your cWatch portal and run scans on the customer websites.

## 3 Advanced Configuration

- The cWatch plugin uses FTP connection through port 21 to scan websites and collect logs by default.
- If you are using SFTP or using FTP on a different port on the server on which Plesk is installed, you can change the configuration by editing the `.env` file on the server.
- This section explains how to configure FTP connection and log collection for the cWatch plugin.

See the following sections for more guidance

- [FTP Settings](#)
- [Log Settings](#)

### 3.1 FTP Settings

- The default FTP connection settings used by cWatch plugin is as follows:
  - `FTP_TYPE=FTP`
  - `FTP_PORT=21`

#### To reconfigure the FTP settings

- Open the following file on the server that runs Plesk:  
`/opt/psa/admin/plib/modules/cwatchforplesk/.env`
- Set FTP or SFTP connection type and port by editing the following lines:
  - `FTP_TYPE=FTP`
  - `FTP_PORT=21`
- Save the file

#### Note:

- cWatch plugin does not support FTPS connection.
- The plug-in may work incorrectly if FTP or SFTP are disabled.

### 3.2 Log Settings

- The cWatch plugin collects logs from the customer websites by default
- The logs can be viewed from the admin panel. See [View Logs](#) for more details.
- You can enable or disable log collection at any time by editing the `.env` file on the server.

#### To enable / disable logs

- Open the following file on the server that runs Plesk:

```
/opt/psa/admin/plib/modules/cwatchforplesk/.env
```

- Set the value (true/false) for 'CW\_DEBUG'
  - CW\_DEBUG=false - Logs are not collected
  - CW\_DEBUG=true - All events including API requests from the plugin and the responses from the API are saved.
- Save the file

## 4 Manage Customers and Websites

- The cWatch plugin lets you activate licenses for customers, initiate malware scans on customer websites and view logs.
- You can login to customer's cWatch account and access their cWatch customer portal. This is useful for troubleshooting and configuration.

cWatch extension has two interfaces:

- **Admin Interface** - Configure connection to your partner portal API and view logs. See **Admin Interface** for more details.
- **Customer Interface** - View customer websites, activate licenses, run malware scans on customer websites and more. See **Customer Interface** for more details

### 4.1 Admin Interface

The admin interface lets you configure connection parameters for cWatch plug-in to connect to your partner portal API and view logs of API requests from the plug-in and their responses.

#### To open the admin interface

- Login to your Plesk account
- Click 'Extensions' on the left
- Select the 'My Extensions' tab

The extensions added to your Plesk control panel are shown as tiles.

- Locate the cWatch tile and click 'Open'



The screenshot displays the Plesk Admin Interface. At the top left, it says 'plesk web host edition'. A notification bubble reads 'How to develop an extension? Please check out here!'. The user is logged in as 'Administrat...'. The left sidebar contains a search bar and a menu with items: Home, Hosting Services, Customers, Resellers, Domains, Subscriptions, Service Plans, Server Management, Tools & Settings, Extensions (highlighted), Docker, WordPress, My Profile, and Profile & Preferences. The main content area shows the 'cWatch' configuration page with two tabs: 'Configuration' (active) and 'Logs'. Under 'API Configuration', there are three fields: 'Partner Portal API URL \*' with value 'http://cwatchpartnerport...', 'Partner Portal API Username \*' with value 'admin@cwatchpartner.co', and 'Partner Portal API Password \*'. Below these fields are two buttons: 'Save Changes' (green) and 'Test Connection' (grey).

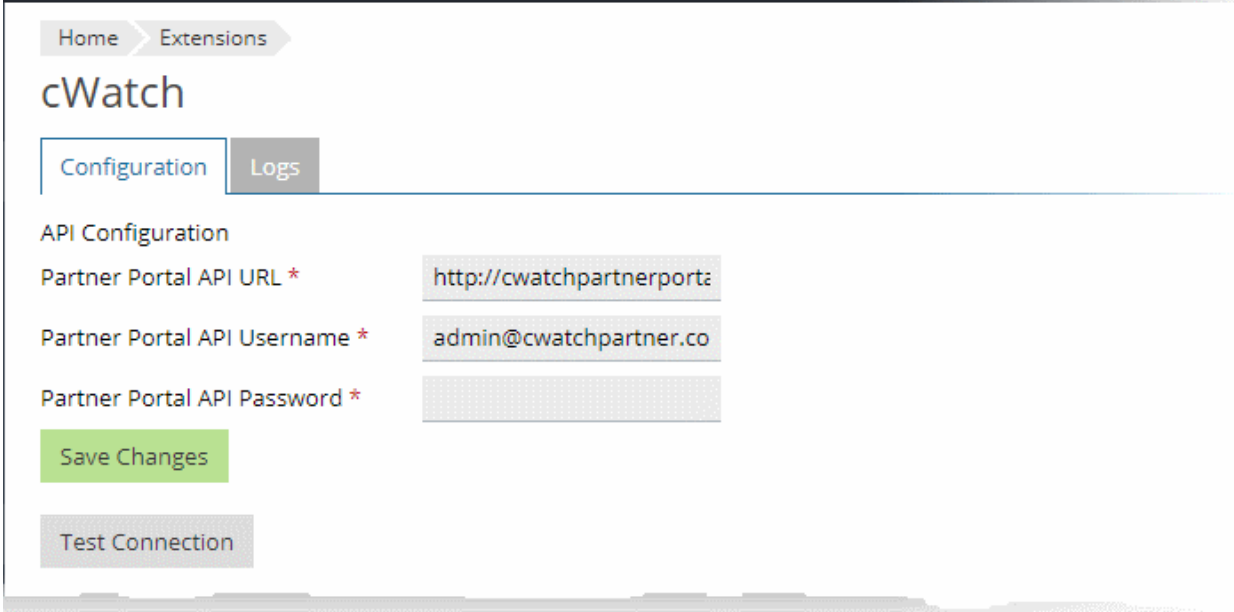
- The admin interface has two tabs:
  - **Configuration** - Set connection parameters
  - **Logs** - View API request logs

### 4.1.1 Basic Configuration

The 'Configuration' tab in the admin interface lets you re-configure the connection parameters for your cWatch partner portal API.

#### To view and modify the API connection parameters

- Click 'Extensions' on the left
- Select the 'My Extensions' tab
- Locate the cWatch tile and click 'Open'



The screenshot shows the 'cWatch' admin interface. At the top, there are navigation tabs for 'Home' and 'Extensions'. Below this, the 'cWatch' title is displayed. There are two main tabs: 'Configuration' (which is active) and 'Logs'. Under the 'Configuration' tab, the 'API Configuration' section is visible. It contains three input fields: 'Partner Portal API URL \*' with the value 'http://cwatchpartnerport:', 'Partner Portal API Username \*' with the value 'admin@cwatchpartner.co', and 'Partner Portal API Password \*' which is currently empty. Below these fields are two buttons: a green 'Save Changes' button and a grey 'Test Connection' button.

- Click the 'Configuration' tab (if it is not already opened):
- Edit the URL and login credentials of your partner portal API, if required.
- Click 'Test Connection' to check whether the extension could reach your partner portal API
- Click 'Save Changes'.

### 4.1.2 View Logs

The 'Logs' tab in the admin interface lets you view the logs of API requests made by the cWatch plug-in and the responses received from the API.

#### To view the logs

- Click 'Extensions' on the left
- Select the 'My Extensions' tab
- Locate the cWatch tile and click 'Open'
- Click the 'Logs' tab in the admin interface

Home > Extensions

## cWatch

Configuration | **Logs**

Show **10** entries Search:

Date	Command	Status	Action
2019-01-14 07:34:52	POST login	Success	<a href="#">Details</a>
2019-01-14 06:53:42	GET domain/10385/settings/scanner	Success	<a href="#">Details</a>
2019-01-14 06:53:41	GET domain/10384/settings/scanner	Success	<a href="#">Details</a>
2019-01-14 06:53:41	GET domain/10385/malwareremoval?pageSize=100&pageNumber=1	Success	<a href="#">Details</a>
2019-01-14 06:53:40	GET customer/site/listBySite?siteName=host01.cwwplesk.pp.ua&email=cwatchweb@gmail.com	Success	<a href="#">Details</a>
2019-01-14 06:53:40	GET domain/10387/settings/scanner	Success	<a href="#">Details</a>
2019-01-14 06:53:40	GET domain/10384/malwareremoval?pageSize=100&pageNumber=1	Success	<a href="#">Details</a>
2019-01-14 06:53:39	GET customer/site/listBySite?siteName=cwwplesk.pp.ua&email=cwatchweb@gmail.com	Success	<a href="#">Details</a>
2019-01-14 06:53:39	GET domain/10385/settings/scanner	Success	<a href="#">Details</a>
2019-01-14 06:53:39	GET domain/10387/malwareremoval?pageSize=100&pageNumber=1	Success	<a href="#">Details</a>

Showing 1 to 10 of 4,852 entries [1](#) [2](#) [3](#) [4](#) [5](#) ... [486](#)

[Clear All Logs](#)

- Click 'Details' in the row of a log entry to view its request and response details

2019-01-14 06:53:40 GET domain/10387/settings/scanner Success Details

2019-01-14 06:53:40 GET domain/10384/malwareremoval?pageSize=100&pageNumber=1 Success Details

2019-01-14 06:53:39 GET customer/site/listBySite?siteName=cwwplesk.pp.ua&email=cwatchweb@gmail.com Success Details

Configuration Logs

Back to Logs

Date

2019-01-14 06:53:40

Request

```
http://cwatchpartnerportalstaging-env.us-east-1.elasticbeanstalk.com/domain/10384/malwareremoval?pageSize=100&pageNumber=1
GET /domain/10384/malwareremoval?pageSize=100&pageNumber=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0
Host: cwatchpartnerportalstaging-env.us-east-1.elasticbeanstalk.com
accept: application/json
Content-Type: application/json
Content-Length: 0
Authorization: eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJtb2R1bGVzZ2FyZGVuQHVhcG1haWwY29tIiwiaXNhwIjoxNTQ3NTM1MjE0LCJyYWIjZCI6IktUnHhGZVWnSW
```

Response

```
{
  "currentPage": 1,
  "totalPages": 1,
  "summaries": [
    {
      "filesDetected": 2,
      "progress": 100,
      "othersCount": 0,
      "mrrId": "188172",
      "exploitCount": 0,
      "numberOfMalware": 2,
    }
  ]
}
```

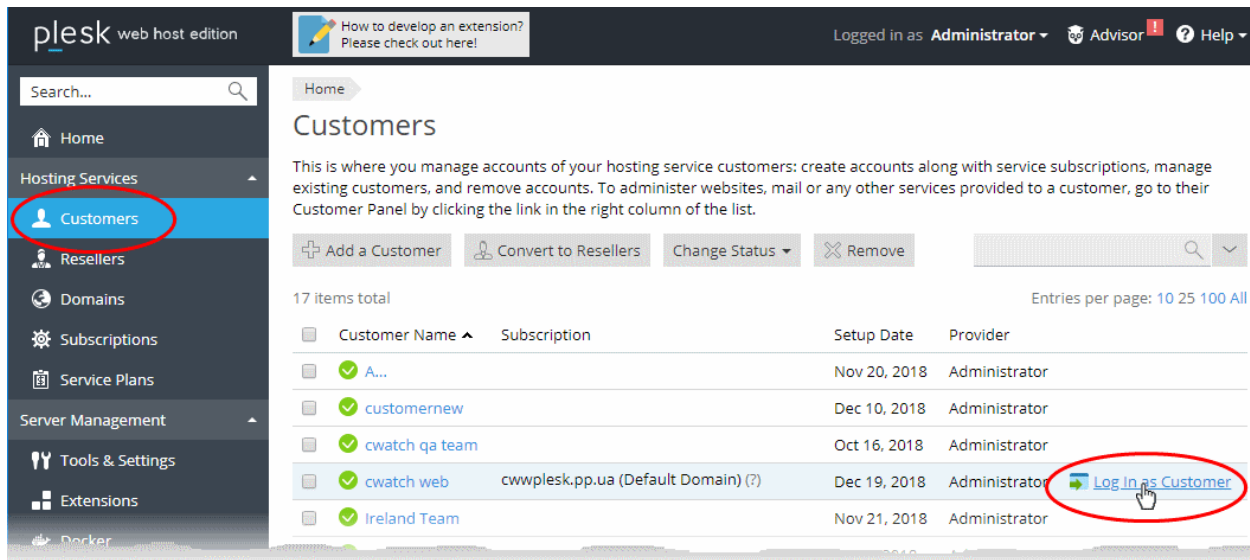
- Click 'Clear All' Logs to delete the log entries.

## 4.2 Customer Interface

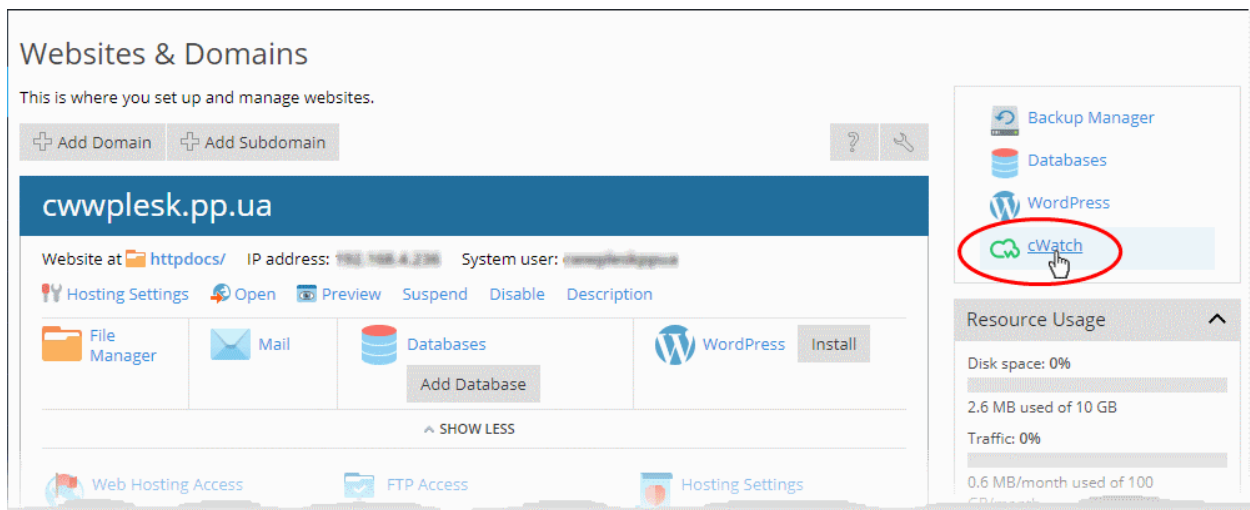
- The customer interface for a customer of cWatch plugin shows the websites associated with them
- You can activate or upgrade license for a website, initiate malware scans on websites and view the results
- You can also login to the cWatch customer portal and perform all management actions on customer sites. This includes malware scans, malware removal requests, custom firewall rules and more. See the cWatch admin guide at <https://help.comodo.com/topic-285-1-848-11000-Introduction-to-Comodo-cWatch-Web-Security.html> for detailed information on the products capabilities.

### To open the cWatch plugin customer interface

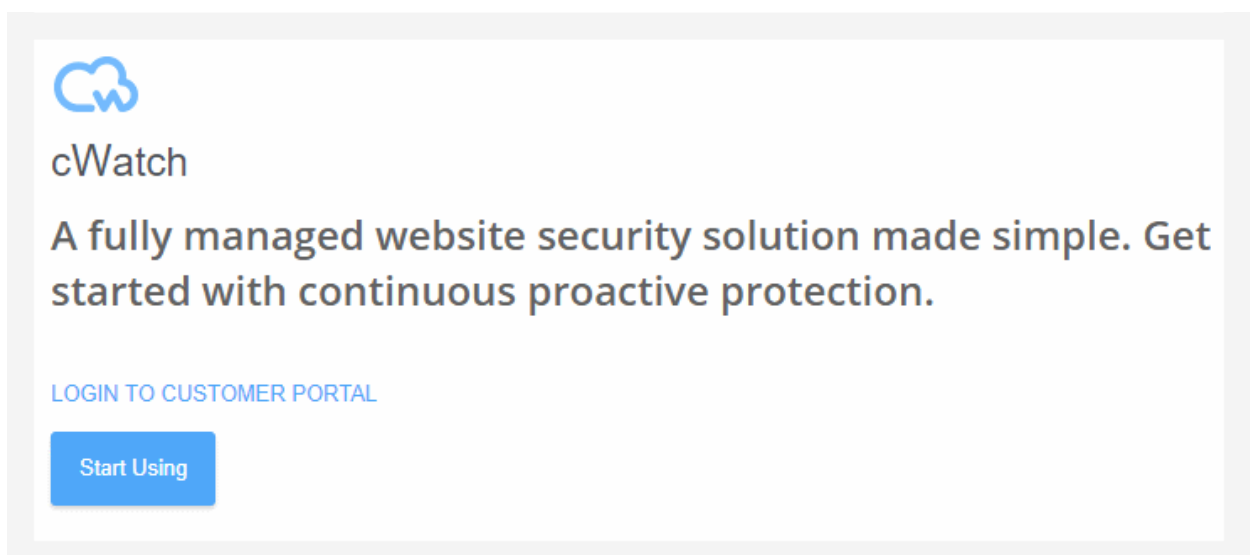
- Login to your Plesk account
- Click 'Customers' on the left to view the list of your customers
- Click 'Log In as Customer' at the for right, in the row of a customer



The Plesk customer panel opens:

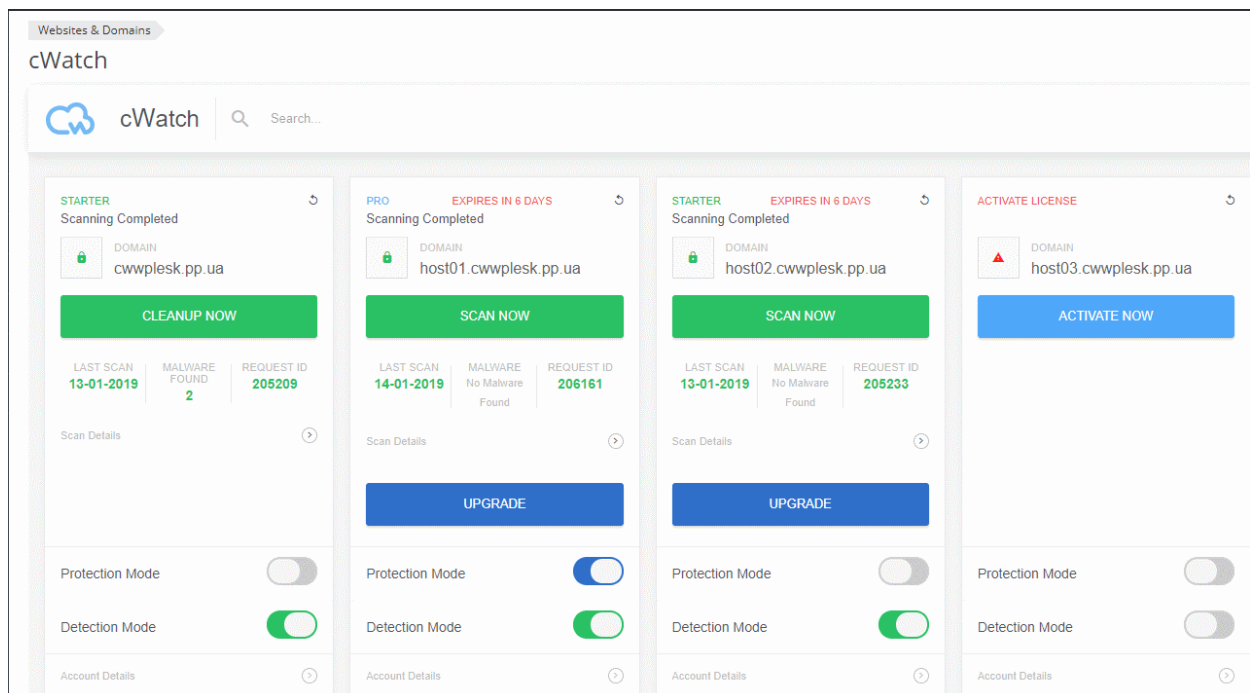


- Click the 'cWatch' link from the list of enabled services on the top-right
- If this is the first time you are opening the customer interface, you will be shown a dialog indicating the account setup.



- Click 'Start Using'

The cWatch customer interface opens:



Each customer website is shown as a tile.

The screenshot shows a web security tile with the following elements:

- License status: **PRO** (blue text), **EXPIRES IN 6 DAYS** (red text), and a refresh icon.
- Status: **Scanning Completed**.
- Domain: **host01.cwwplesk.pp.ua** (next to a lock icon).
- Action: **SCAN NOW** (green button).
- Scan Summary Table:

LAST SCAN	MALWARE	REQUEST ID
<b>14-01-2019</b>	No Malware Found	<b>206161</b>
- Section: **Scan Details** (with a right arrow icon).
- Action: **UPGRADE** (blue button).
- Protection Mode:  (blue toggle).
- Detection Mode:  (green toggle).
- Section: **Account Details** (with a right arrow icon).

The tile displays the license activated for the website, last scan time, the results of the last scan and more. The tile allows you to:

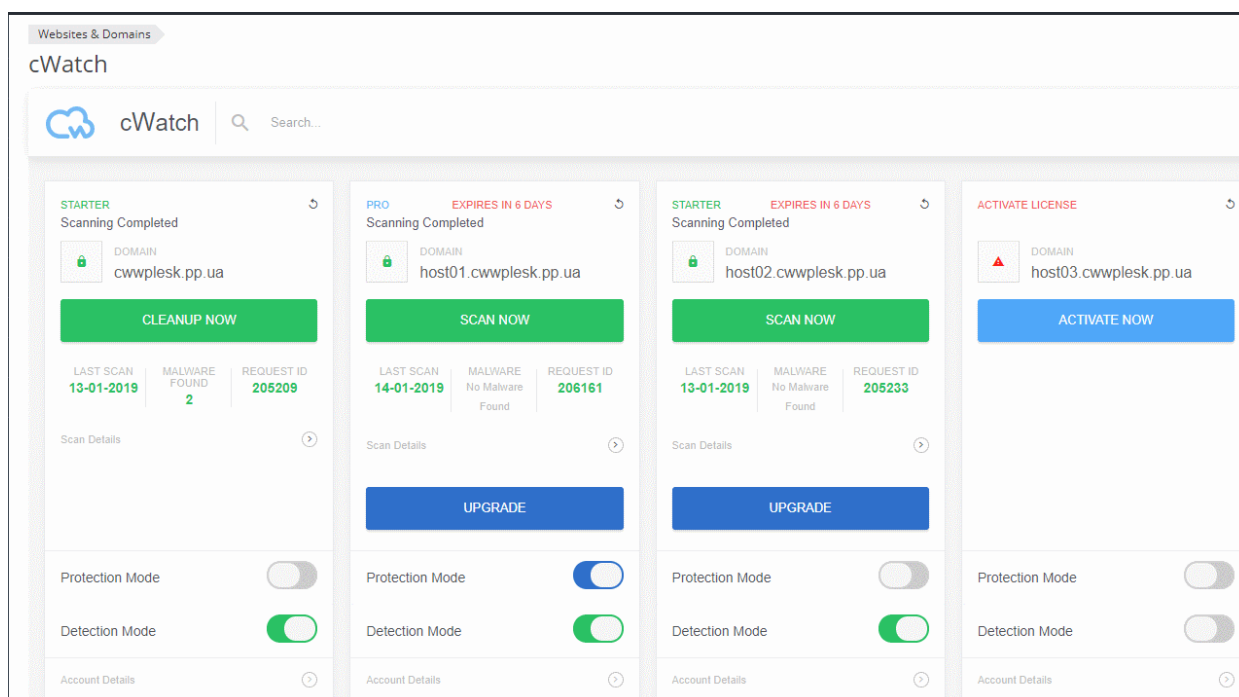
- **Activate a new license/Upgrade the license for the website**
- **Run manual malware scan on the website**
- **Login to a Customer Account and Manage their Websites**

## 4.2.1 Activate / Upgrade Website License for a Customer

- This section explains how you can activate or upgrade a license for a customer website
- You should have first distributed paid and trial licenses to customers. Only unused licenses will be available for selection when associating a license to a website.
  - See <http://help.comodo.com/topic-285-1-927-12634-distribute-and-manage-licenses.html> for help to distribute licenses from the cWatch partner portal.
- If no licenses are possessed by the customer, you will be directed to the license purchase page.

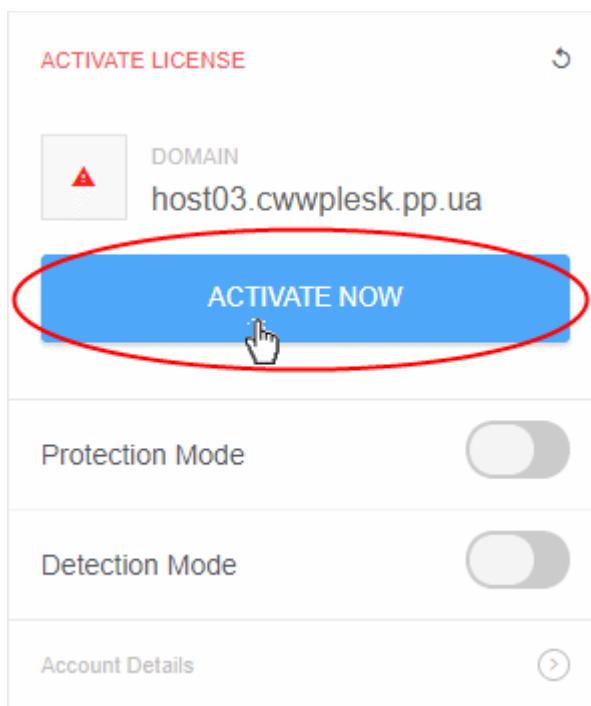
### To activate license for a website

- Login to your Plesk account
- Click 'Customers' on the left to view a list of your customers
- Click 'Log In as Customer' in a customer row
- Click the 'cWatch' link in the list of enabled services (top-right) to open the customer interface

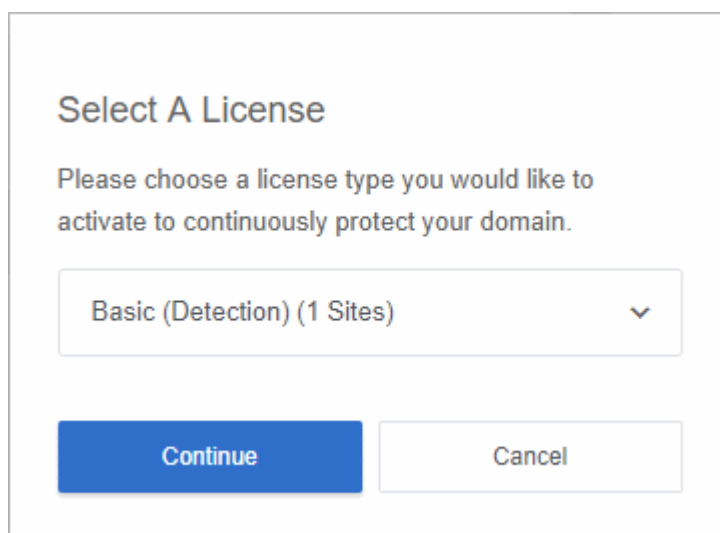


- Click 'Activate Now' on a website tile to associate a license with the site

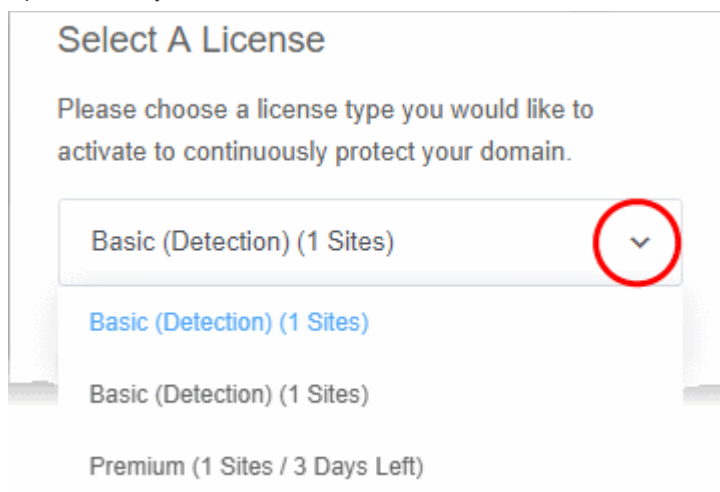




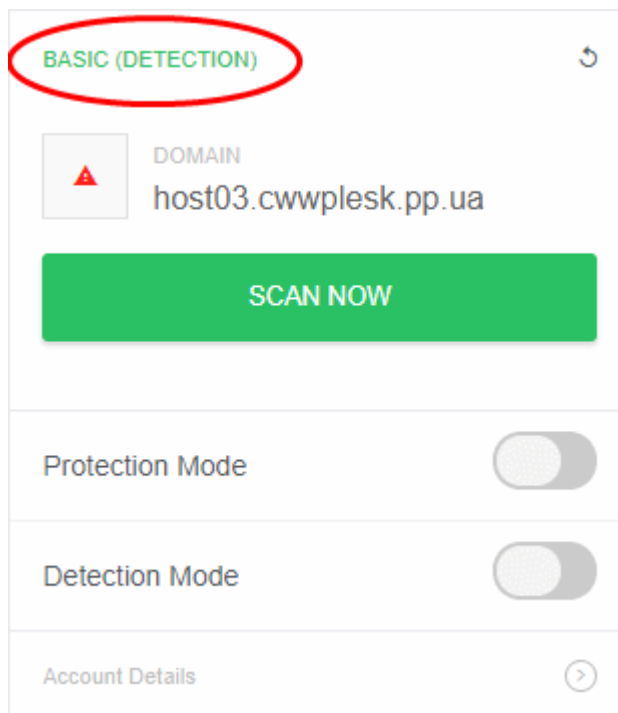
- Choose the type of license you want to activate on the site.



- cWatch features vary according to license type. See **Membership Plans** for more details.
- The drop-down lets you select available licenses for the customer:



- Choose the type of license you want to associate with the site then click 'Continue'
- The license you applied is shown at the top-left corner of the site tile:



You can now set the security mode, run scans on the site and more.

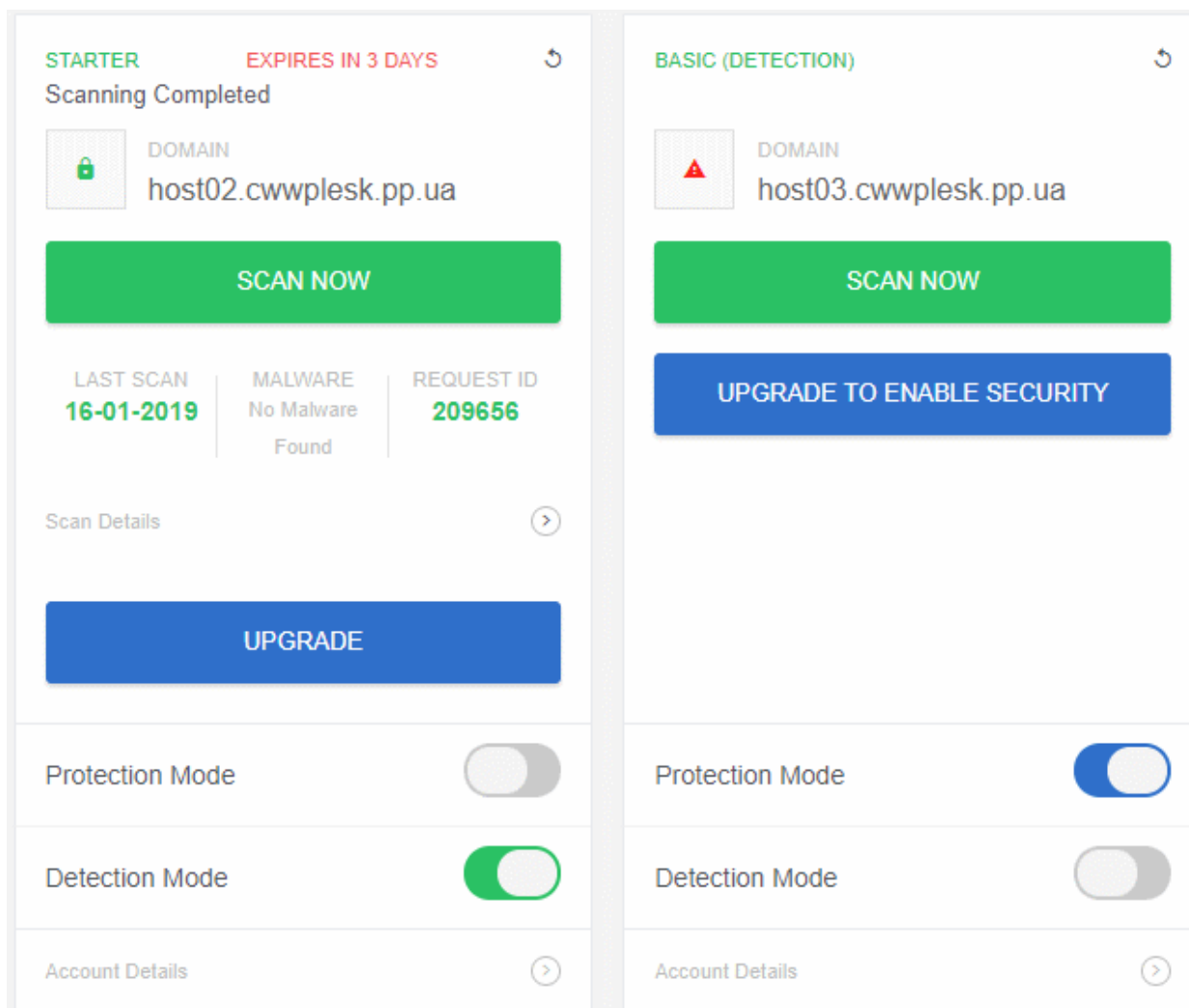
- **Detection Mode** - Enables all features found in the 'Starter' license type. Detection mode is available to Starter, Pro or Premium license types.
- **Protection Mode** - Enables all features found in the Pro or Premium license type, depending on the type of license applied to the site. Protection mode is only available to Pro or Premium license types.
  - See **Membership Plans** for features / services covered by different license types

### Upgrade license on a site

- You can upgrade the license on customer website at anytime to improve its protection levels. For example, if you want to enable protection mode or detection mode on a site.
- A free basic license can be upgraded to a paid 'Starter', 'Pro' or 'Premium' license.
- See **Membership Plans** for more details on features on each license.

### Upgrade a license

- Open the cWatch customer interface as described **above**
- Click 'Upgrade' or 'Upgrade to Enable Security' in a website tile



- You will be taken to the license purchase page set in your cWatch partner portal.
- See <http://help.comodo.com/topic-285-1-927-13698-Set-License-Purchase-Links.html> for help to set up a license purchase page.

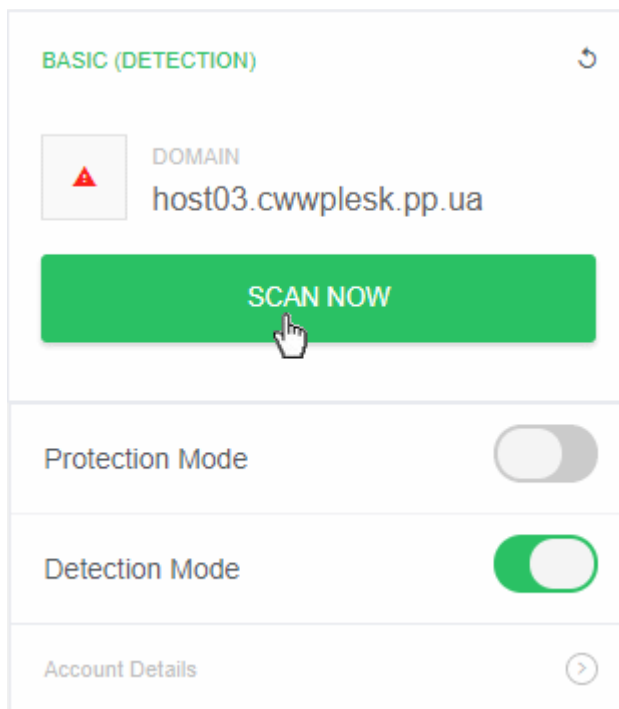
## 4.2.2 Scan and Clean customer websites

You can run on-demand malware scans on websites and clean malware identified (if any) from the customer interface of cWatch extension.

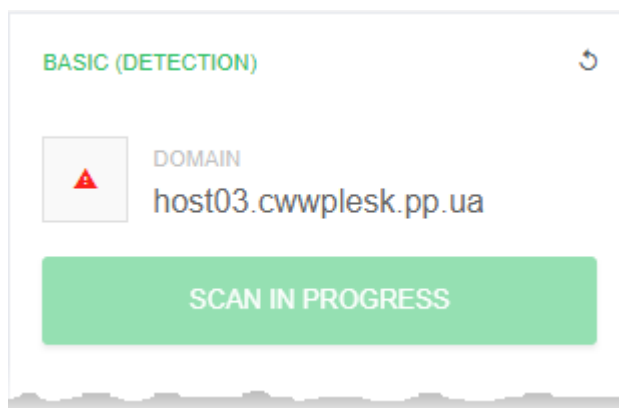
### To run a scan

- Login to your Plesk account
- Click 'Customers' on the left to view the list of your customers
- Click 'Log In as Customer' at the for right, in the row of a customer
- Click the 'cWatch' link from the list of enabled services on the top-right to open the cWatch web extension customer interface

The websites added for the customer account are shown as tiles.



- Click 'Scan Now' in the tile of the website to be scanned.
- The scanning progress is shown:



- On completion, the scan summary is shown:

The screenshot displays the 'BASIC (DETECTION)' section of the cWatch Web - Plesk Extension admin interface. At the top, there is a refresh icon. Below it, a lock icon is next to the domain 'host03.cwwplesk.pp.ua'. A prominent green button labeled 'CLEANUP NOW' is positioned below the domain. A summary table shows the following data:

LAST SCAN	MALWARE FOUND	REQUEST ID
17-01-2019	2	210448

Below the table, there are three expandable sections: 'Scan Details' with a right-pointing arrow, 'Protection Mode' with a grey toggle switch, and 'Detection Mode' with a green toggle switch. At the bottom, there is an 'Account Details' section with a right-pointing arrow.

- The number of malware files, if identified, is shown in the 'Malware Found' column
- Click 'Scan Details' to view the scan results and the history of scans:

**BASIC (DETECTION)** ↻

DOMAIN

host03.cwwplesk.pp.ua

CLEANUP NOW

LAST SCAN

**17-01-2019**

MALWARE FOUND

**2**

REQUEST ID

**210448**

Scan Details

>

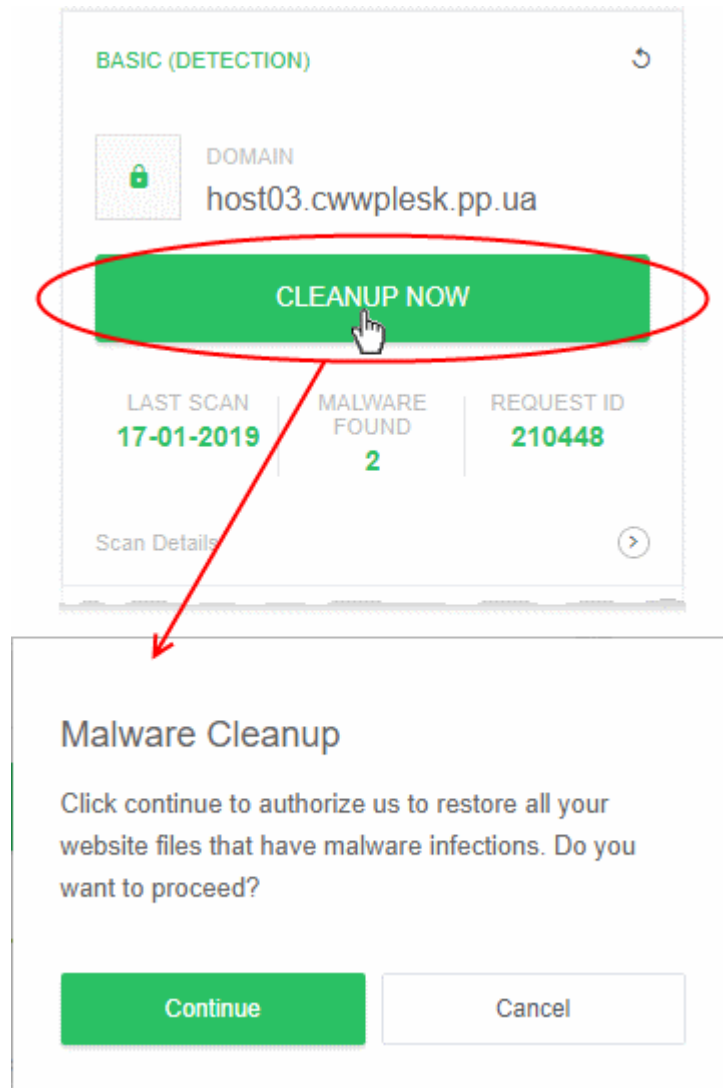
SCAN HISTORY FOR < HOST03.CWWPLESK.PP.UA >

	FILE PATH	FILE VERDICT	SHA1	STATUS
←	//5TrojWare.5269-10665c.php	TrojWare.5269	984a14e0209c63dc77d4112075215dcb2482ed70	Detected
	//7TrojWare.5269-10665a.php	TrojWare.5269	82d0b80943f4f50020056c42be920688cdea5c22	Detected

**SCAN SUMMARIES**

19-12-2018 12:46:40	19-12-2018 12:56:08	19-12-2018 12:57:58	19-12-2018 13:00:55	19-12-2018 13:08:13	19-12-2018 13:18:34
19-12-2018 13:22:32	19-12-2018 13:23:37	19-12-2018 13:25:52	19-12-2018 13:34:58	19-12-2018 13:52:36	19-12-2018 14:04:33
20-12-2018 16:53:26	21-12-2018 16:33:34	22-12-2018 16:33:22	23-12-2018 16:33:28	24-12-2018 16:33:15	25-12-2018 16:33:22
26-12-2018 16:23:32	27-12-2018 16:23:24	28-12-2018 16:23:26	29-12-2018 16:23:34	30-12-2018 16:23:32	31-12-2018 16:23:34
01-01-2019 16:23:16	02-01-2019 16:23:17	03-01-2019 16:23:28	04-01-2019 16:13:29	05-01-2019 16:13:30	06-01-2019 16:13:36
07-01-2019 16:13:21	08-01-2019 16:13:17	09-01-2019 16:03:36	10-01-2019 16:03:19	11-01-2019 15:53:34	12-01-2019 15:53:26
13-01-2019 15:53:28	14-01-2019 16:03:33	15-01-2019 16:03:32	16-01-2019 15:53:34		

- Scan History - The list of malware files identified in the last scan is shown.
- Scan Summaries - The previous scans run on the website with date and time stamp
  - Red - Malware identified
  - Green - No malware identified
  - Click a time/date stamp to view the list of malware identified during the respective scan
- Click 'Cleanup Now' to remove the malware identified during the latest scan.



- Click 'Continue' in the confirmation dialog to proceed with the malware clean-up

The malware will be removed from the website

### 4.2.3 Login to a Customer Account and Manage their Websites

The customer interface area lets you login to a customer's portal and manage their websites. This is useful for troubleshooting and configuration.

Login to the customer portal:

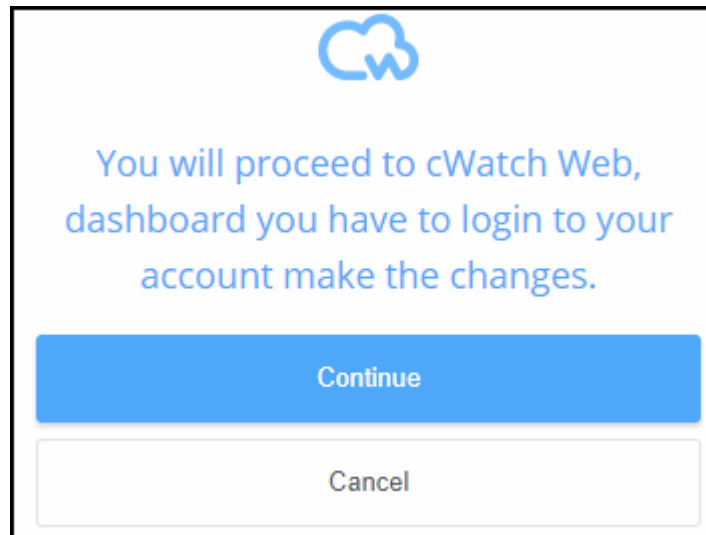
- Login to your Plesk account
- Click 'Customers' on the left to view a list of your customers
- Click 'Log In as Customer' at the right of a customer row
- Click the 'cWatch' link in the list of enabled services at top-right.

Each site on the customer account is shown as a separate tile:

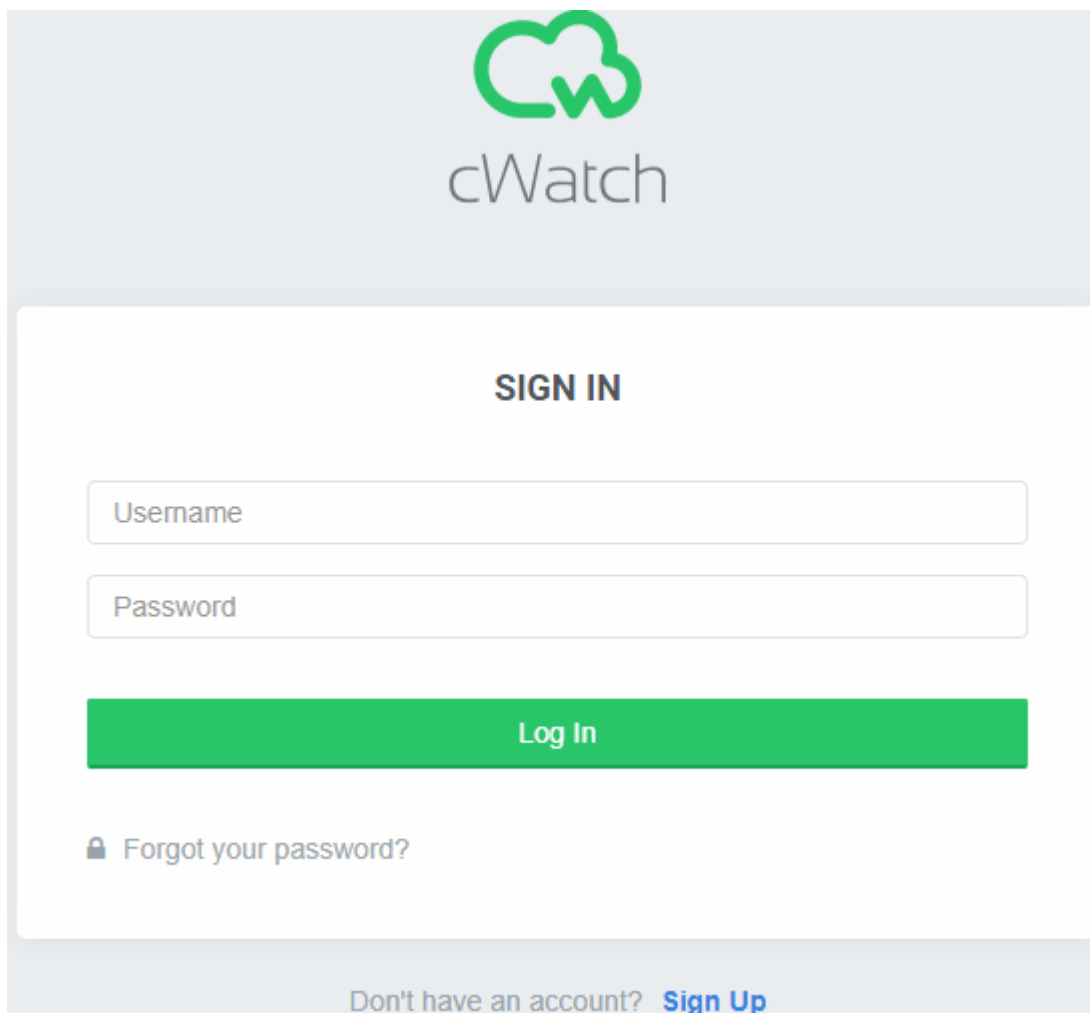
The screenshot displays the cWatch Web interface. At the top, it indicates 'PREMIUM PAID WITH TRIAL' and 'Scanning Completed'. Below this, the domain 'host03.qaplesk.pp.ua' is shown with a lock icon. A prominent green 'SCAN NOW' button is visible. The scan results are summarized in three columns: 'LAST SCAN' (17-01-2019), 'MALWARE' (No Malware Found), and 'REQUEST ID' (210537). Below the scan details, there are two toggle switches: 'Protection Mode' (turned on) and 'Detection Mode' (turned on). At the bottom, the 'Account Details' link is circled in red, with a mouse cursor pointing to it.

- Click 'Account Details' on a website tile.
- Click 'Continue' at the confirmation:





You will be taken to the login page of cWatch customer portal.



- Enter the username / password of the customer and click 'Log In'

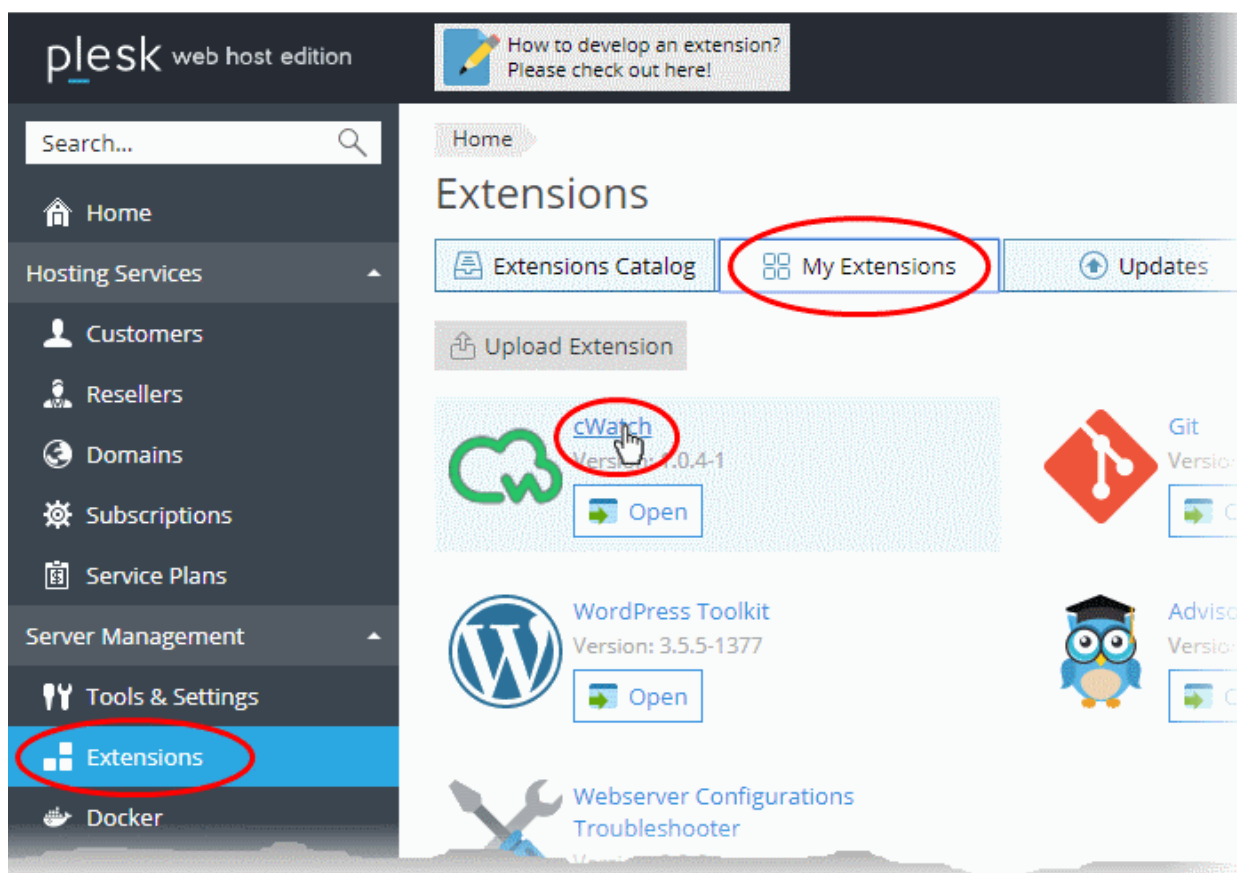
The customer dashboard opens.

## 5 Uninstall cWatch Extension

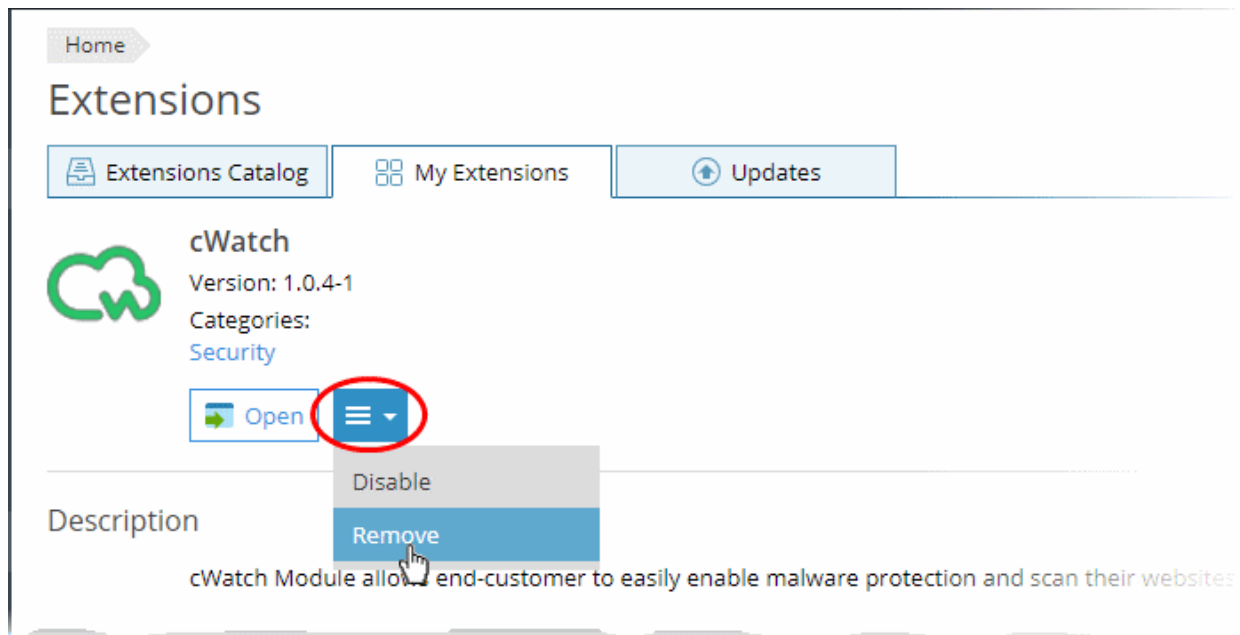
- Login to your Plesk account
- Click 'Extensions' on the left
- Select the 'My Extensions' tab

The extensions added to your Plesk control panel are shown as tiles.

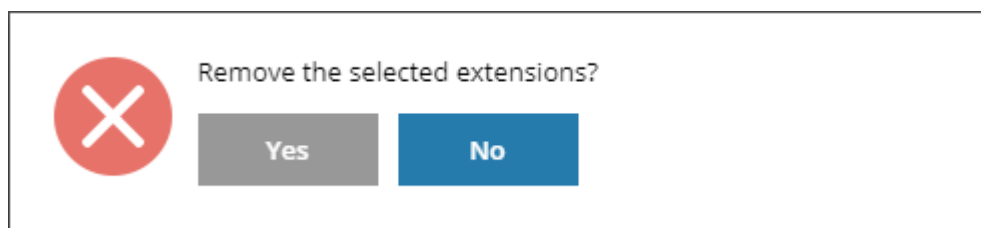
- Locate the cWatch tile and click on cWatch link as shown below:



The details page for cWatch extension opens:



- Click the drop-down as shown above and choose 'Remove'.



- Click 'Yes' in the confirmation dialog to remove the extension. The extension will no longer be available to your customers.

## 6 Membership Plans

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

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

- Please see <https://cwatch.comodo.com/legal/partners-plans.php> to view the features included with each license type.

## 7 Manage your CAM Account

- You will have received your Comodo Accounts Manager (CAM) account details after signing up as a partner / reseller with Comodo.
- The CAM interface lets you purchase licenses, track customer activity, deposit funds and more.
- Login to your CAM account at <https://accounts.comodo.com/login>
  - Use the same UN/PW as your cWatch account
- Click 'Services > 'Reseller Portal' (top-left):

The screenshot displays the Comodo Reseller Portal interface. At the top right, there is a summary of account balances: CA Reseller Balance (\$0.00 USD), CSS Reseller Balance (\$0.00 USD), and Current Bonus Balance (\$0.00 USD). Below this, a navigation bar includes 'Services', 'My Account', 'Help', and 'Contacts', with a 'Logout' button on the right. The main content area is titled 'Reseller Portal' and includes a welcome message and the last visit date (18 Apr 10:25). The 'Account Snapshot' section shows the CA Reseller Balance, CSS Account Balance, Total licenses purchased, and Total licenses activated. The 'Quick Links' section provides links for Product prices, Purchase History, Customer Activations History, and Distributing Companies Management. The 'Purchase Licenses' section is divided into Comodo Security Products (Customer Solutions, Enterprise Solutions, and Comodo CA Products) and Comodo CA Products (E-Commerce Solutions). At the bottom, there is a table for 'My recent activity (last month)' with columns for Date, Activity Type, Products, Terms, Activation Codes, Price, Distribution Company, and Reseller (Tar2).

The reseller portal allows you to...

- View your CSS account balance
- Deposit funds into your CSS account
- View total licenses purchased and activated
- Purchase other Comodo products

...and more.

Visit <https://help.comodo.com/topic-211-1-725-8860-The-Reseller-Portal.html> for detailed information about how to manage your CAM account.

# About Comodo Security Solutions

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

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

## About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

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