

**COMODO**  
Creating Trust Online®



# Comodo cWatch Web Security

Software Version 1.3

## Quick Start Guide

Guide Version 1.3.113018

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

# Comodo cWatch Office - Quick Start Guide

Comodo cWatch Office is a web filtering solution that provides comprehensive, DNS based security for your network devices, workstations and roaming devices. The solution monitors all inbound and outbound web traffic to provide real-time protection against the online threats and malicious websites. You can apply default or specific web filtering protection policies for individual devices and networks.

This document explains how you can purchase licenses, enroll networks/devices and configure protection settings:

- [Purchase Device License\(s\)](#)
- [Login to cWatch Office](#)
- [Add Networks and Devices](#)
- [Configure Protection Settings for Devices and Networks](#)
- [View Protection Statistics](#)

## Purchase Device Licenses

- Licenses are charged per network or device.
- You can purchase up to 20 device licenses at a time. If you wish to protect more than 20 devices, you can upgrade your license account by purchasing additional device licenses.

**Note:** cWatch Office is free for the first five devices on your account.

- You can purchase a license from <https://secure.comodo.net/home/purchase.php?pid=210>.

### To purchase a cWatch Office license

- Visit <https://secure.comodo.net/home/purchase.php?pid=210>

You will be taken to the license purchase page:

**COMODO** | Creating Trust Online™ | Need Assistance? 888-351-7956 | CHAT NOW! | USA, UK, AU

**Shopping Cart** | **Account Details** | **Complete Order**

**cWatch Office Starter**  
Please select license period :  1 year  
Number of devices : 6  
cWatch Office Starter \$ 9.90 per device

**TOTAL : \$ 59.40**

**ENTER CUSTOMER DETAILS**

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

New Comodo User  
E-mail address \* :

**PAYMENT DETAILS**

Cardholder Name \* :   
Credit Card No. \* :   
CVV \* :  / Expiration Date \* :  /

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

**Continue »**

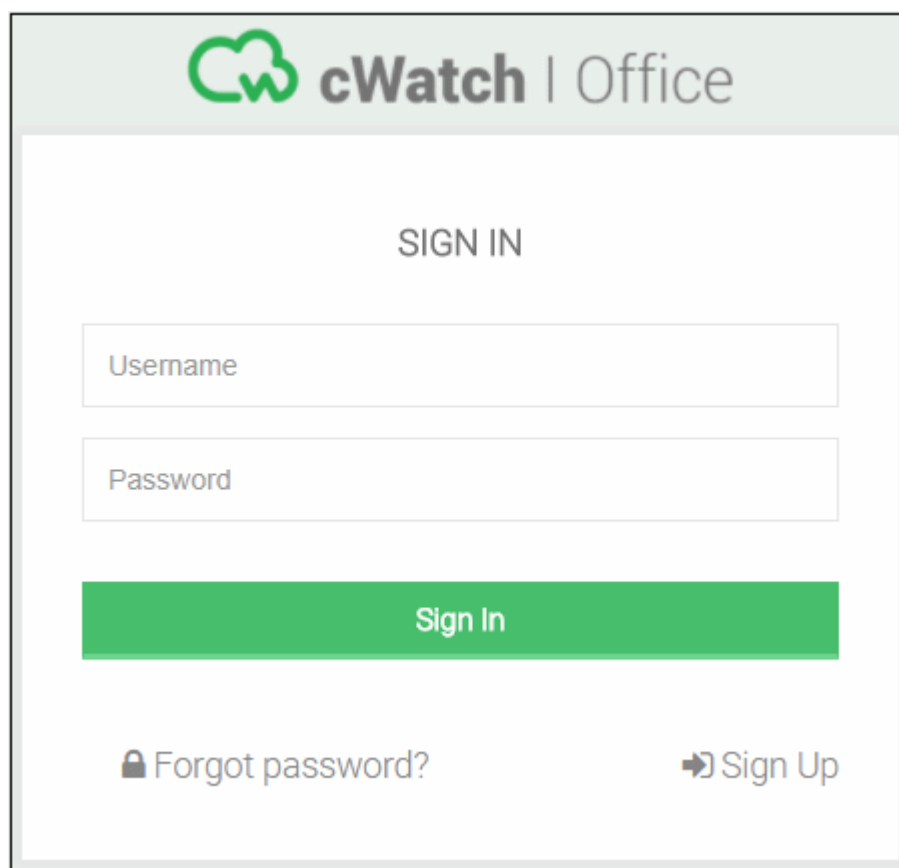
**SATISFACTION 30 DAY MONEY BACK GUARANTEE**  
Satisfaction Guaranteed, No Questions Asked \*

- Select the license period
- Use the slider to select the number of devices or networks to be covered by the license. The minimum is 6 and maximum is 20. You can purchase additional licenses if you wish to protect more than 20 devices.
- Next, enter your details:
  - If you already have a Comodo account, select 'Existing Comodo User' and enter your username and password.
  - If you don't have a Comodo account, select 'New Comodo User'. Enter your email address and a password to create a new account.
- Complete the payment details section.
- Read the 'End User License/Subscriber Agreement' and tick the checkbox to agree.

- Click 'Continue'. You will receive an order confirmation mail after your order has been successfully processed.
- Your licenses are now active. Existing customers should next login to their cWatch Office account and start enrolling their devices.
- New users will first need to activate their Comodo account by following the link in the account verification email.
- Next, login to cWatch Office at <https://office.cwatch.comodo.com/login> and add devices and networks to be protected.

## Login to cWatch Office

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



The screenshot shows the login interface for cWatch Office. At the top, there is a header with the cWatch logo (a green cloud with a white 'w') and the text 'cWatch | Office'. Below the header, the text 'SIGN IN' is centered. There are two input fields: 'Username' and 'Password'. Below the password field is a green button labeled 'Sign In'. At the bottom of the form, there are two links: 'Forgot password?' with a lock icon and 'Sign Up' with a right-pointing arrow icon.

- Use your Comodo Account username and password specified during sign-up to login.

On your first login to cWatch Office, the welcome screen will be displayed:



- Click 'Start' to start the Device/Network enrollment wizard.
- See **Add Networks and Devices** for guidance on adding networks and devices to be protected

## Add Networks and Devices

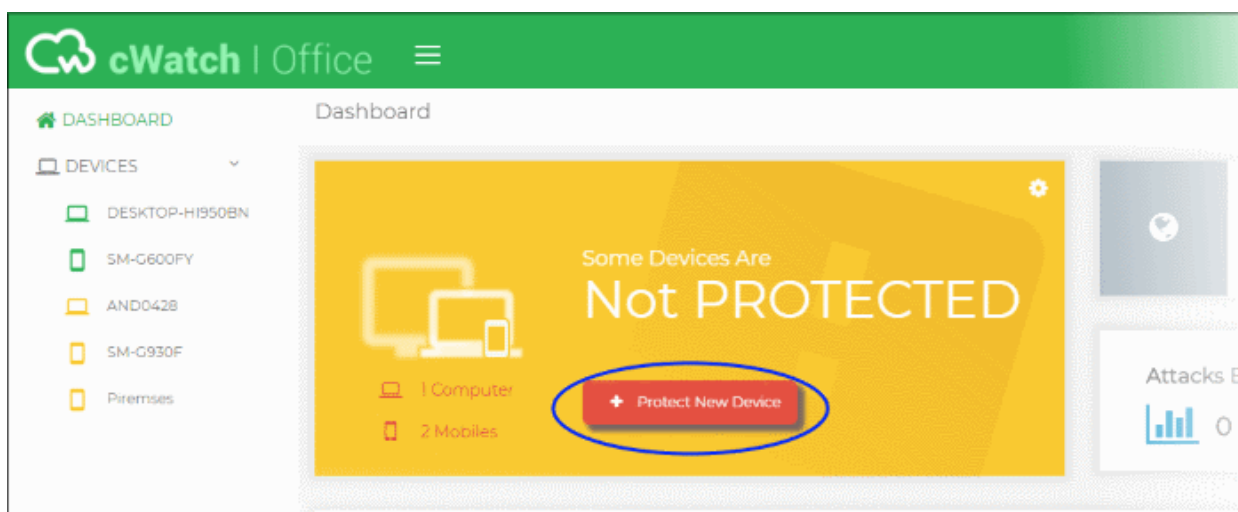
- The device enrollment wizard lets you add devices and networks you want to protect with cWatch Office.
- The number of devices/networks that can be added to your account depends on your license.
- Default protection settings will be applied immediately after device enrollment.
- You can customize protection settings for each device or network. Guidance on customizing protection settings is available in the section **Configure Protection Settings for Devices and Networks**.

### To add a new device or network

- Login to cWatch Office with your Comodo account credentials.

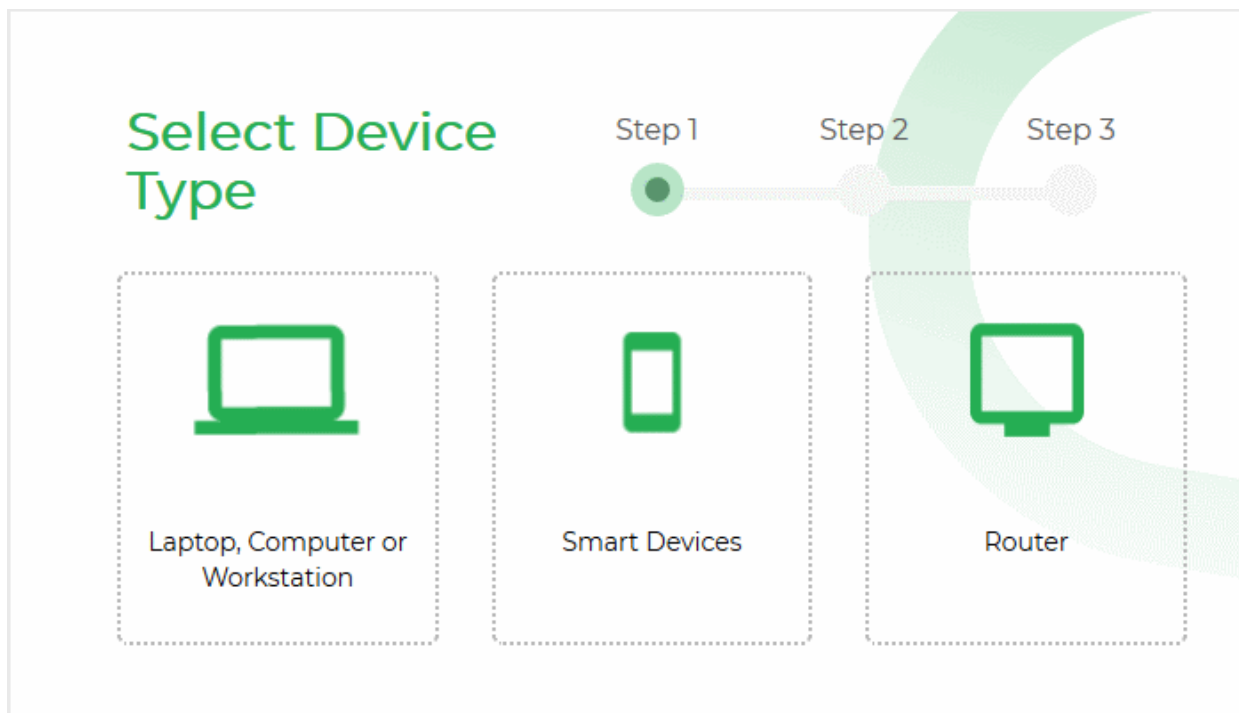
The dashboard will appear by default.

- Click 'Protect New Device' on the status tile



**Note:** If you are logging-in to cWatch Office for the first time, click 'Start' on the 'Welcome' page to begin the device enrollment wizard

The enrollment wizard will start:



The wizard contains two steps:

- **Step 1 - Select the device type**
- **Step 2 - Enroll the device**

### Step 1 - Select the device type

- Choose the type of device to be enrolled. The available options are:
  - **Laptop, Computer or Workstation** - Add Windows based devices like desktops, laptops, work stations and more
  - **Smart Devices** - Add Android and iOS devices used by your employees
  - **Router** - Add a network

### Step 2 - Enroll the device

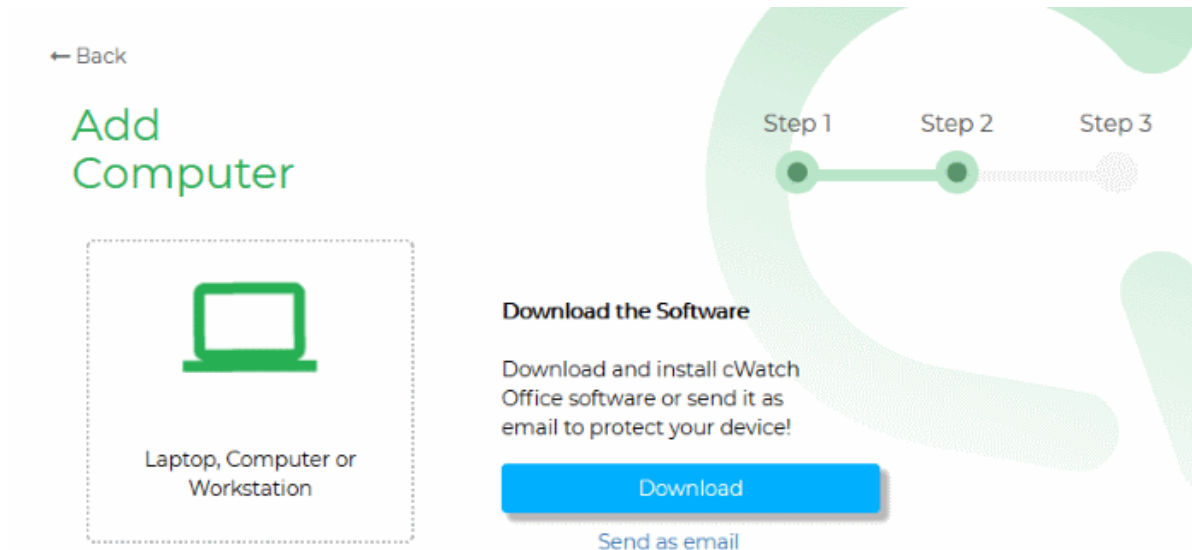
See the following sections for help with device type chosen in step 1:

- **Enroll Windows Devices**
- **Enroll Smart Devices**
- **Enroll Networks**

### Enroll Windows Devices

- Click 'Protect New Device' in the dashboard to start the device enrollment wizard.
- Select Laptop, Computer or Workstation

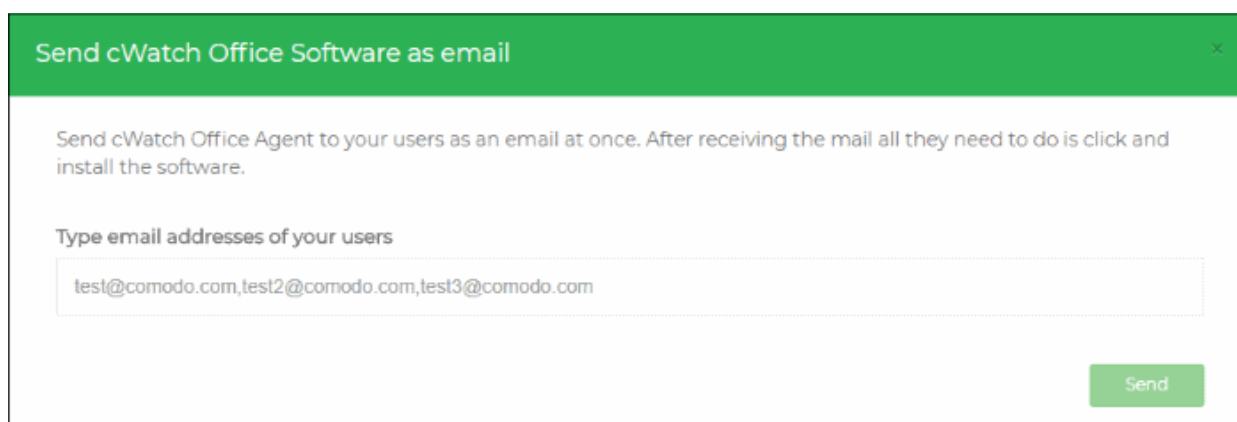
The instructions for enrolling a Windows device will appear:



## Install the agent on the device

You can install the agent on the device manually, or by sending an enrollment mail to the end-user. The device will automatically enroll with the cWatch server after the agent has been installed.

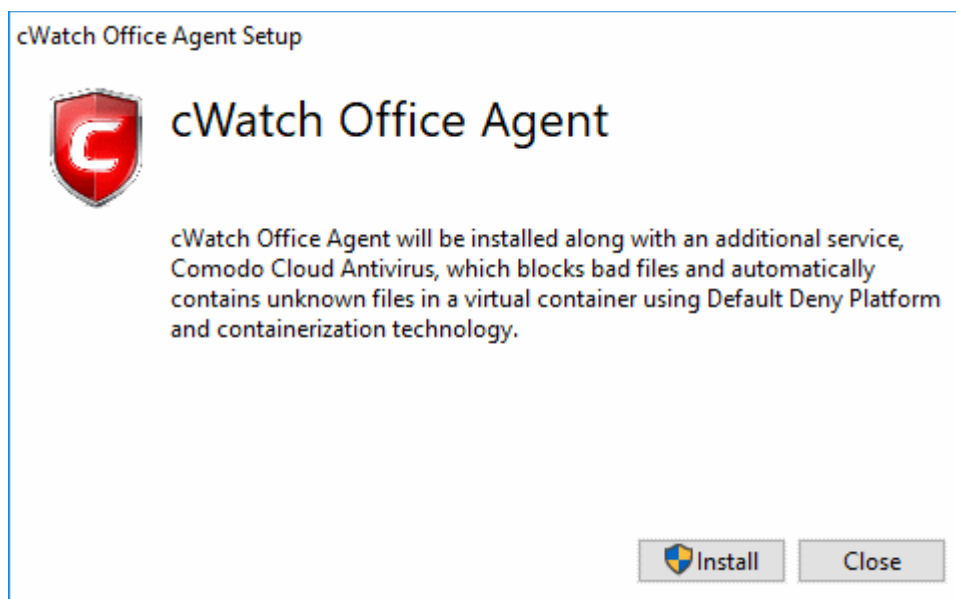
- **Manual install**
  - Click 'Download' to save the agent setup file. Install the file on the target device(s).
    - Alternatively, pass the file to the end-user to install by themselves.
  - You can use the same agent for all devices in this account, but you cannot use the same agent on devices in different accounts.
- **Enrollment email** - Click 'Send as email' to send a mail to the device owner. The mail contains a link to download and install the agent.




- Enter the email addresses of your end-users in the text box. You can add multiple addresses separated by a comma.
- Click 'Send'.

An email will be sent to the user(s) with instructions on how to install the agent.

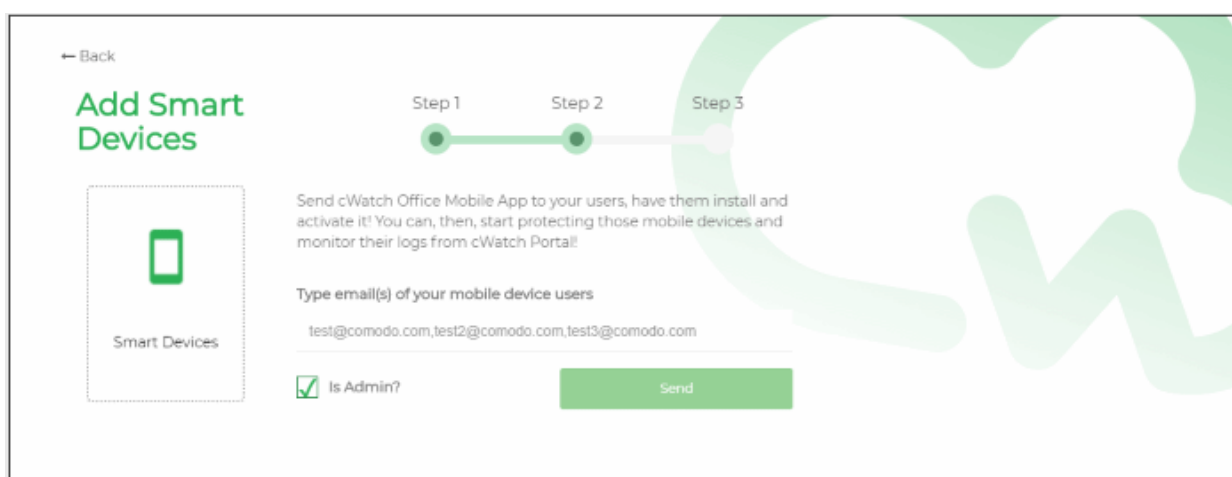
- Open the email on the device you want to enroll and follow the setup instructions
- Download the setup file and double-click on it.



- Click 'Install'
- Along with the agent, CCAV application, which implements core antivirus and containerization service for Windows devices will also be installed.
- That's it. The application will be installed automatically.
- After installation, the device will be automatically enrolled to cWatch office console. The cWatch tray icon  will appear on the endpoint screen.

## Enroll Smart Devices

The instructions for enrolling a smart device will appear on selecting 'Smart Devices' in step 1:



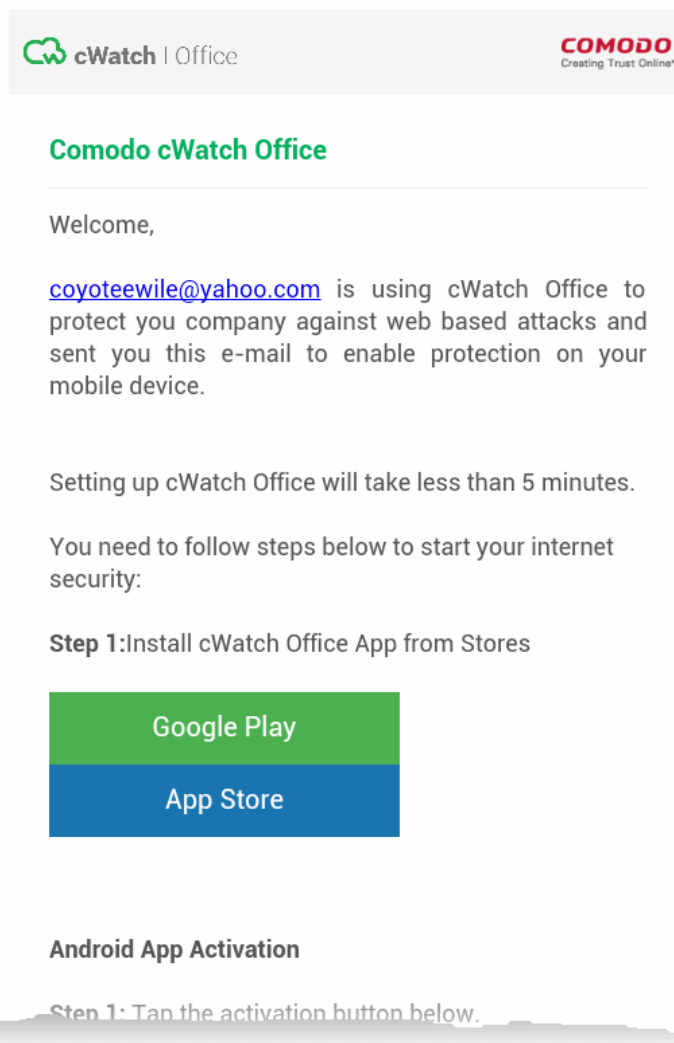
- Enter the email address(es) of the users whose devices you want to enroll. You can add multiple addresses separated by commas.
- Select the 'Is Admin?' checkbox if you want to assign an admin role to the user(s). Admins can use the cWatch app on their device to view web traffic stats for all protected devices.
- Click 'Send'.

An invitation mail will be sent to the target user(s) with instructions on how to install the app and register it with



cWatch.

An example mail is shown below:



See the following sections for help on installing the app and registering it with cWatch for Android and iOS devices:

- **Enroll Android Devices**
- **Enroll iOS Devices**

## **Enroll Android Devices**

Enrollment of Android Devices involves:

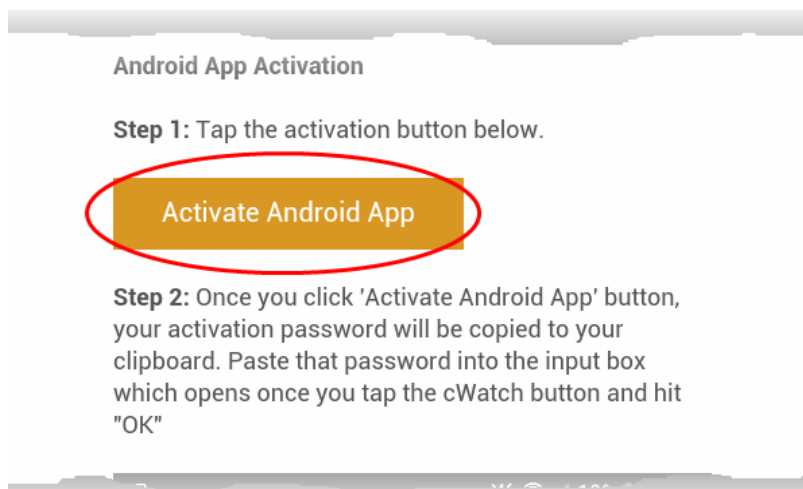
- **Installing the cWatch Office app**
- **Activating the app and registering it with cWatch Office**
- **Installing the SSL certificate so that the block page is correctly displayed when a HTTPS website is blocked**

## **Download and Install the cWatch Office app**

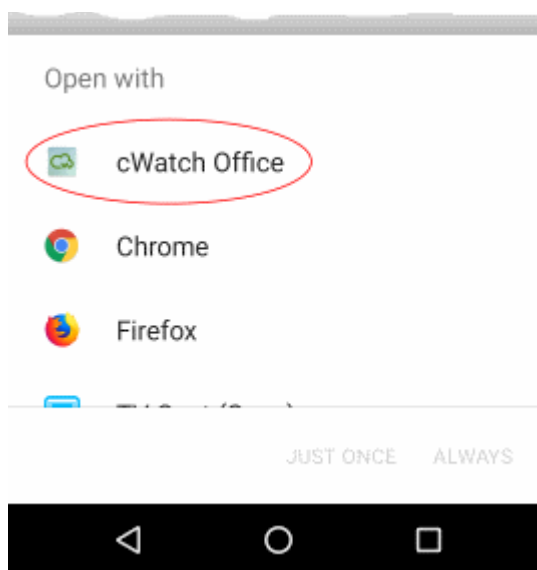
- Tap 'Google Play' in 'Step 1' in the enrollment mail
- This will open the Google Play store at the cWatch Office app page.
- Download and install the app on the device

## **Activate the app and register it with cWatch Office**

- Once the app is installed, go back to the email and tap 'Activate Android App' in step 1 of 'Android App Activation':

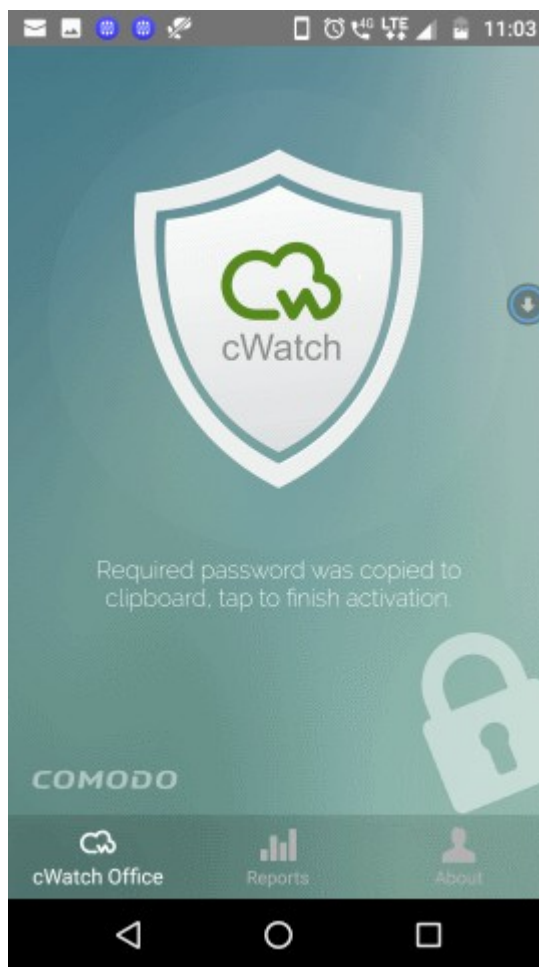


- Choose to open the link with cWatch Office:

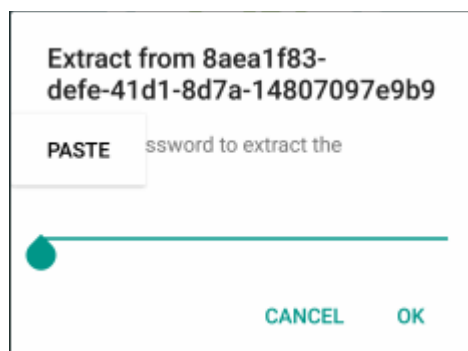


The cWatch app will open and start the registration process with the cWatch Office console.

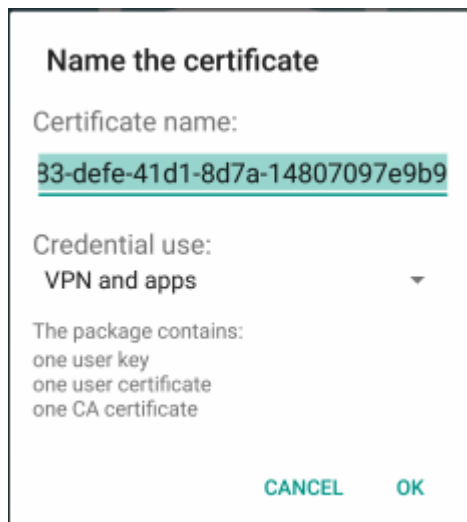
- A password will have been automatically generated and copied to the clipboard of the device. This password is required to extract a certificate and set a VPN profile so the device can connect to the cWatch console.
- The user needs to paste this password into the app.
- Tap the cWatch shield to start registration:



- To paste the password, just long press the text box and choose 'Paste' from the options:



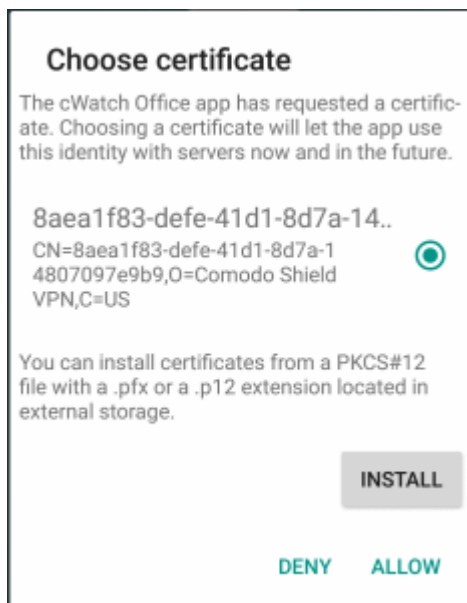
The certificate will be extracted, ready for installation:



- Select 'OK'

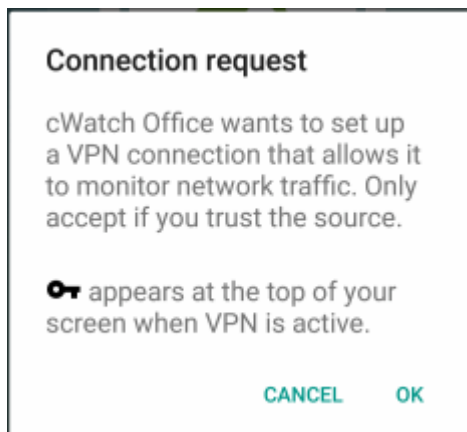
The next step is to install the certificate.

- The correct certificate will be automatically chosen.
- Tap 'Allow' to install the certificate.

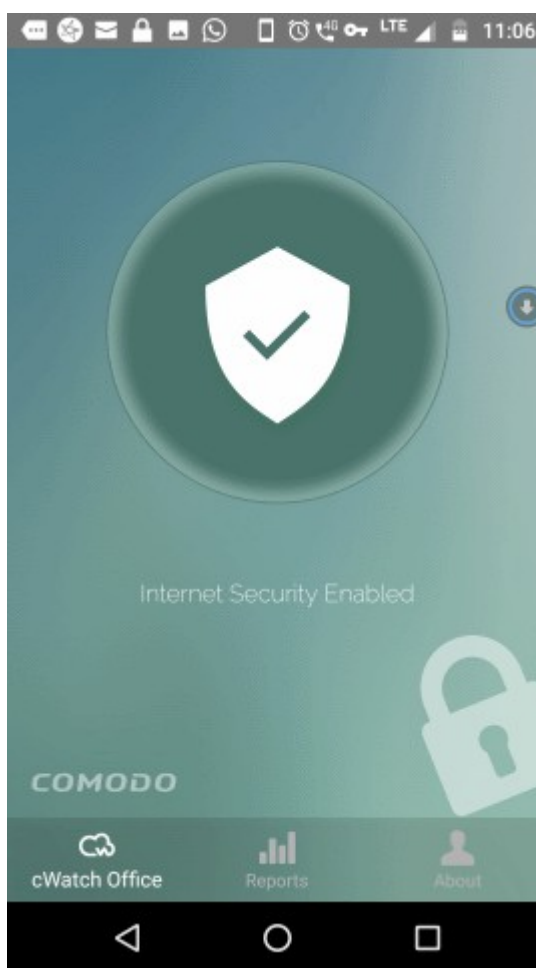


The next step is to allow the VPN connection.

- Select 'OK' to allow cWatch to setup a VPN connection to monitor network traffic



Installation and activation are now complete:

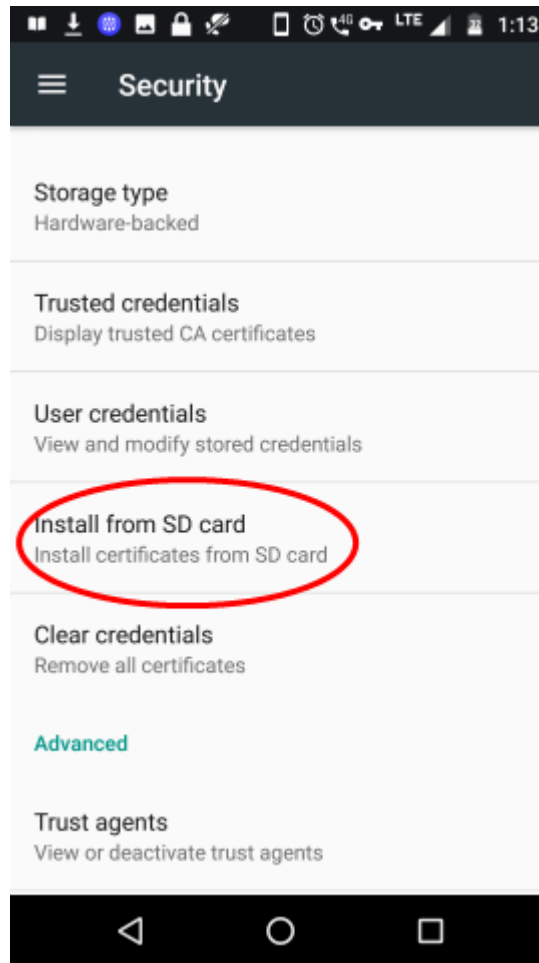


The app will connect to the cWatch Office console.

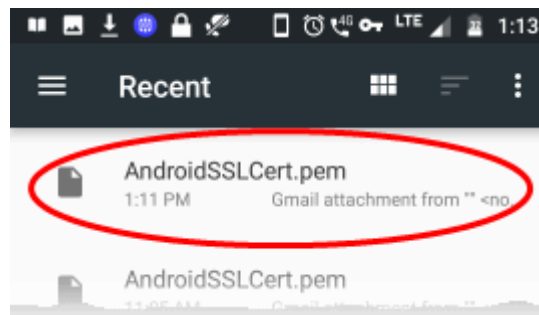
- The device will be added to cWatch Office and will be displayed under 'Devices' on the left.
- The default protection settings will be applied to the device

### **Install SSL certificate to correctly display warning page when HTTPS websites are blocked**

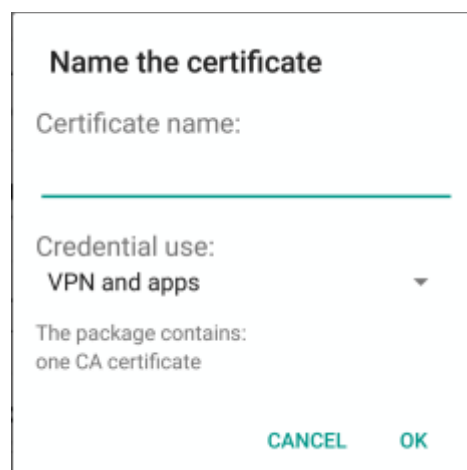
- Open the invitation email again and download the certificate file ('AndroidSSLCert.pem') attached to the mail
- In Android, open 'Settings' > 'Security' > 'Install from SD Card'



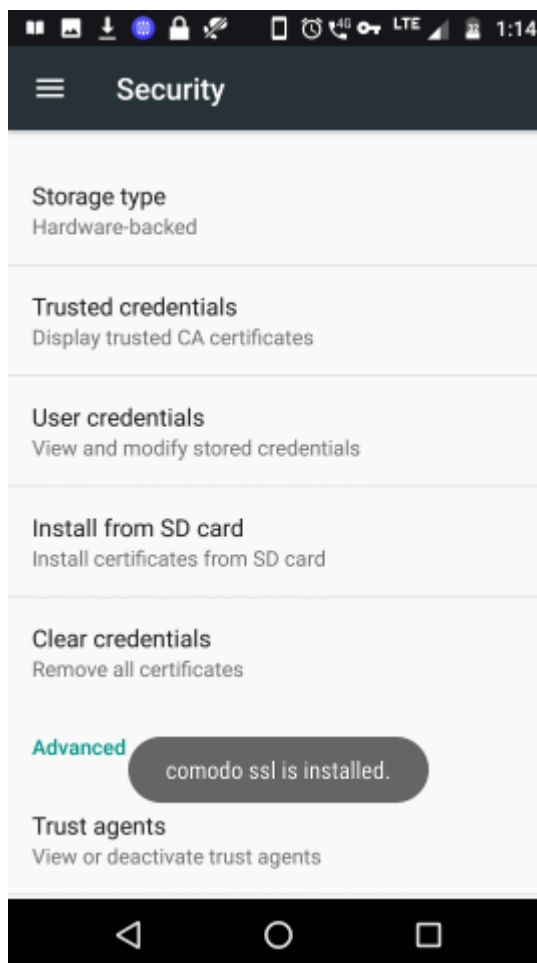
- Select 'AndroidSSLCert.pem' from the list:



- Enter a friendly name for the certificate:



- Click 'OK' to install the certificate



## Enroll iOS Devices

Enrollment of iOS Devices involves:

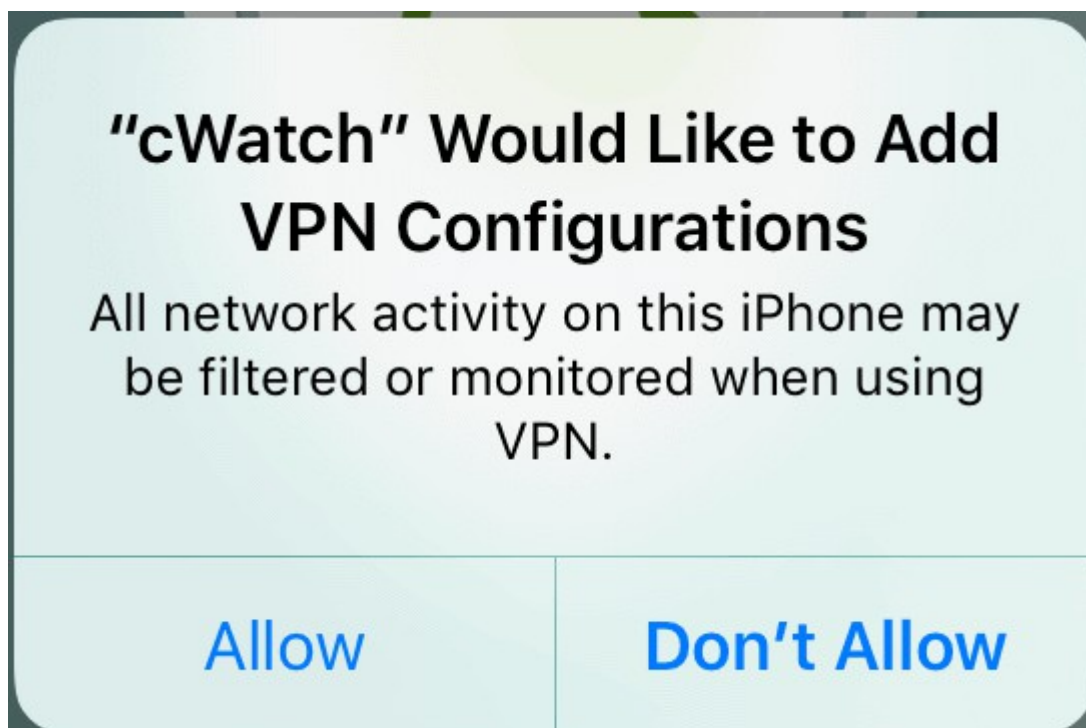
- **Installing the cWatch Office app**
- **Configuring the VPN connection**
- **Installing the SSL certificate so that the block page is correctly displayed when a HTTPS website is blocked**

## Download and Install the cWatch Office app

- Tap 'App Store' in 'Step 1' in the enrollment mail
- This will open the App Store at the cWatch Office app page.
- Download and install the app on the device

## Configure the VPN connection

- Once the app is installed, go back to the email and tap 'Activate iOS App' in step 1
- The cWatch app will start.
- Tap the cWatch logo on the app screen
- A VPN configuration confirmation dialog will appear.



- Click 'Allow'

A new VPN configuration will be created. The cWatch app will connect to the cWatch Office console.

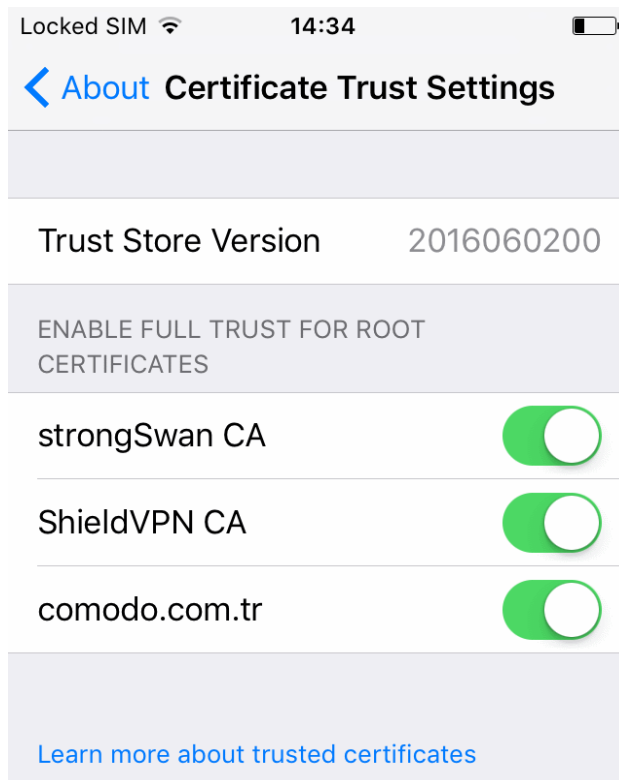
- The device will be added to cWatch Office and will be displayed under 'Devices' on the left.
- The default protection settings will be applied to the device

**Install the SSL certificate so that the block page is correctly displayed when a HTTPS website is blocked**

- In iOS, open 'Settings' > 'General' > 'About' > 'Certificate Trust Settings'

A list of certificates installed on the device is shown under 'Enable Full Trust for Root Certificates'.

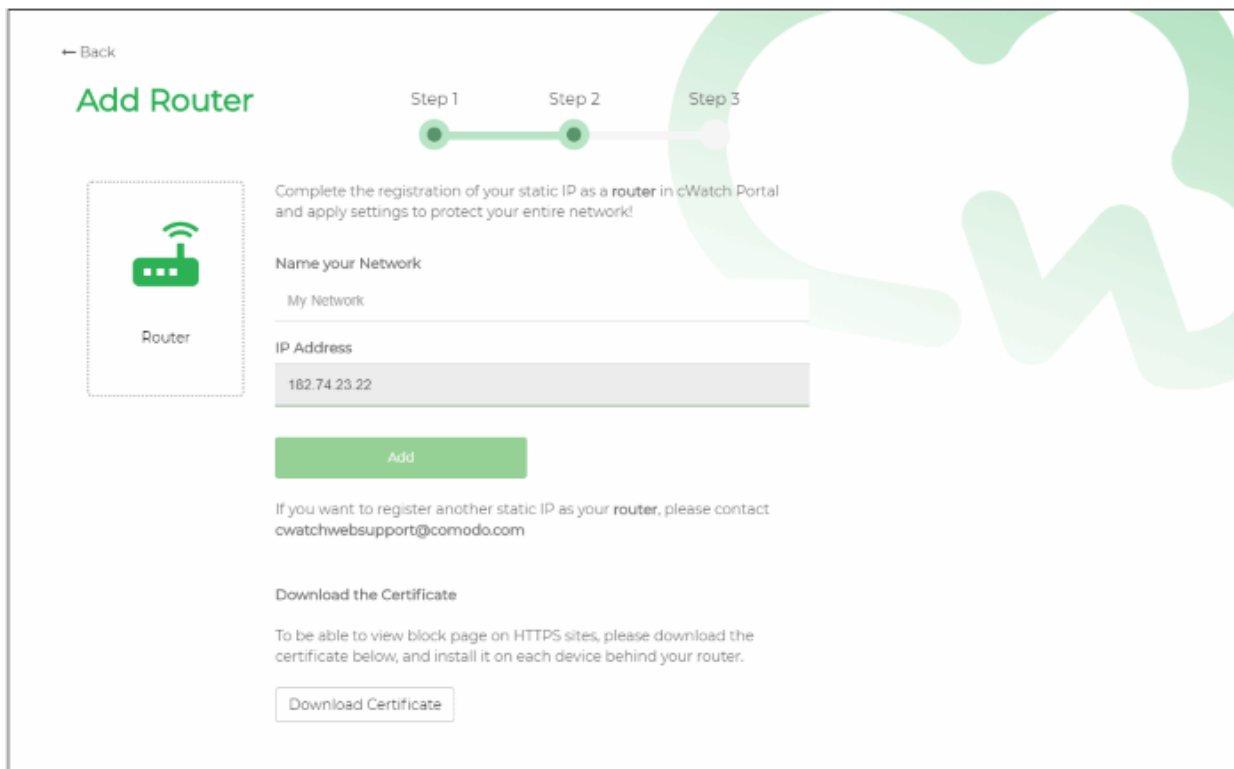




- Enable the certificate named 'comodo.com.tr'

## Enroll Networks

The instructions for enrolling a network will appear on selecting 'Router' in step 1:



Enrolling a network involves:

- **Adding network IP address to cWatch console**

- **Configuring DNS settings on the router**
- **Installing the SSL certificate so that the block page is correctly displayed when a HTTPS website is blocked**

## Add network IP address to cWatch console

The public IP address of the network from which you are currently connecting to cWatch Office console will be automatically fetched and displayed in the 'IP Address' field of the Instructions page.

- To enroll the same network, enter a name for the network in the 'Name your Network' text box and click 'Add'

**Note:** If you want to enroll a different network, please send an email with your account details and network IP address to [cwatchwebsupport@comodo.com](mailto:cwatchwebsupport@comodo.com).

The network will be added to cWatch Office and will be displayed under 'Devices' on the left.

## Configure DNS settings on the router

You have to configure the DNS settings of your router to point to Comodo Secure DNS addresses.

- Set your DNS server addresses as:
  - Primary DNS server : 8.26.56.26
  - Secondary DNS server: 8.20.247.20

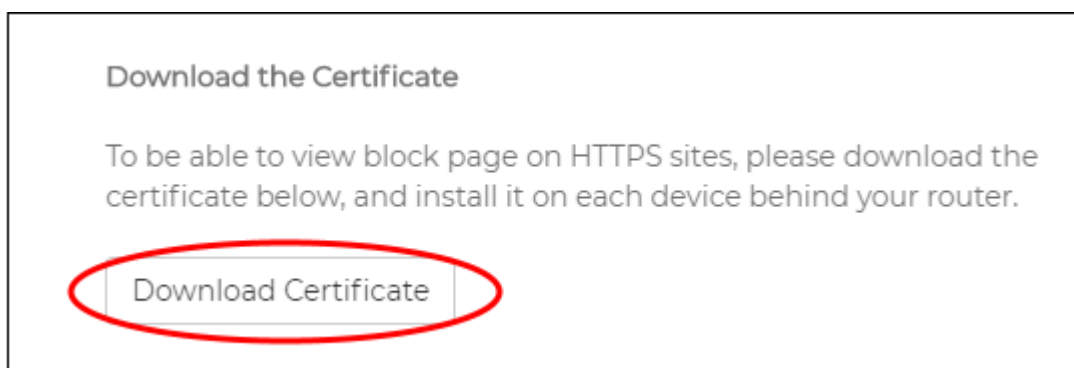
cWatch Office will now be placed between the internet and your router and will act as your internet gateway. For help to configure your router, see <https://www.comodo.com/secure-dns/switch/router.html>.

## Install SSL certificate for displaying warning page when HTTPS websites are blocked

- cWatch office displays a warning page to end-users whenever a website is blocked.
- You need to install an SSL certificate on each device behind the router in order to correctly display this warning page when a HTTPS site is blocked.
- The certificate can be downloaded from the instructions page in the device enrollment wizard.
- You can distribute the certificate to the users through any out-of-band communication method like email.
- Users should install the certificate on their device.

### To download the certificate

- Click 'Download Certificate' on the instructions page and save the file 'blockpage.pem'



- Send the certificate file to the user of devices on your network
- The users can install the certificates on their devices

## Configure Protection Settings for Devices and Networks

- cWatch Office filters websites based on their content type, or 'category'.
- Examples categories include adult websites, gambling sites, news sites, social media sites and sporting websites. Protection settings let you to define categories to be allowed and blocked on devices.
- Default protection settings will be applied to the devices immediately upon enrollment.
  - You can view the default settings by clicking 'Default Settings' in the overall protection status tile displayed in the dashboard
- You can use the default cWatch settings or you can configure custom settings for particular devices.

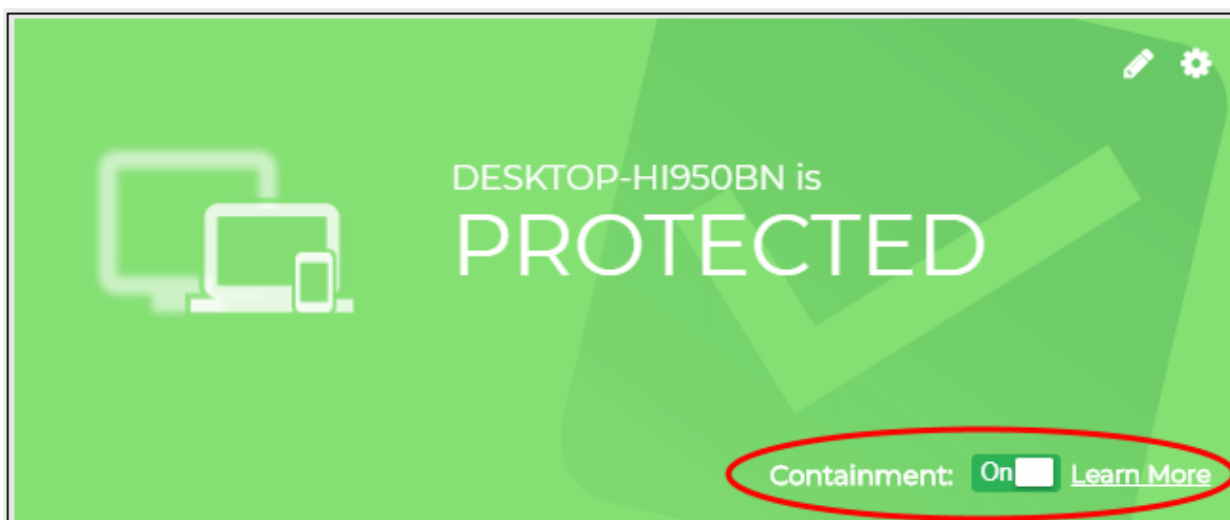
Click the links below to know about configuring protection settings:

- [Configure containment](#)
- [Configure protection settings](#)

### Enable / disable containment feature (Windows devices only)

To configure containment:

- Click on a Windows device in the left-hand menu
- Containment status is shown in the main, protection summary tile:



Containment is enabled by default. The following applies when containment is enabled:

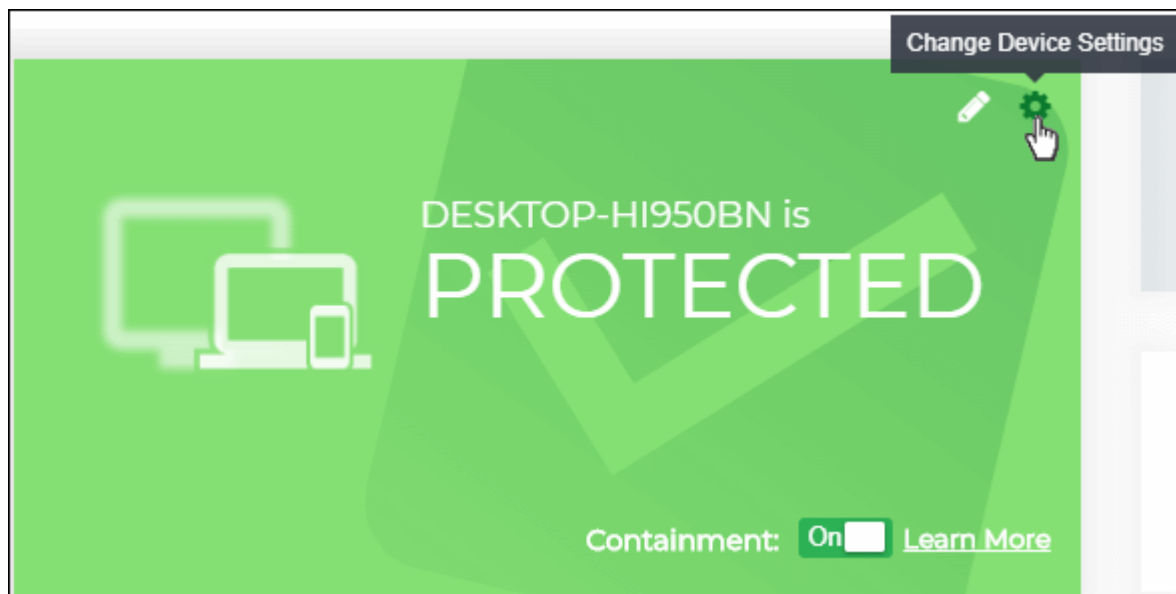
- Files with an 'unknown' trust-rating will be run in a secure virtual environment, isolated from the underlying file system and user data. A green border is shown around the application window.
- Details about the file are sent to Valkyrie, a verdicting system that analyzes the file to determine whether it is safe or malicious. See <https://valkyrie.comodo.com/> for more information.
  - You can see the results by logging into Valkyrie at <https://valkyrie.comodo.com/login> with your cWatch Office credentials. See <https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html> for more help with this.
  - If an unknown file is found to be safe it will be allowed to run normally next time.
- Click 'Learn More' for an explanation of containment.

### Configure protection settings for a device

To configure protection settings for a device:

- Select the device from the left pane to open its 'Device Overview' page

- Click the gear icon  at top-right of the protection status tile



The 'Device Web Browsing Settings' for the device will open. It contains the settings as per the default protection settings shipped with cWatch Office.

← Back

## Device Web Browsing Settings

This is the rule set specific for this device.  
These settings will be applied only to this device and overwrite Default Settings.

### What Do You Want To Block?

1) Do you want to block access to Adult Content?  
*Ex: Playboy, Pornhub*

Yes  No

2) Do you want to block access to Social Networks?

Marketing-Merchandising	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Intimate Apparel & Swimwear	<input checked="" type="checkbox"/>	<input type="checkbox"/>

### Do you want to whitelist any websites?

### Do you want to blacklist any websites?

From this page, you can:

- **Select the website categories to be blocked**
- **Configure allow/block policies for miscellaneous website categories**
- **Create website blacklist/whitelist for the device**

## Select blocked Website Categories

- The 'What Do You Want To Block?' area lets you decide which website categories are allowed or blocked on the device. The categories in this area are those which many organizations may considering blocking:

**What Do You Want To Block?**

1) Do you want to block access to Adult Content?  
Ex: Playboy, Pornhub  
 Yes  No

2) Do you want to block access to Social Networks?  
Ex: Facebook, Twitter, Instagram, Tumblr etc.  
 Yes  No

3) Do you want to block access to News Websites?  
Ex: Huffington Post, New York Times, The Economist etc.  
 Yes  No

4) Do you want to block access to Sports Related Websites?  
Ex: ESPN, Euro Sports, NBA etc.  
 Yes  No

5) Do you want to block Gambling Websites?  
Ex: Bwin, Betting, Online Casinos etc.  
 Yes  No

6) Do you want to block Shopping Websites?  
Ex: Amazon, Best Buy, Ali Baba etc.  
 Yes  No

7) Do you want to block Personal & Dating Services?  
Ex: Match.com, My Single Friend etc.  
 Yes  No

8) Do you want to block Chat & Instant Messaging Services?  
Ex: Whatsapp, Slack etc.  
 Yes  No

9) Do you want to block Gaming sites?  
Ex: Steam, PokerStars.net, bigfishgames.com, King.com etc.  
 Yes  No

10) Do you want to block Advertising & PopUps sites?  
Ex: Ads & Popups shown while surfing websites  
 Yes  No

- Select 'Yes' to categories you want to block
- Select 'No' to categories you want to allow
- 

## Additional Website Categories

The 'Additional Categories' area lets you allow or block categories which are less 'clear-cut'. Your company may or may not wish to block them:

## Do you want to block some additional categories?

Categories	Allow	Block
Job Search & Career Development	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Entertainment	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Hosted Personal Pages	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Instant Moderated Forums	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Blogs & Wikis	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Advocacy-NGO	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Health	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Marketing-Merchandising	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Intimate Apparel & Swimwear	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Select 'Block' for categories you want restrict
- Select 'Allow' for categories you want to permit

### Whitelist or Blacklist Websites

- Whitelisted sites will be allowed and blacklisted sites will be blocked regardless of the category to which they belong. For example, if you block access to 'Shopping websites', but decide to white-list 'example-shop.com', then 'example-shop.com' will be allowed.
- You can add as many websites as you want to the whitelist/blacklist for a device. The list will be active only for the specific device.

#### To add websites to whitelist

- Enter the domain name (without 'www.') in the text box below 'Do you want to whitelist any websites?' and click the '+' button.

## Do you want to whitelist any websites?

acronymfinder.com



en.wikipedia.org

## Do you want to blacklist any websites?

- Repeat the process to add more websites
- To remove a website, place your mouse over the website name and click 'x'

## Do you want to whitelist any websites?

acronymfinder.com



en.wikipedia.org



## Do you want to blacklist any websites?

### To add websites to whitelist

- Enter the domain name (without 'www.') in the text box below 'Do you want to blacklist any websites?' and click the '+' button.
  - Repeat the process to add more websites
  - To remove a website, hover your mouse over the website name and click 'x'
- Click 'Save' for your settings to take effect

## Do you want to blacklist any websites?

example.com



pokersample.com

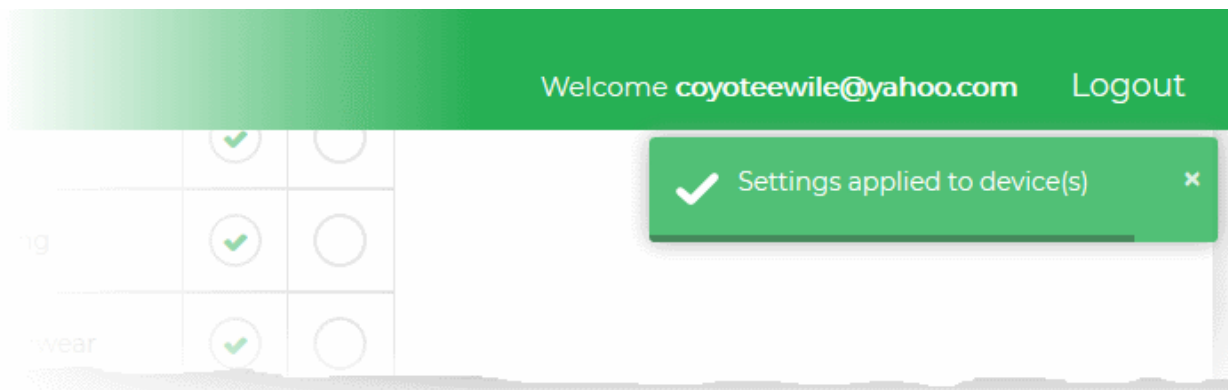
Discard

Save

Apply to Other Devices



The protection settings will be saved and immediately applied to the device.



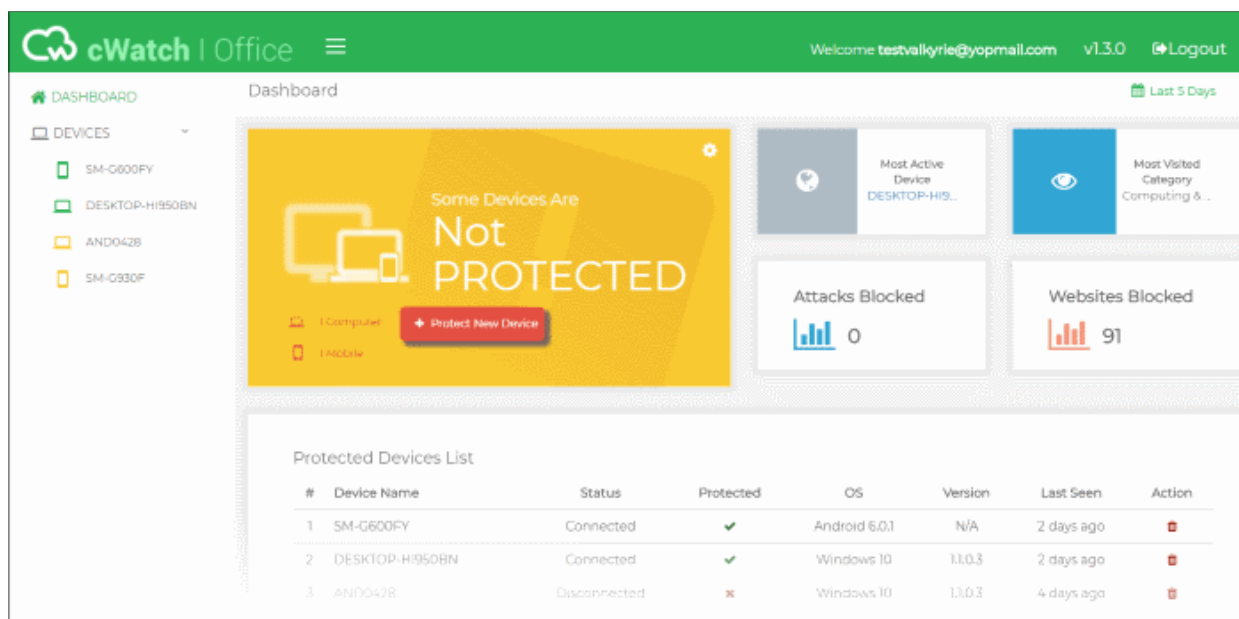
## View Protection Statistics

The dashboard shows protection and browsing statistics for your devices. Statistics include websites visited, websites blocked, attacks blocked and more.

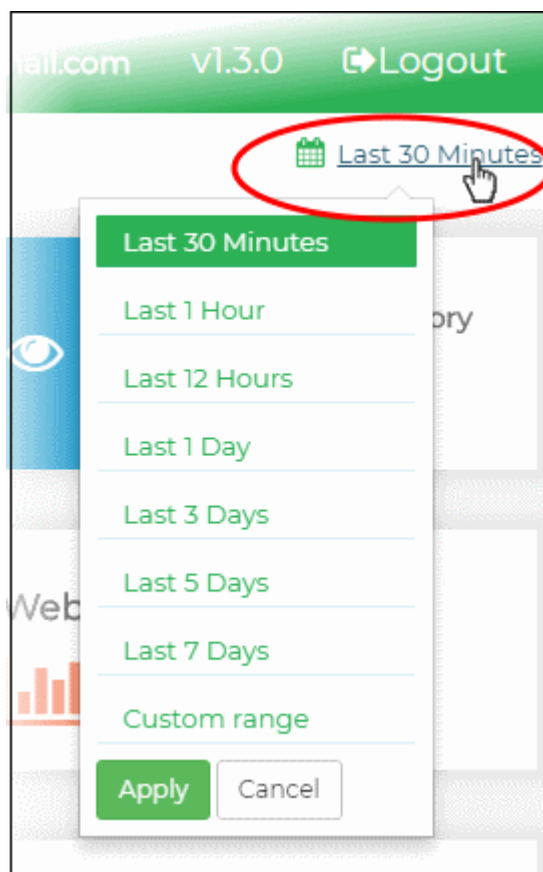
- **The 'Dashboard'** - Data on all devices enrolled for your account.
- **The 'Device Overview'** - Data on specific devices

### The Dashboard

- Click 'Dashboard' on the left to open the dashboard.



- Use the date range picker at top-right to choose the time period of the statistics:



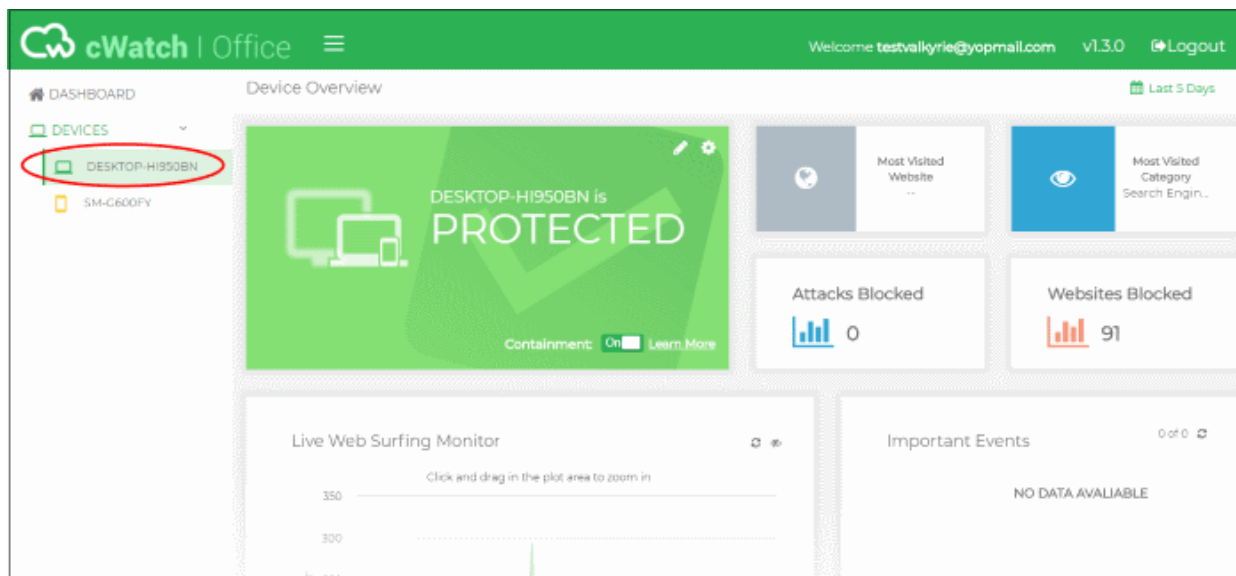
The 'Dashboard' contains the following tiles:

- **Overall protection status** - Shows how many enrolled devices are connected to cWatch protection. It also allows you add new networks/devices and view default protection settings.
- **Most active device** - The device which has visited the largest number of sites / pages within the selected time period. This includes both allowed and blocked websites.
- **Most visited category** - The website category visited most often by devices in your network.
- **Attacks blocked** - The total number of attacks blocked on all enrolled devices/networks within the selected period.
- **Websites blocked** - The total number of website access attempts that were intercepted and blocked on all devices.
- **Protected Devices List** - Shows all devices that have been enrolled to cWatch, along with details like the device name, OS and connection status.
- **Live web surfing monitor** - Shows the number of websites visited by each enrolled device during the selected time-period.
- **Important events** - A timeline of noteworthy security events across all devices/networks in the selected time period. Events can include blocked websites and potential attacks which were prevented by cWatch Office.
- **Most visited websites** - The ten websites visited most often by all devices in your cWatch network.
- **Most blocked categories** - The ten website categories which were most often visited and blocked in your cWatch network.
- **Last visited websites** - The 100 websites most recently visited by devices in your cWatch account.

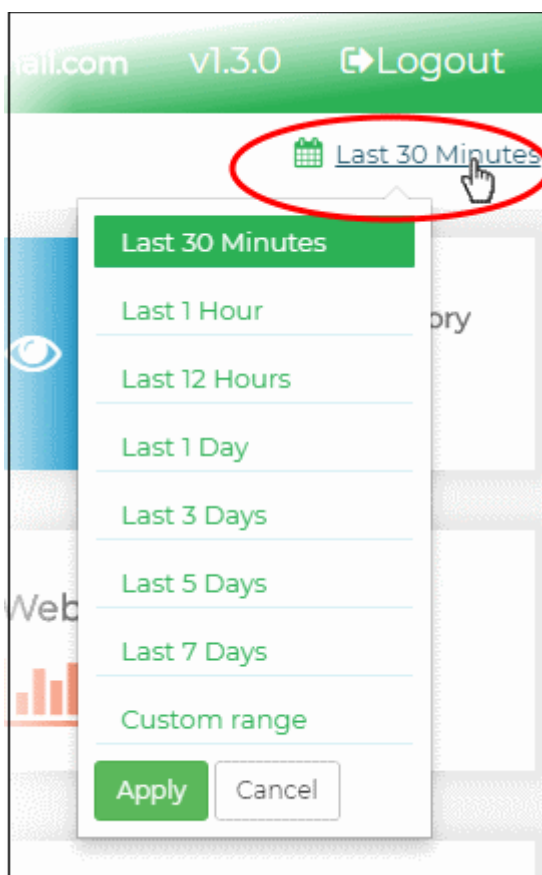
- **Top devices** - The ten devices which made the most website requests within the selected time-period.

## The Device Overview

- Click the name of a device/network on the left to open the 'Device Overview' page:



- The date picker at top-right lets you choose the time period of the statistics:



The 'Device Overview' page contains the following tiles:

- **Device protection status** - Shows whether or not the device is connected to the cWatch console. It also allows you to view and manage the protection settings in effect on the device.
- **Most visited website** - The website most often visited by the device.

- **Most visited category** - The website category visited most often by the device within the selected period.
- **Attacks blocked** - The total number of attacks blocked on the device within the selected period.
- **Websites blocked** - The total number of website access attempts that were intercepted and blocked on the device.
- **Live web surfing monitor** - Shows the number of websites visited by the device during the selected time-period.
- **Important events** - A timeline of noteworthy security events on the device in the selected time period. Events can include blocked websites and potential attacks which were prevented by cWatch.
- **Most visited websites** - The ten websites visited most often by the device.
- **Most blocked categories** - The ten website categories which were most often visited and blocked on the device. The categories blocked depend on the protection settings active on the device.
- **Last visited websites** - The 100 websites most recently visited by the device.

# 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)