

COMODO
Creating Trust Online®



Comodo
cWatch Office
Software Version 1.3

Administrator Guide

Guide Version 1.3.113018

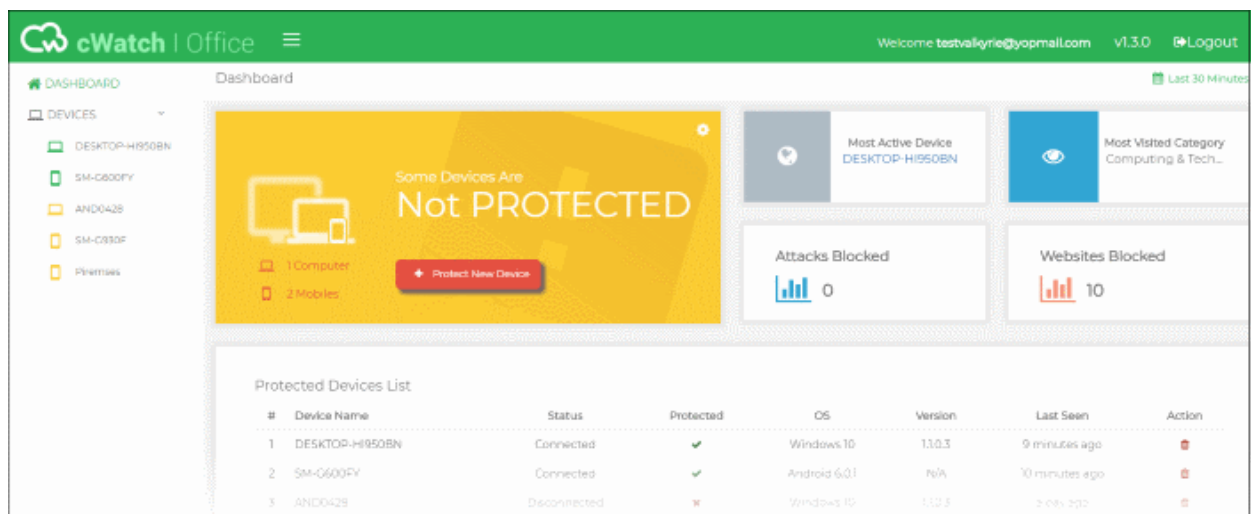
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo cWatch Office.....	3
1.1 Purchase a License.....	4
1.2 Login to the Administrative Console.....	6
1.3 Add Networks and Devices.....	7
1.3.1 Enroll Windows Devices.....	8
1.3.2 Enroll Smart Devices.....	11
1.3.2.1 Enroll Android Devices.....	11
1.3.2.2 Enroll iOS Devices.....	20
1.3.3 Enroll Networks.....	25
2 The Admin Console.....	28
3 The cWatch Office Dashboard.....	29
3.1 View Default Protection Settings.....	35
4 Device Overview.....	39
4.1 Manage Protection Settings on a Network/Device.....	44
4.2 Manage Protection Settings for Several Devices.....	51
5 The cWatch Mobile Admin Console.....	52
5.1 The Home Screen.....	54
5.2 View cWatch Office Reports.....	54
5.3 View Device Summaries.....	59
5.4 About.....	61
6 Upgrade Your License.....	62
About Comodo Security Solutions	63

1 Introduction to Comodo cWatch Office

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 online threats and malicious websites. You can apply a default protection policy to all devices or set specific policies for individual devices. cWatch's powerful dashboard provides an over-arching summary of blocked threats and the browsing history of devices in your network.



Features

- Default security policies provide blanket protection from online threats for local, roaming and mobile devices
- Simple interface make it easy to create and deploy custom protection policies.
- Easily create exceptions with your own domain blacklists and whitelists
- Supports iOS, Android and Windows devices
- Unknown files are contained in a highly secure, virtual environment on Windows devices
- Use the cWatch app on your mobile device to remotely monitor your network from any location
- Easy setup - quickly enroll your devices using our 5 minute wizard

Guide Structure

This guide is intended to take you through the configuration and use of cWatch Office and is broken down into the following main sections:

- **Introduction to Comodo cWatch Office**
 - **Purchase a License**
 - **Login to the Administrative Console**
 - **Add Networks and Devices**
 - **Enroll Windows Devices**
 - **Enroll Smart Devices**
 - **Enroll Android Devices**

- **Enroll iOS Devices**
 - **Enroll Networks**
- **The Admin Console**
- **The cWatch Office Dashboard**
 - **View Default Protection Settings**
- **Device Overview**
 - **Manage Protection Settings for a Network/Device**
 - **Manage Protection Settings for Several Devices**
- **The cWatch Mobile Admin Console**
 - **The Home Screen**
 - **View cWatch Office Reports**
 - **View Device Summaries**
 - **About**
- **Upgrade Your License**

1.1 Purchase a License

The number of devices or networks that can be enrolled to your cWatch Office account depends on your license. You can subscribe for license from <https://secure.comodo.net/home/purchase.php?pid=210>

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

You can add up to 20 devices to a single license. You can purchase additional licenses if you wish to protect more than 20 devices.

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! |

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 * :

30 DAY MONEY BACK GUARANTEE

Satisfaction Guaranteed,
No Questions Asked *

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

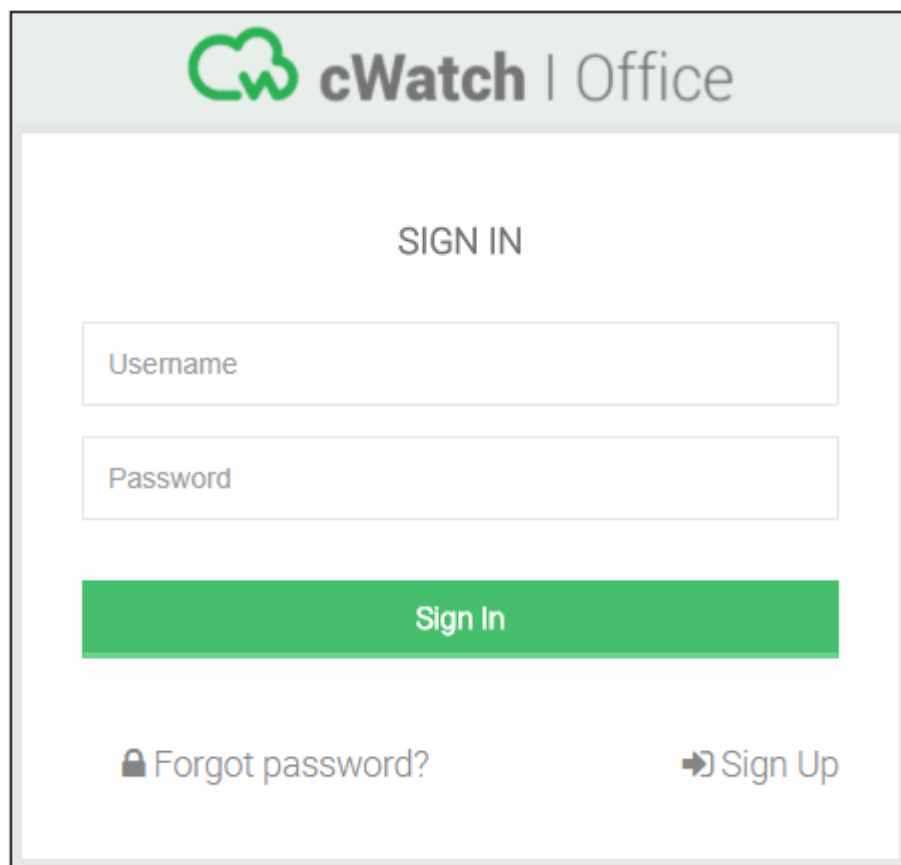
Continue »

- 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, you need to add your devices and networks to cWatch Office:
 - Login at <https://office.cwatch.comodo.com/login> using your Comodo account username and password.
 - Click 'Start' on the 'Welcome' screen to begin enrolling your devices.
 - See [Add Networks and Devices](#) if you need more help with this.

1.2 Login to the Administrative Console

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:

Welcome to cWatch Office

We will take you through cWatch Office Setup Wizard to help you register your devices to cWatch Office and start protecting your device from web-based attacks.

Start

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

1.3 Add Networks and Devices

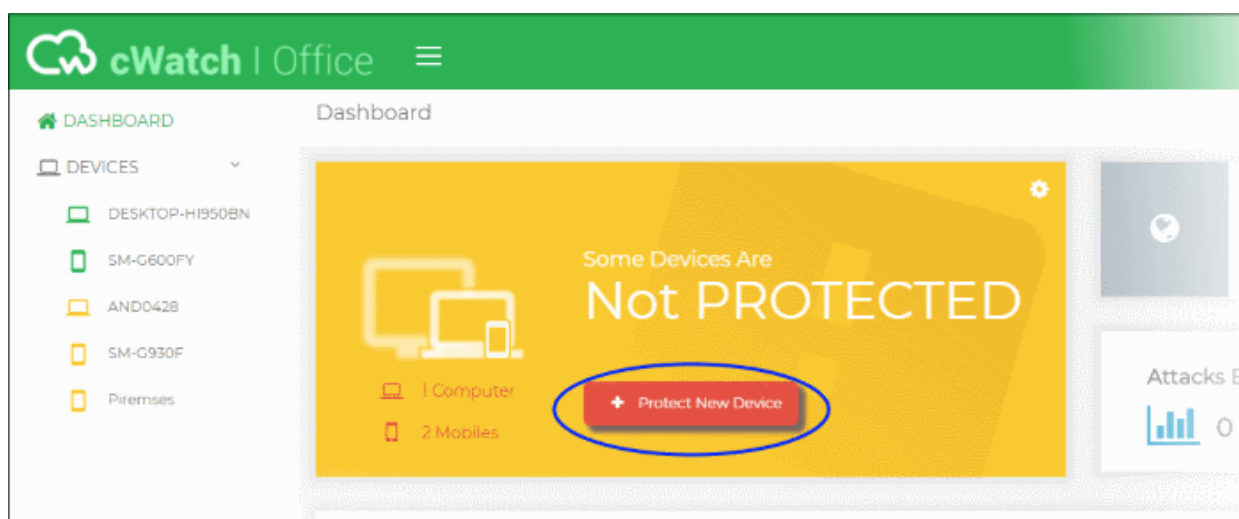
- The device enrollment wizard lets you add devices and networks you want to protect with cWatch.
- The number of devices/networks that can be added to your account depends on your license. See [Purchasing a License](#) for details about license types
- Default protection settings will be applied immediately after enrollment. See [View Default Protection Settings](#) for more details
- You can customize protection settings for each device or network from the device overview interface. You can also apply settings from one device to other devices. See [Manage Protection Settings for a Network/Device](#) for more guidance on this.

To start the device enrollment wizard

- Login to cWatch Office

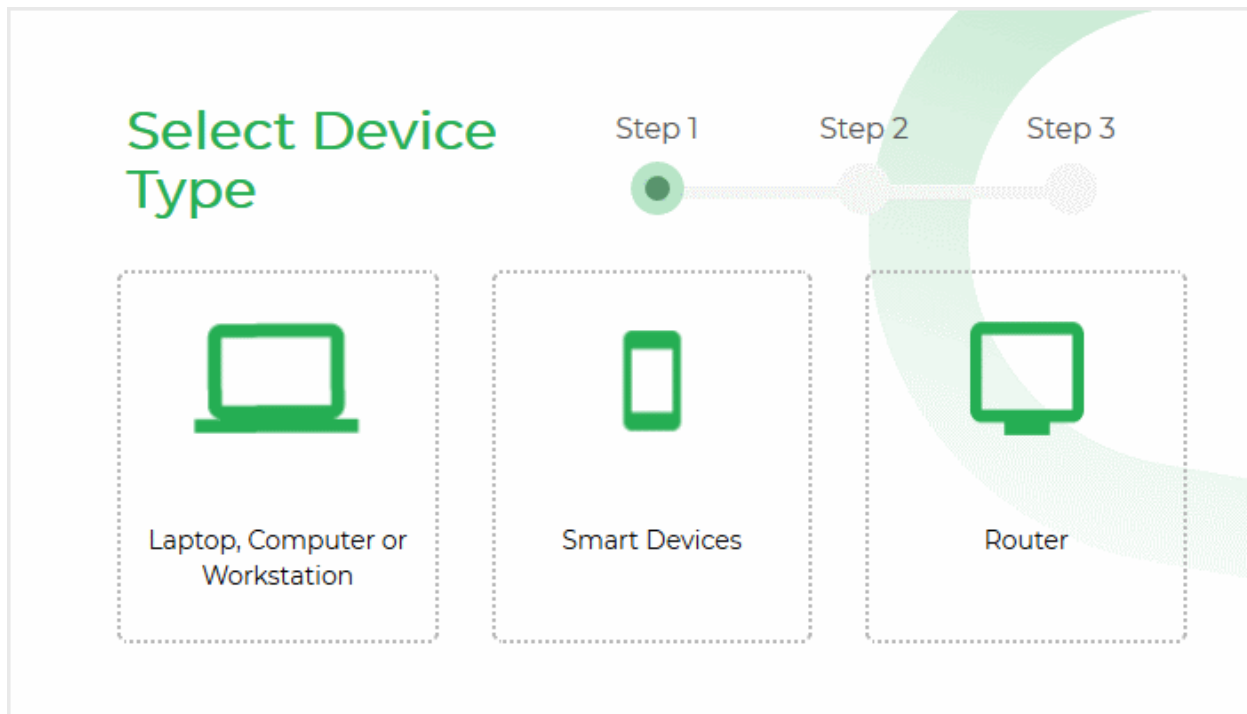
The dashboard will appear

- Click 'Protect New Device' from 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 wizard will start.



- Select the type of the device you want to enroll.

See the following sections for help with each type:

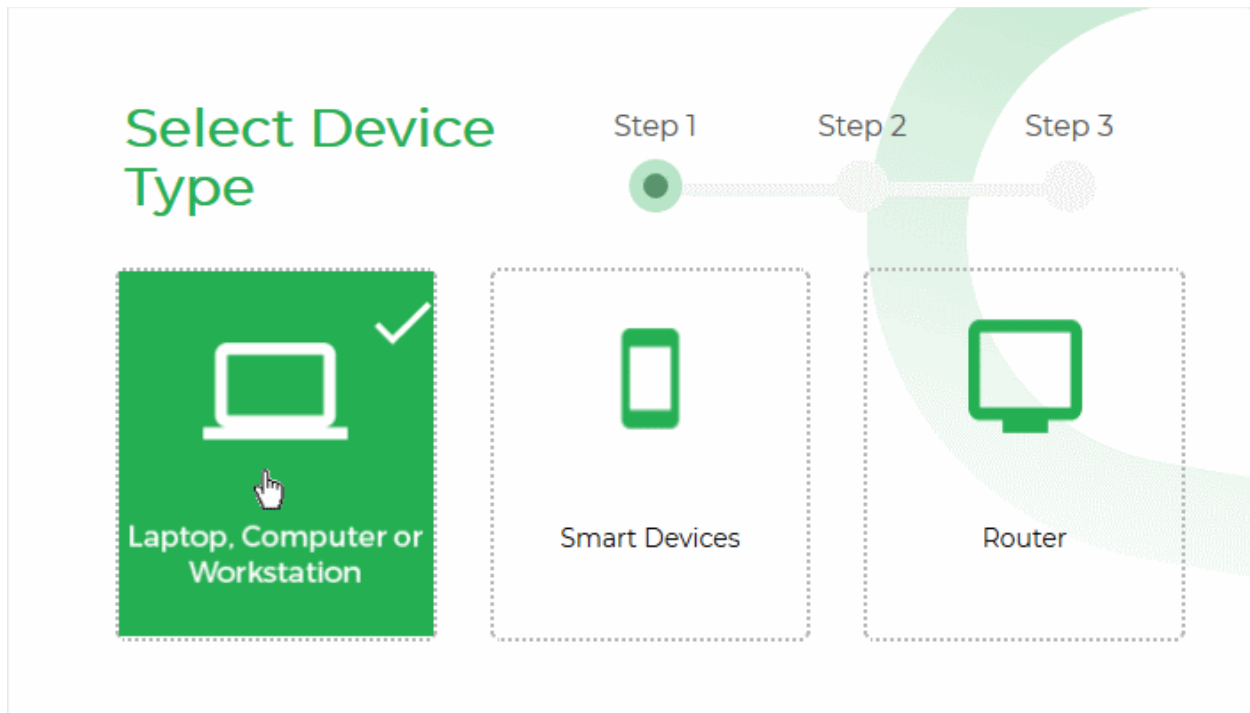
- [Enroll Windows Devices](#)
- [Enroll Smart Devices](#)
- [Enroll Networks](#)

1.3.1 Enroll Windows Devices

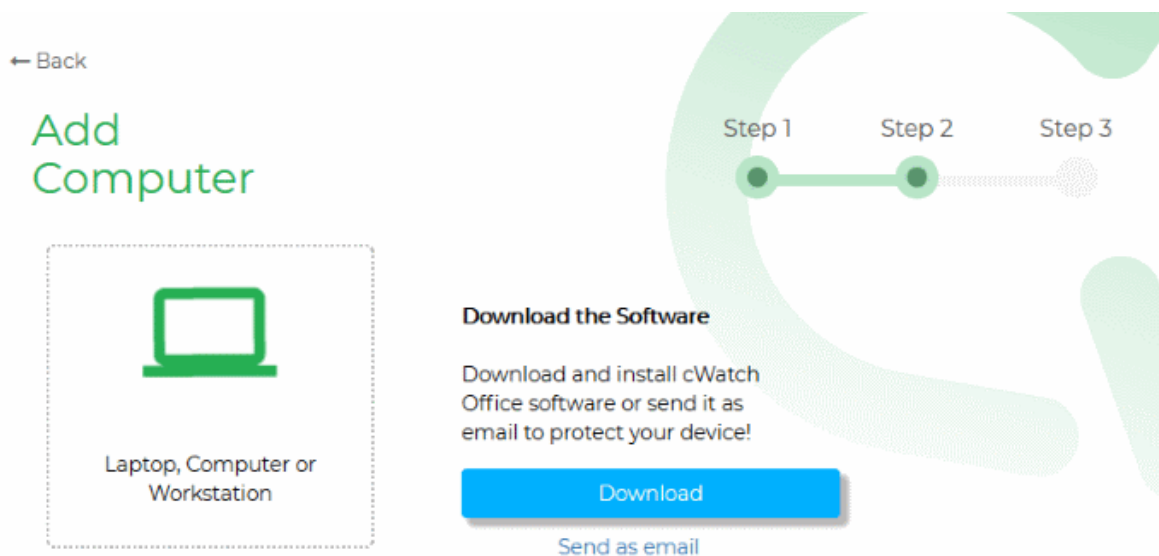
- To enroll a Windows device you need to install an agent on the device
- You can download the agent by clicking 'Protect New Device' on the dashboard
- Default protection settings will be applied to the device immediately after enrollment
- You can edit protection settings for the device from the device dashboard interface as required. See [Manage Protection Settings for a Network/Device](#) for more details.

To enroll a Windows device

- 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:

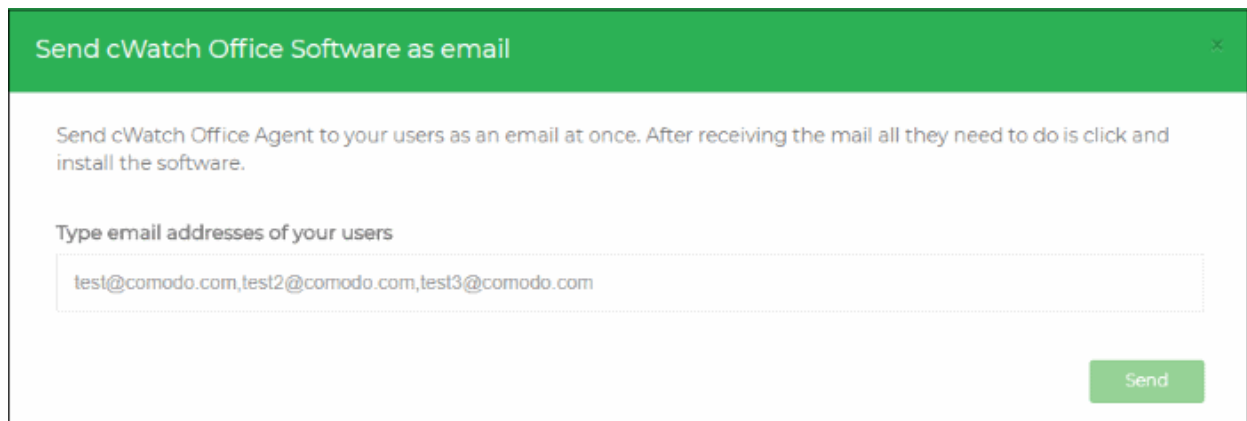


Install the agent on the device

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

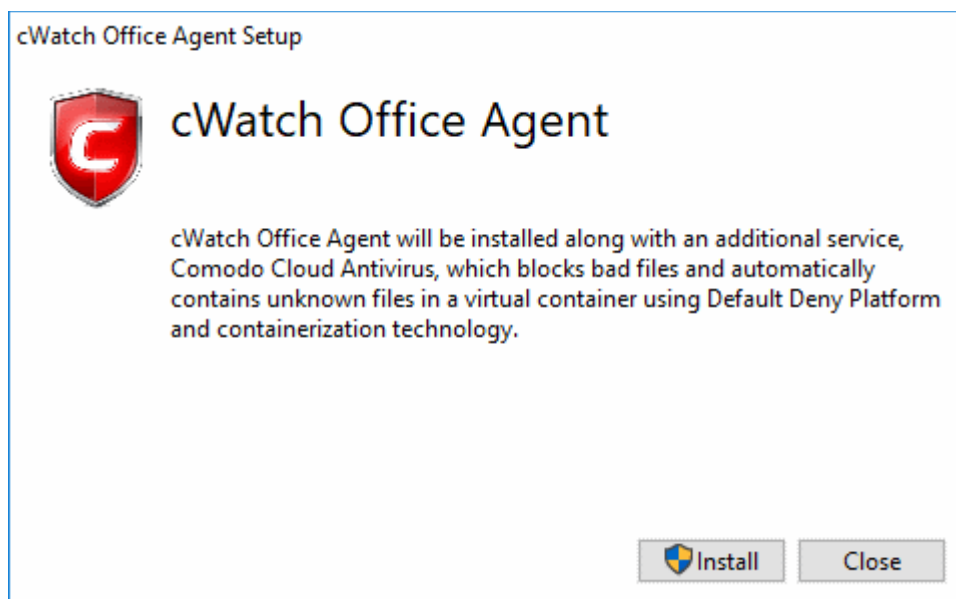
download and install the agent.




- 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.

1.3.2 Enroll Smart Devices

- This section explains how to enroll employee Android and iOS devices for cWatch Office protection
- You need to install the cWatch app on each device you wish to enroll. The app must be activated in order to register it with the cWatch console.
- Android devices also require an SSL certificate to be installed. This is required in order to display the warning page when cWatch blocks a HTTPS website.
- iOS devices require you to trust a certificate installed by cWatch during enrollment. This is necessary in order to display the warning page when cWatch blocks a HTTPS website.
- You can initiate enrollment by sending invitation emails to users from the cWatch Office console. The email contains instructions to download, install and activate the app, and instructions on how to install the SSL certificate.
- Default protection settings will be applied to the device immediately after enrollment
- You can edit protection settings for the device from the cWatch interface. See [Manage Protection Settings for a Network/Device](#) for more details.
- Users can view web traffic stats for their device from the app.
- If a user has cWatch administrator privileges, they can see traffic stats for all devices enrolled to the account.

See the following sections for help to enroll smart devices:

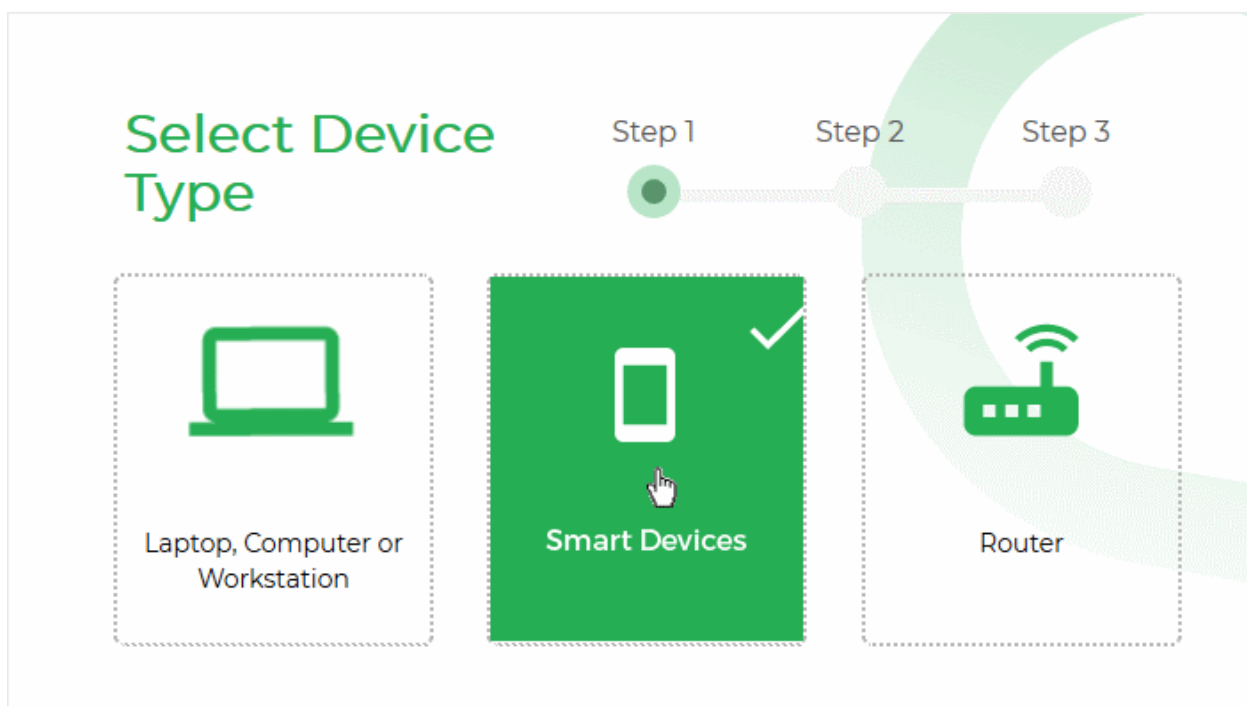
- [Enroll Android Devices](#)
- [Enroll iOS Devices](#)

1.3.2.1 Enroll Android Devices

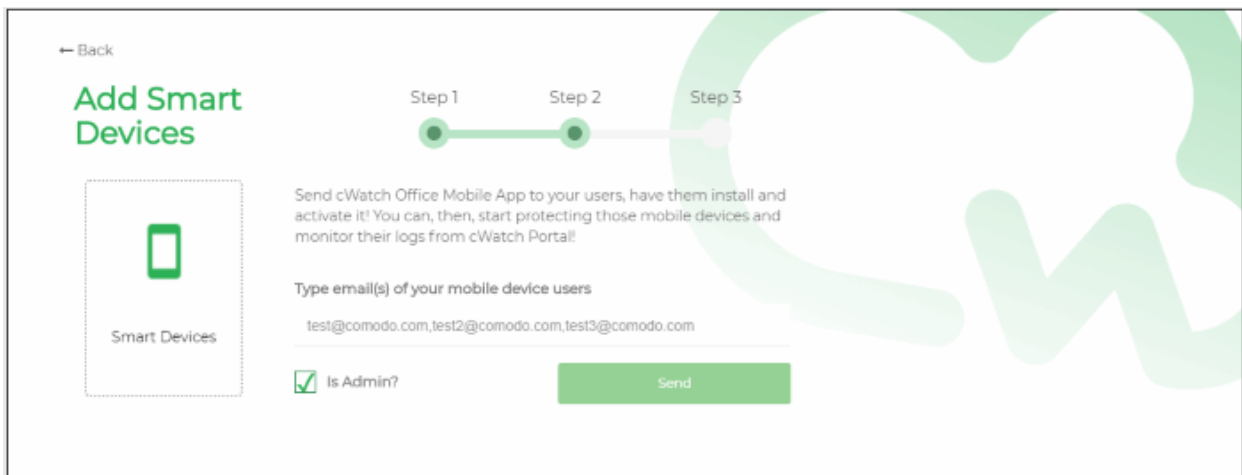
You can initiate enrollment of Android devices by sending invitation mails to users (device owners) from the device enrollment wizard.

To add an Android Device

- Click 'Protect New Device' in the dashboard to start the enrollment wizard.
- Select 'Smart Devices'



The instructions for enrolling an Android device will appear:



← Back

Add Smart Devices

Smart Devices

Step 1 Step 2 Step 3

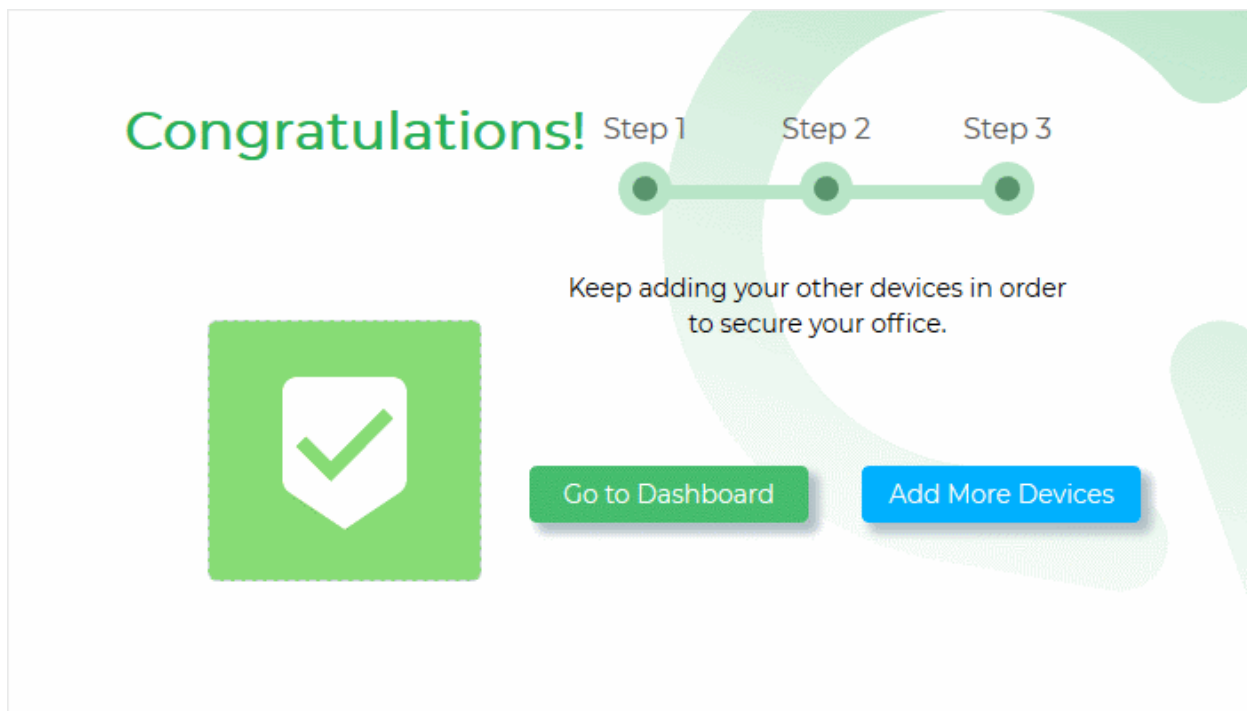
Send cWatch Office Mobile App to your users, have them install and activate it! You can, then, start protecting those mobile devices and monitor their logs from cWatch Portal!

Type email(s) of your mobile device users

test@comodo.com,test2@comodo.com,test3@comodo.com

Is Admin?

- 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:



Comodo cWatch Office

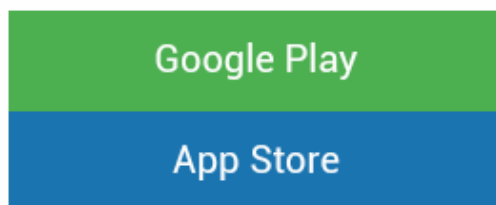
Welcome,

coyoteewile@yahoo.com is using cWatch Office to protect your company against web based attacks and sent you this e-mail to enable protection on your mobile device.

Setting up cWatch Office will take less than 5 minutes.

You need to follow steps below to start your internet security:

Step 1: Install cWatch Office App from Stores



Android App Activation

Step 1: Tap the activation button below.

The end-user now needs to complete three steps to enroll their device:

- **Step 1 - Download and Install the cWatch Office app**
- **Step 2 - Activate the app and register it with cWatch Office**
- **Step 3 - Install the SSL certificate so that the block page is correctly displayed when a HTTPS website is blocked**

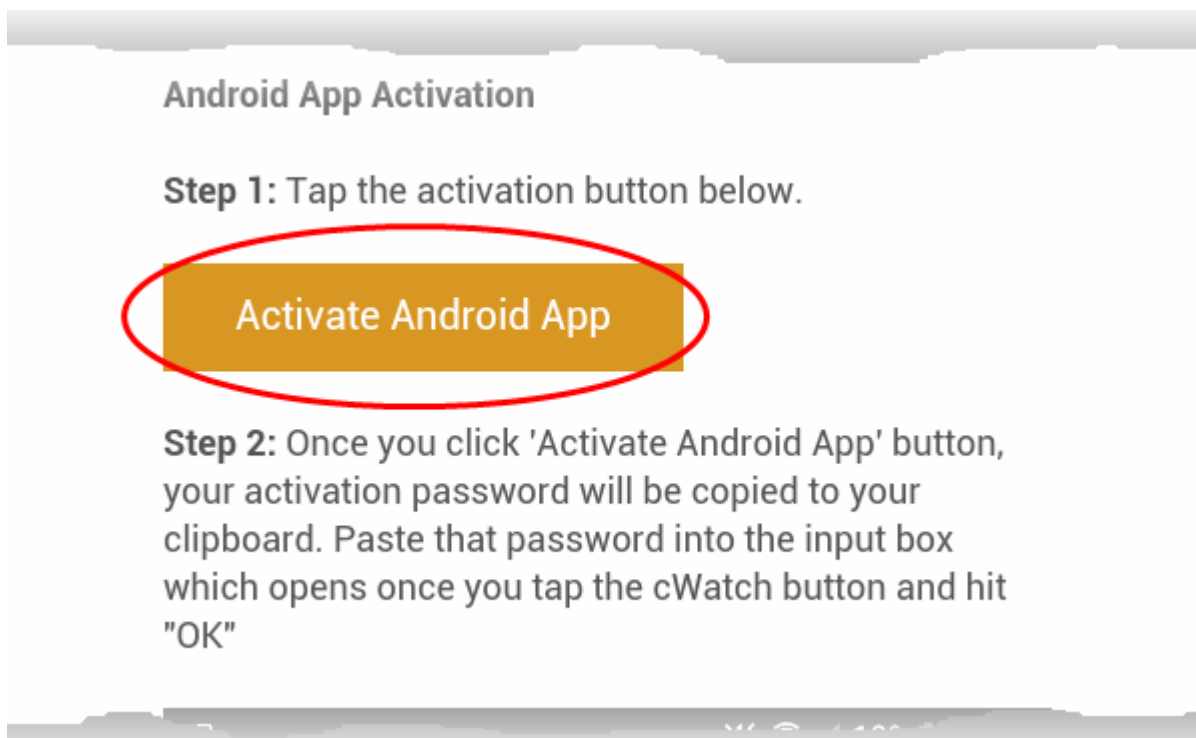
Step 1 - Download and Install the cWatch Office app

- Tap 'Google Play' in 'Step 1' in the enrollment mail

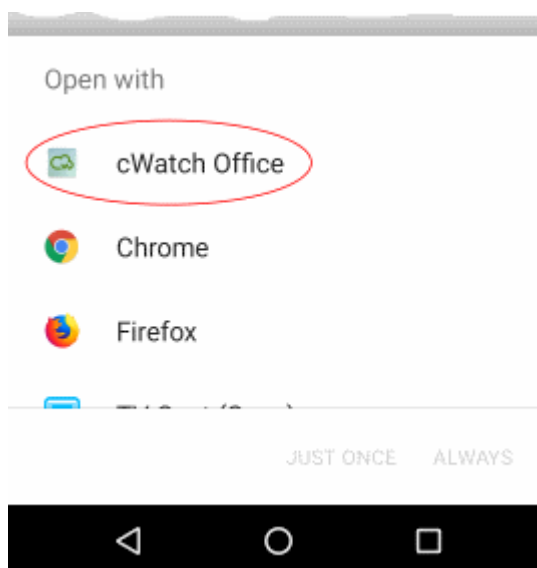
- This will open the Google Play store at the cWatch Office app page.
- Download and install the app on the device

Step 2 - 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':



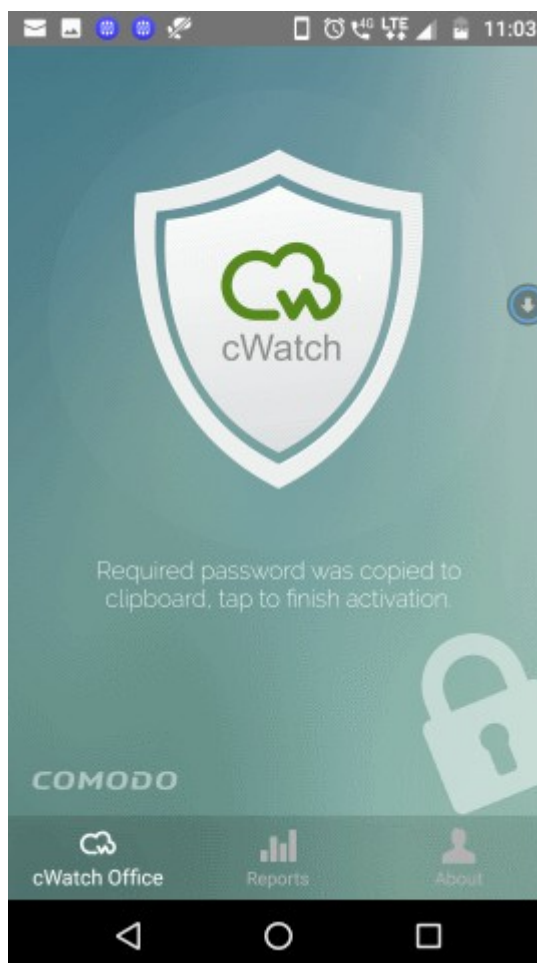
- Choose to open the link with cWatch Office:



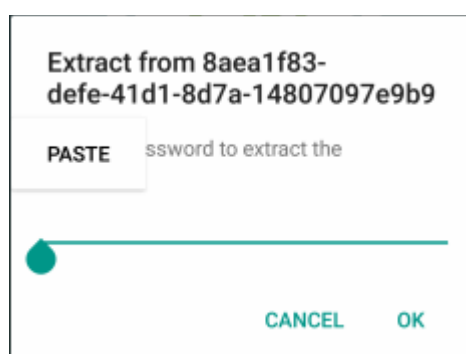
The cWatch app will open and start the registration process with the cWatch Office console.

- 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.

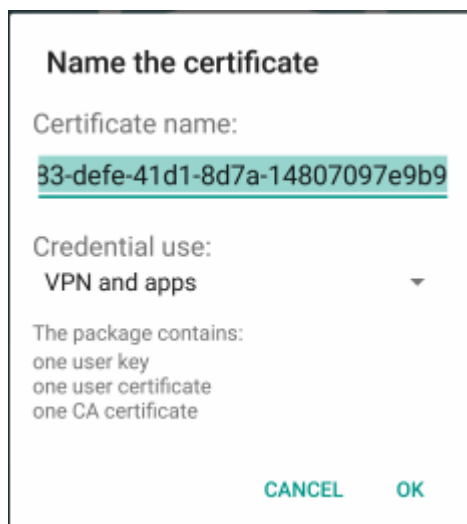
- The user needs to paste this password into the app.
- Tap the cWatch shield to start registration:



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



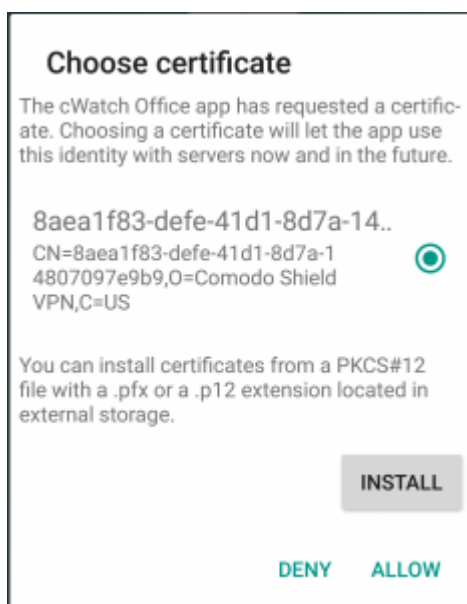
The certificate will be extracted, ready for installation:



- Select 'OK'

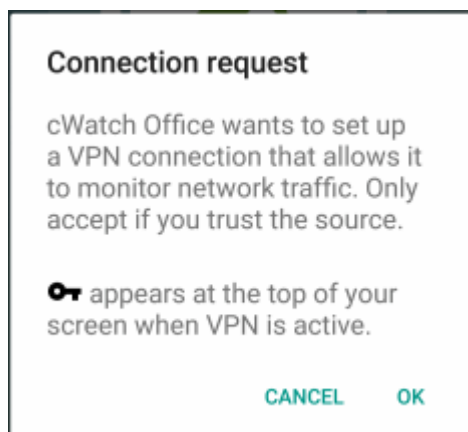
The next step is to install the certificate.

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

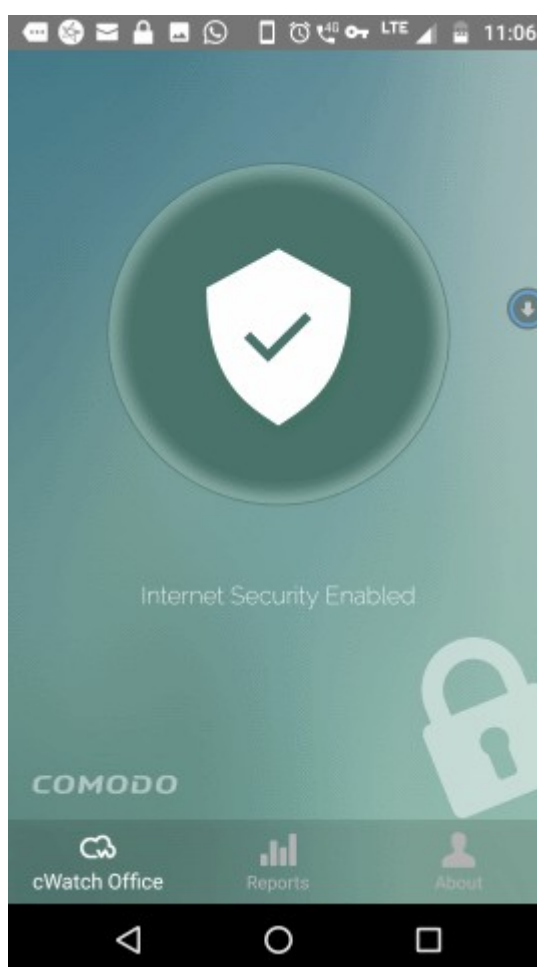


The next step is to allow the VPN connection.

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



Installation and activation is now complete:



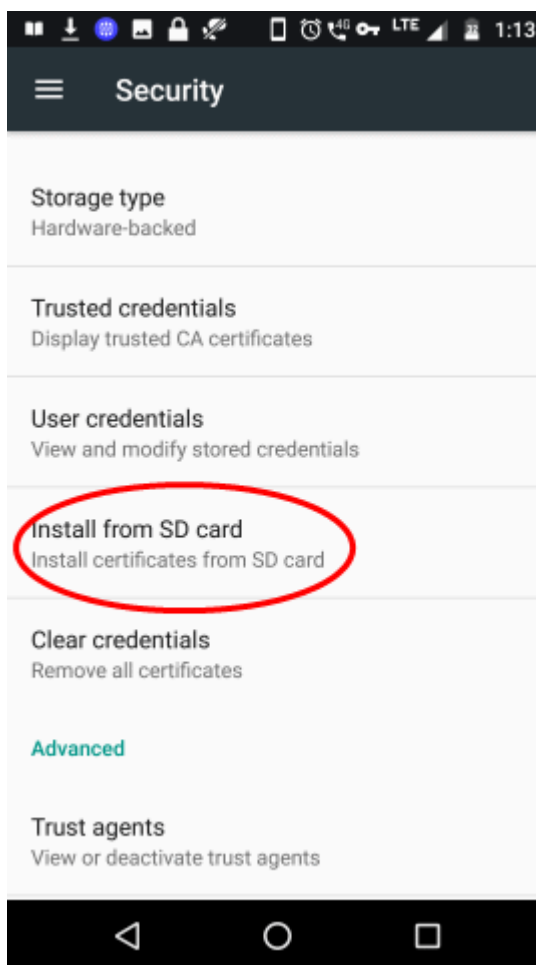
The app will connect to the cWatch Office console and default protection settings will be automatically applied. You can edit the protection settings for the device at any time. See [Manage Protection Settings for a Network/Device](#) for more details.

Step 3 - Install SSL certificate so the warning page is shown when HTTPS sites are blocked

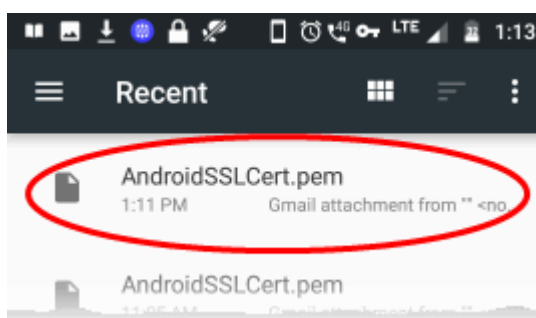
- cWatch office displays a warning page to end-users whenever a website is blocked.
- You need to install an SSL certificate on the device in order to correctly display this warning page when a HTTPS site is blocked.
- The certificate is delivered to users as an attachment to the cWatch invitation mail.
- Users can download the certificate and install it on the device.

To install the certificate

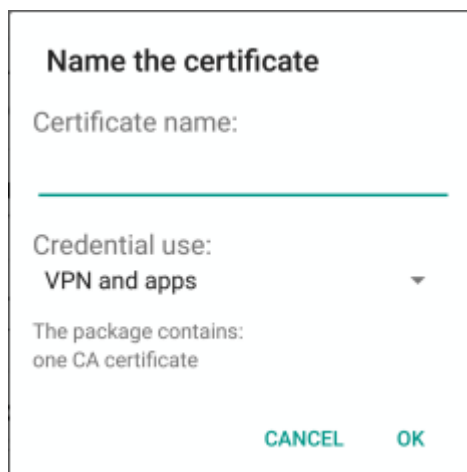
- Download the certificate file ('AndroidSSLCert.pem') from the invitation mail sent to the user
- In Android, open 'Settings' > 'Security' > 'Install from SD Card'



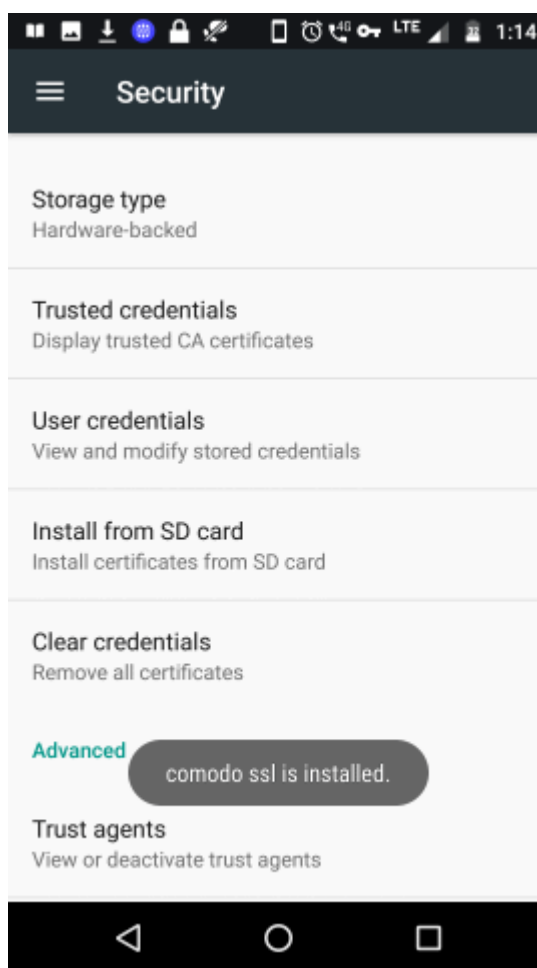
- Select 'AndroidSSLCert.pem' from the list:



- Enter a friendly name for the certificate:



- Click 'OK' to install the certificate

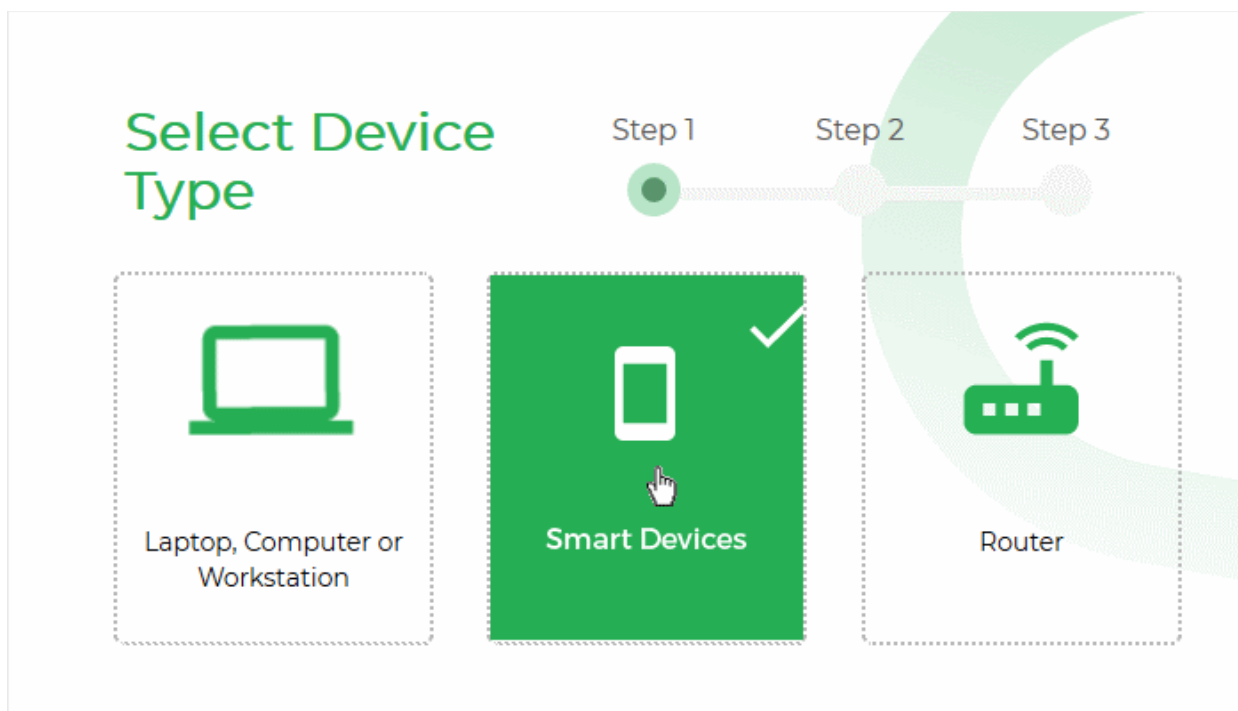


1.3.2.2 Enroll iOS Devices

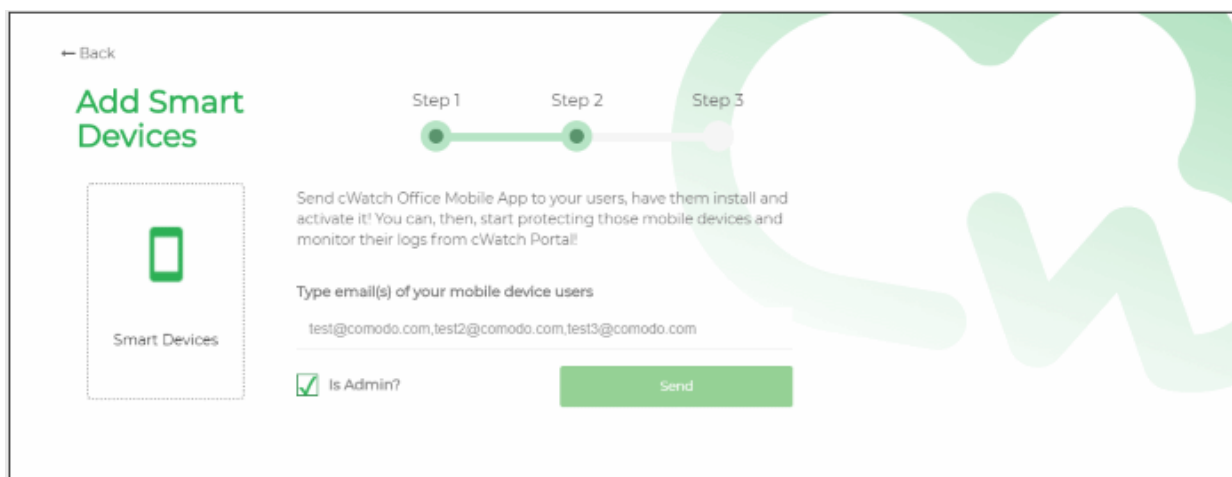
You can initiate enrollment of iOS devices by sending invitation mails to users (device owners) from the device enrollment wizard.

To add an iOS Device

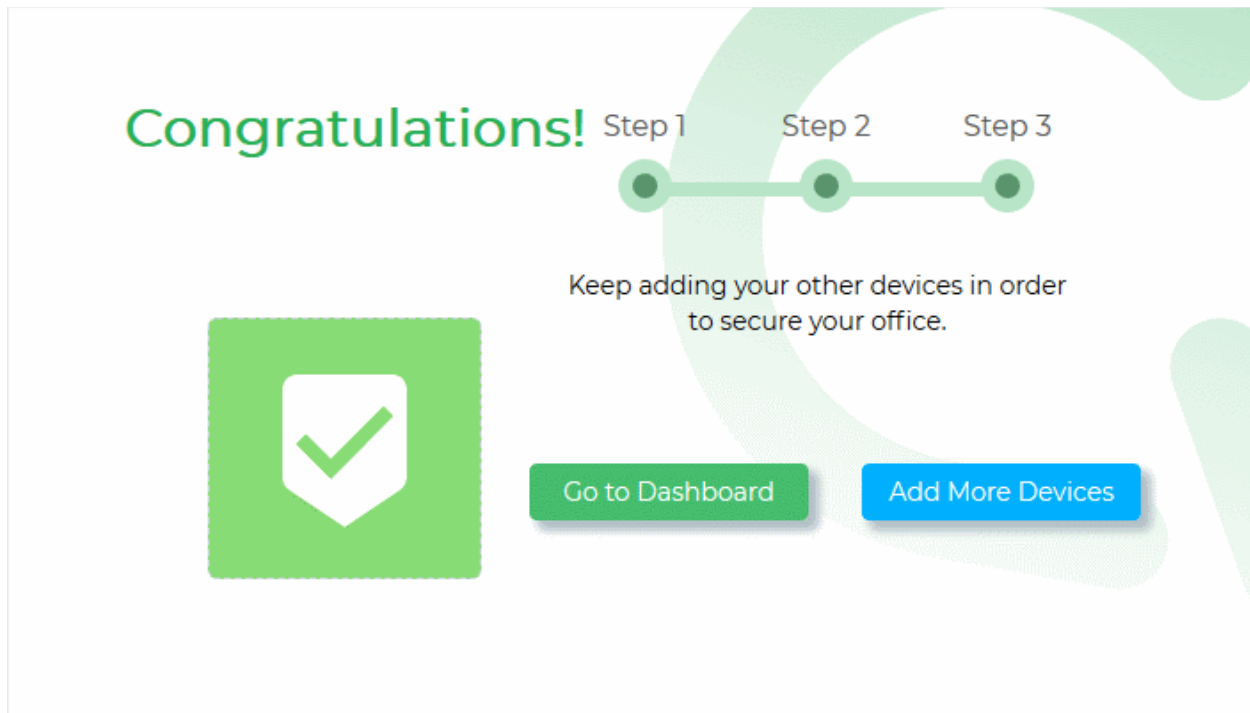
- Click 'Protect New Device' in the dashboard to start the enrollment wizard.
- Select 'Smart Devices'



Instructions for enrolling an iOS device will appear:



- 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 Office.

An example mail is shown below:



Comodo cWatch Office

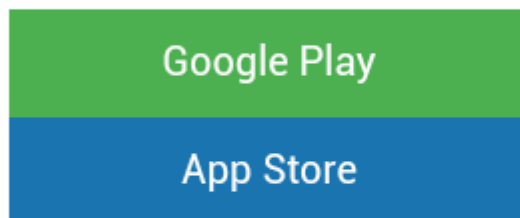
Welcome,

coyoteewile@yahoo.com is using cWatch Office to protect your company against web based attacks and sent you this e-mail to enable protection on your mobile device.

Setting up cWatch Office will take less than 5 minutes.

You need to follow steps below to start your internet security:

Step 1: Install cWatch Office App from Stores



Android App Activation

Step 1: Tap the activation button below.

The end-user now needs to complete three steps to enroll their device:

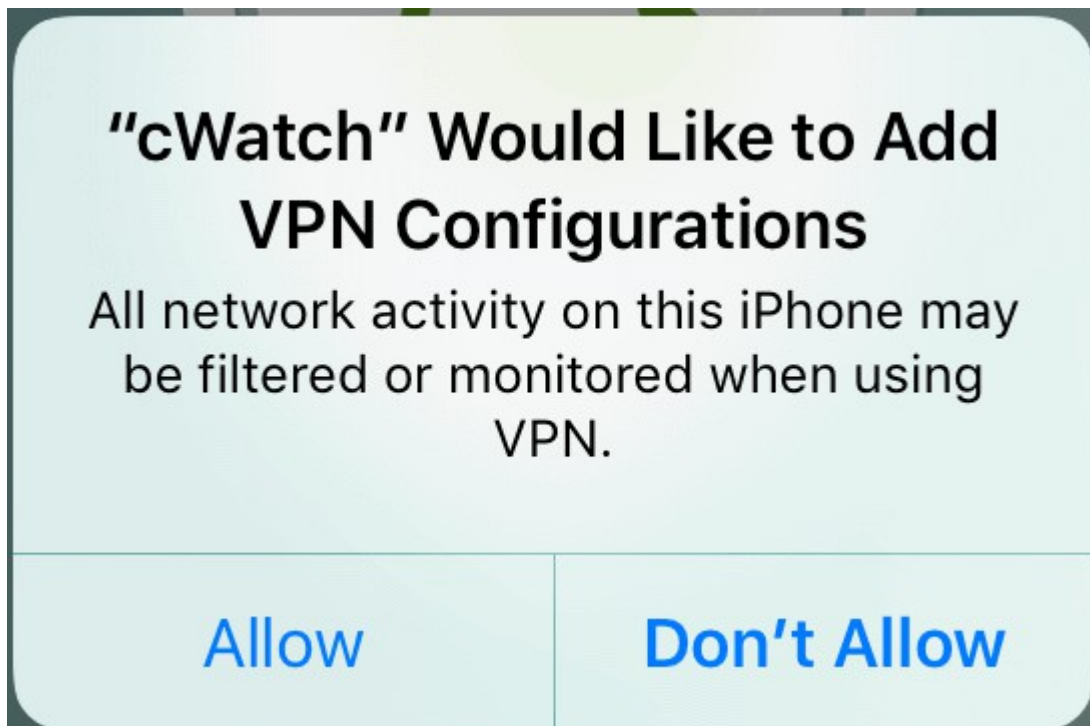
- **Step 1 - Download and Install the cWatch Office app**
- **Step 2 - Configure the VPN connection**
- **Step 3 - Install the SSL certificate so that the block page is correctly displayed when a HTTPS website is blocked**

Step 1 - 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

Step 2 - 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.



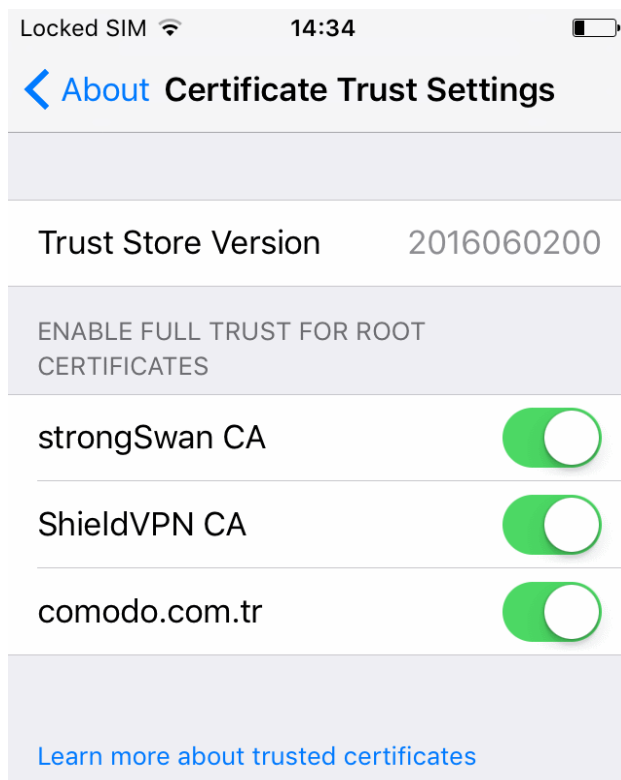
- Click 'Allow'

A new VPN configuration will be created. The app will connect to cWatch Office and the default protection settings will be applied to the device. You can edit protection settings for the device at any time. See [Manage Protection Settings for a Network/Device](#) for more details.

Step 3 - 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'.



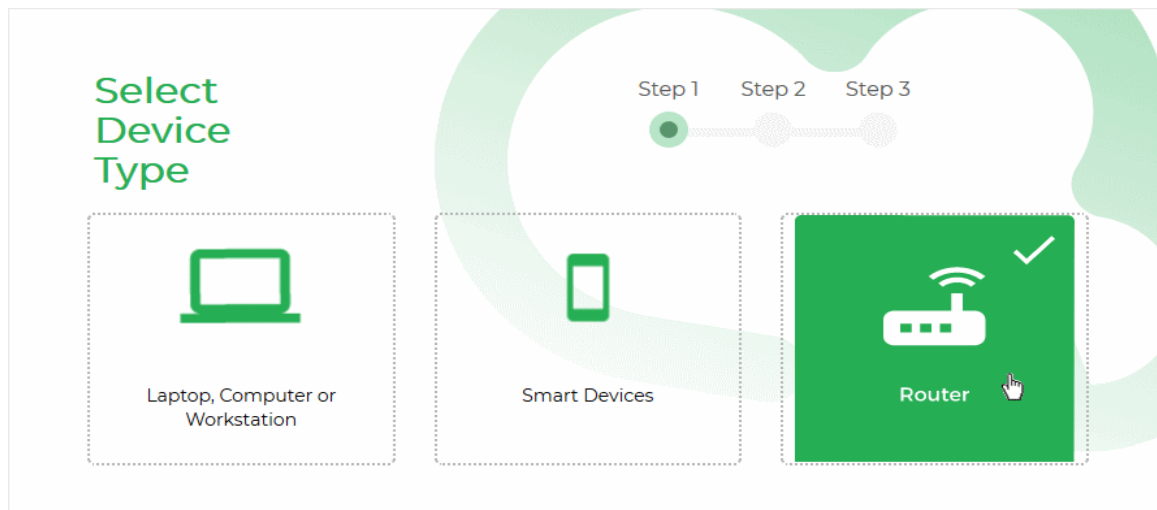
- Enable the certificate named 'comodo.com.tr'

1.3.3 Enroll Networks

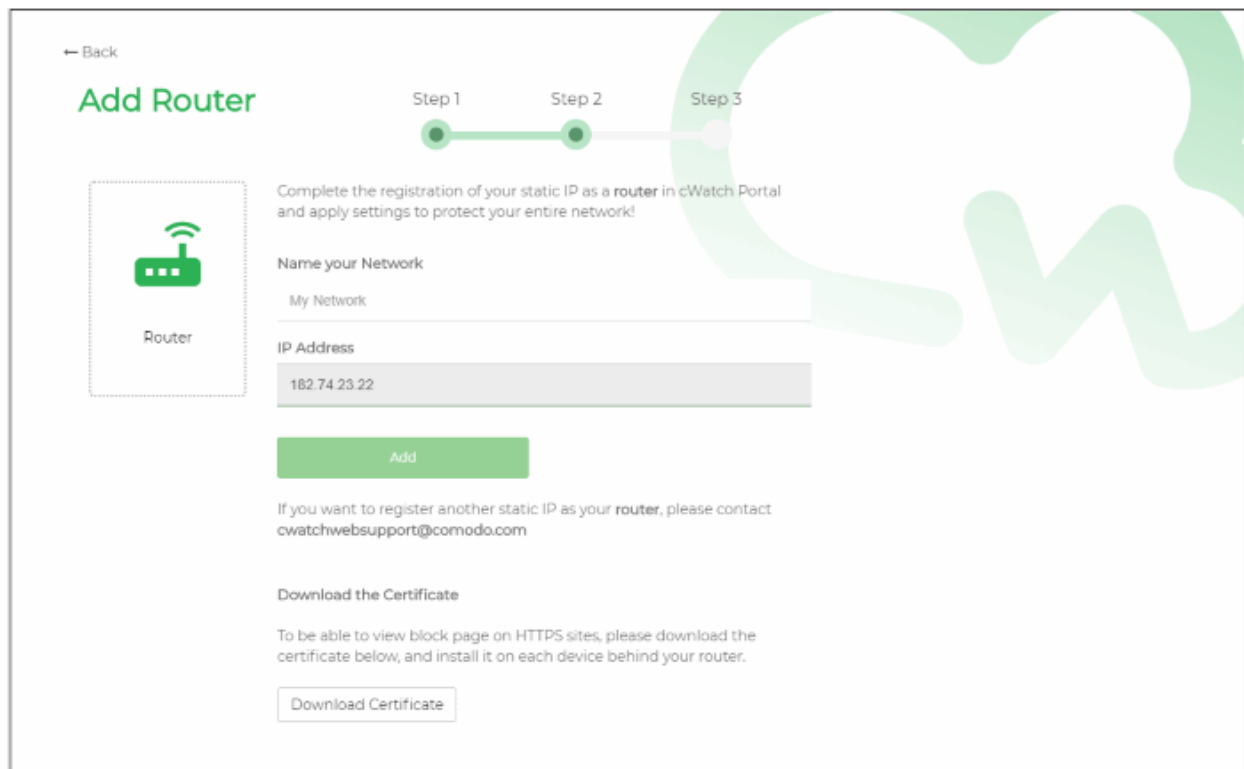
- You can enroll networks with static IP addresses to cWatch Office
- Enrollment of a network requires adding the network IP address to cWatch Office
- The DNS settings of your router needs to be edited, to point to cWatch DNS servers for filtering the web traffic of your network
- An SSL certificate is to be installed on all devices behind the router. This is required in order to display the warning page when cWatch blocks a HTTPS website.
- Default protection settings will be applied to all devices in the network immediately after enrollment
- You can edit protection settings for the network from the device dashboard interface as required. See [Manage Protection Settings for a Network/Device](#) for more details.

To enroll a network

- Click 'Protect New Device' in the dashboard to start the device enrollment wizard.
- Select 'Router'



The instructions for enrolling a network will appear:



Enrolling a network involves three steps:

- **Step 1 - Add network IP address to cWatch console**
- **Step 2 - Configure DNS settings on the router**
- **Step 3 - Install the SSL certificate so that the block page is correctly displayed when a HTTPS website is blocked**

Step 1 - 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.

The network will be added and displayed in the 'Devices' list on the left.

Step 2 - 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

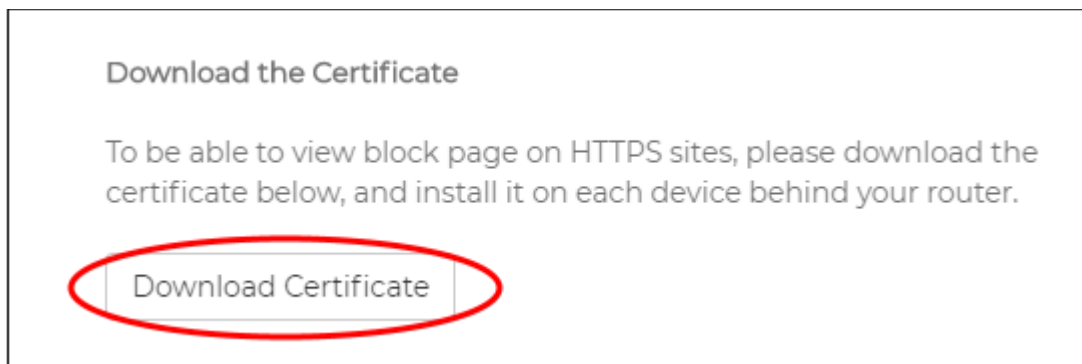
cWatch Office will now be placed between internet and your router and act as your Internet Gateway. For guidance on configuring your router, see the tutorial at <https://www.comodo.com/secure-dns/switch/router.html>.

Step 3 - 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 can download the certificate and install it on their device.

To download the certificate

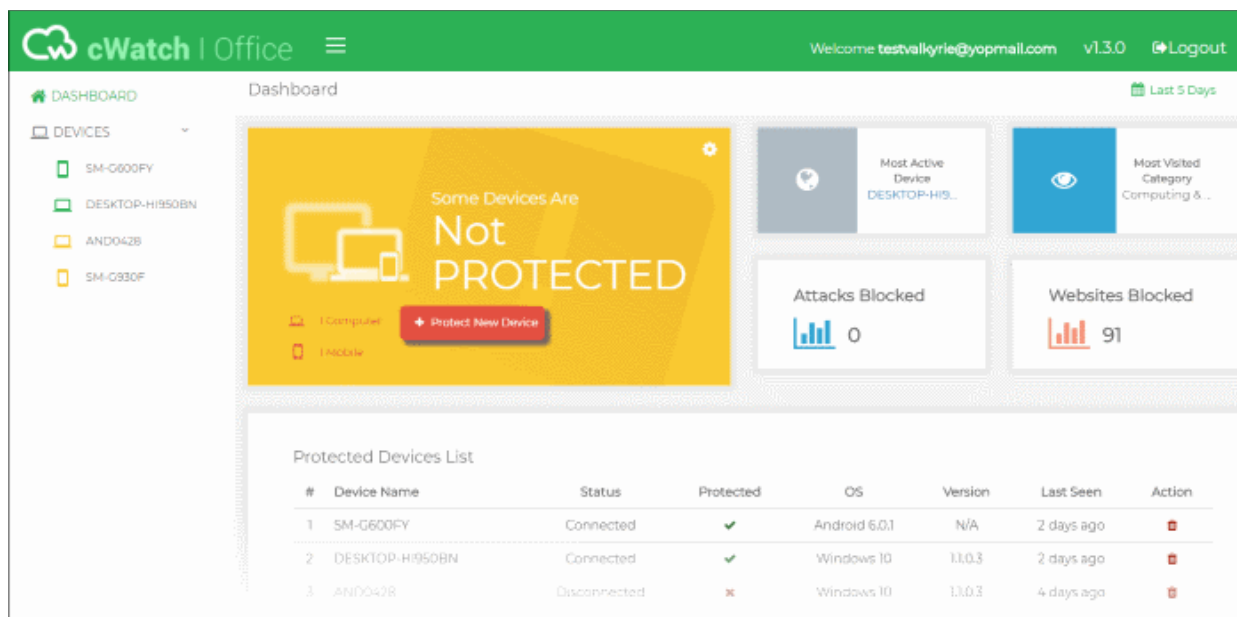
- Click Download Certificate on the instructions page and save the file 'blockpage.pem'



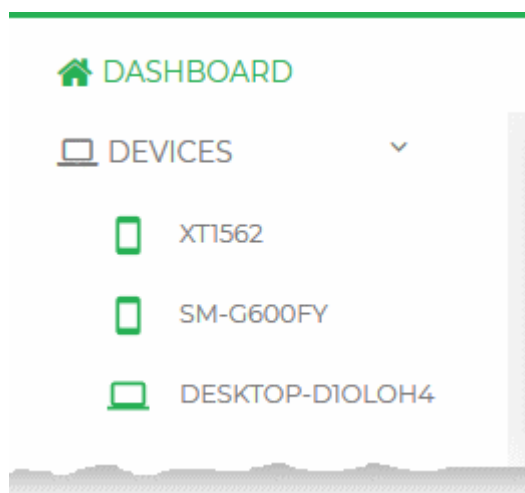
- Send the certificate file to the user of devices on your network
- The users can install the certificates on their devices

2 The Admin Console

The cWatch admin console allows you to add networks and devices, create protection settings, view dashboard statistics and more.



- The menu on the left contains a link to the dashboard and lists all devices added to your account.
- Click on a device to view its details and edit its protection settings.



- **Dashboard** - Opens the dashboard of your cWatch Office account. The dashboard shows statistics on blocked websites on protected networks and devices. You can also add new devices from here. See [The cWatch Office Dashboard](#) for more details.
- **Devices** - Lists devices and networks enrolled for cWatch protection.
The color of the device icon indicates the state of its connection to cWatch Office.
 - Green - Device is connected and protected
 - Yellow - Device is currently disconnected
 - Gray - The registration of the device is pending
- Click a device name to view an overview of device activity in the right pane. The overview shows statistics on websites blocked on the device. You can also edit device protection settings from here. See [The Device Overview](#) for more details.

3 The cWatch Office Dashboard

The dashboard shows top-level data on the networks and devices protected by cWatch Office. Statistics include websites and attacks blocked, recent events, live surfing monitor and more. This allows you to quickly identify harmful websites visited by users and effectively track the risks associated with each device.

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

#	Device Name	Status	Protected	OS	Version	Last Seen	Action
1	SM-G600FY	Connected	✓	Android 6.0.1	N/A	2 days ago	⛔
2	DESKTOP-H950BN	Connected	✓	Windows 10	1.1.0.3	2 days ago	⛔
3	AND042B	Disconnected	✗	Windows 10	1.1.0.3	4 days ago	⛔

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

all.com v1.3.0 Logout

Last 30 Minutes

Last 1 Hour

Last 12 Hours

Last 1 Day

Last 3 Days

Last 5 Days

Last 7 Days

Custom range

Apply Cancel

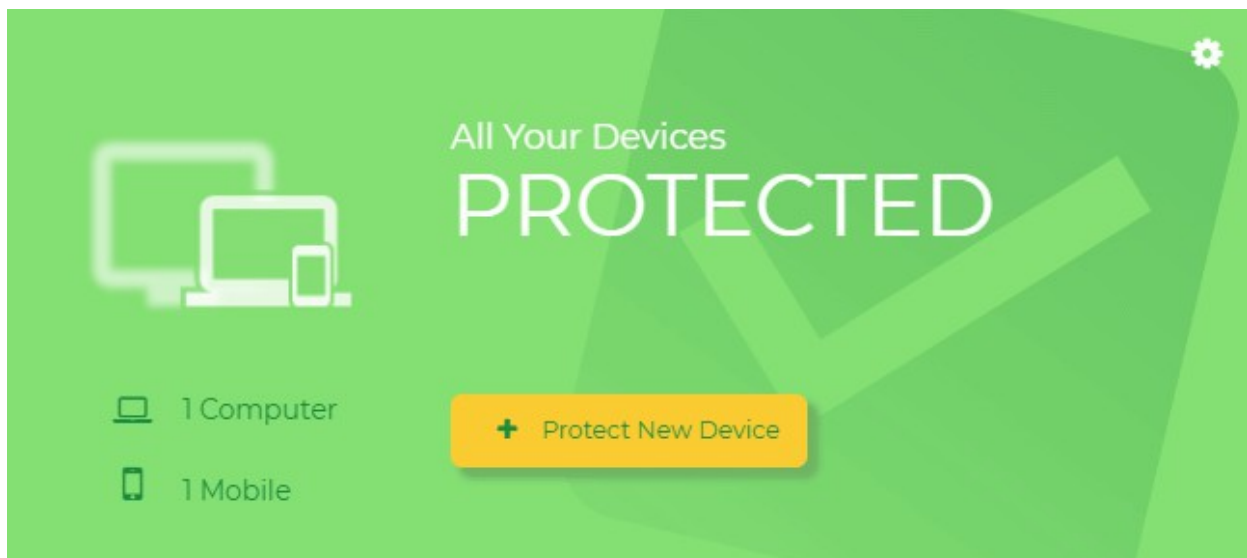
- Statistics are shown for the last 30 minutes by default
- You can change this by clicking the link at top-right and choosing a different range
- Click 'Custom range' to choose a specific date range
- Click 'Apply' to view statistics for the selected range

The 'Dashboard' contains the following tiles:

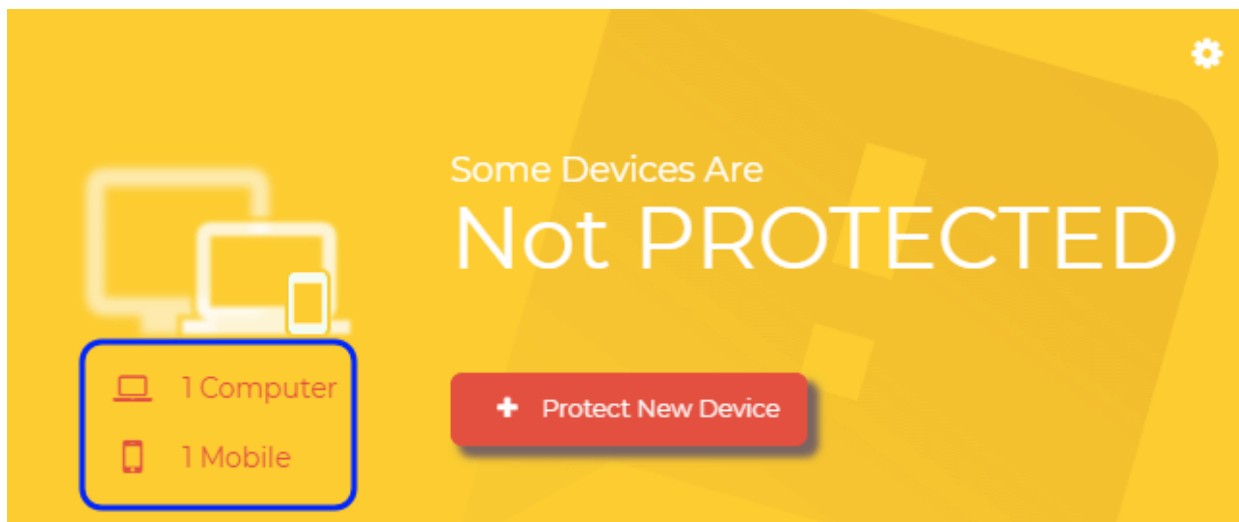
- **Overall protection status**
- **Most active device**
- **Most visited category**
- **Attacks blocked**
- **Websites blocked**
- **Protected Devices List**
- **Live web surfing monitor**
- **Important events**
- **Most visited websites**
- **Most blocked categories**
- **Last visited websites**
- **Top devices**


Overall Protection Status

The overall protection tile shows how many enrolled devices are connected to **cWatch protection**. It also allows you add new networks/devices and view default protection settings.



- The color of the tile indicates the overall protection status:
 - Green - All enrolled devices are connected and protected
 - Yellow - Some devices are offline or not connected to cWatch
 - The number of unprotected devices is shown at the bottom-left:

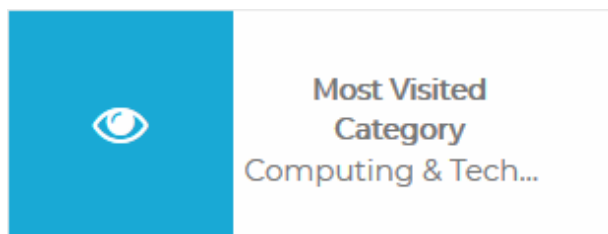
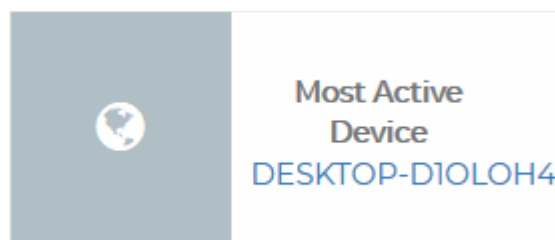


- Click 'Protect New Device' to enroll new devices or networks to cWatch Office protection. See [Add Networks and Devices](#) if you need more help with this.
- Click the gear icon at top-right  to view the default protection settings applied to devices after enrollment. See [View Default Protection Settings](#) for more details.

Most Active Device

The device which has visited the most web pages within the selected time period. This includes to both allowed and blocked websites.

Click the device name to view dashboard statistics for the device. See [The Device Overview](#) for more details.



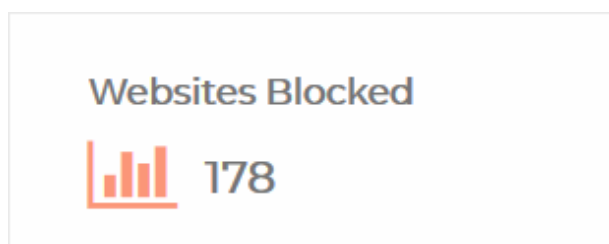
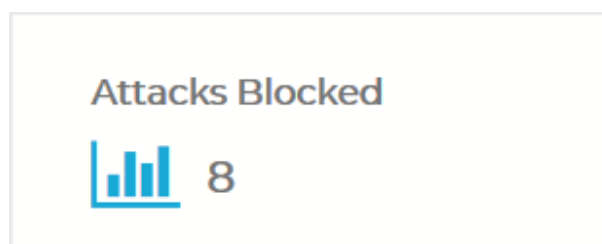
Most Visited Category

The website category visited most often by devices in your cWatch network.

Attacks Blocked

The total number of attacks blocked on all enrolled devices/networks within the selected period.

Tip: The 'Default Protection Settings' page lets you view the types of attacks that cWatch blocks. See [Attack Categories and Threats](#) in [View Default Protection Settings](#) for more details.



Websites Blocked

The total number of website access attempts that were intercepted and blocked on all devices.

The number of sites blocked depends on the protection settings active on your devices/networks.

Protected Devices List

Shows all devices that have been enrolled for cWatch Office protection.

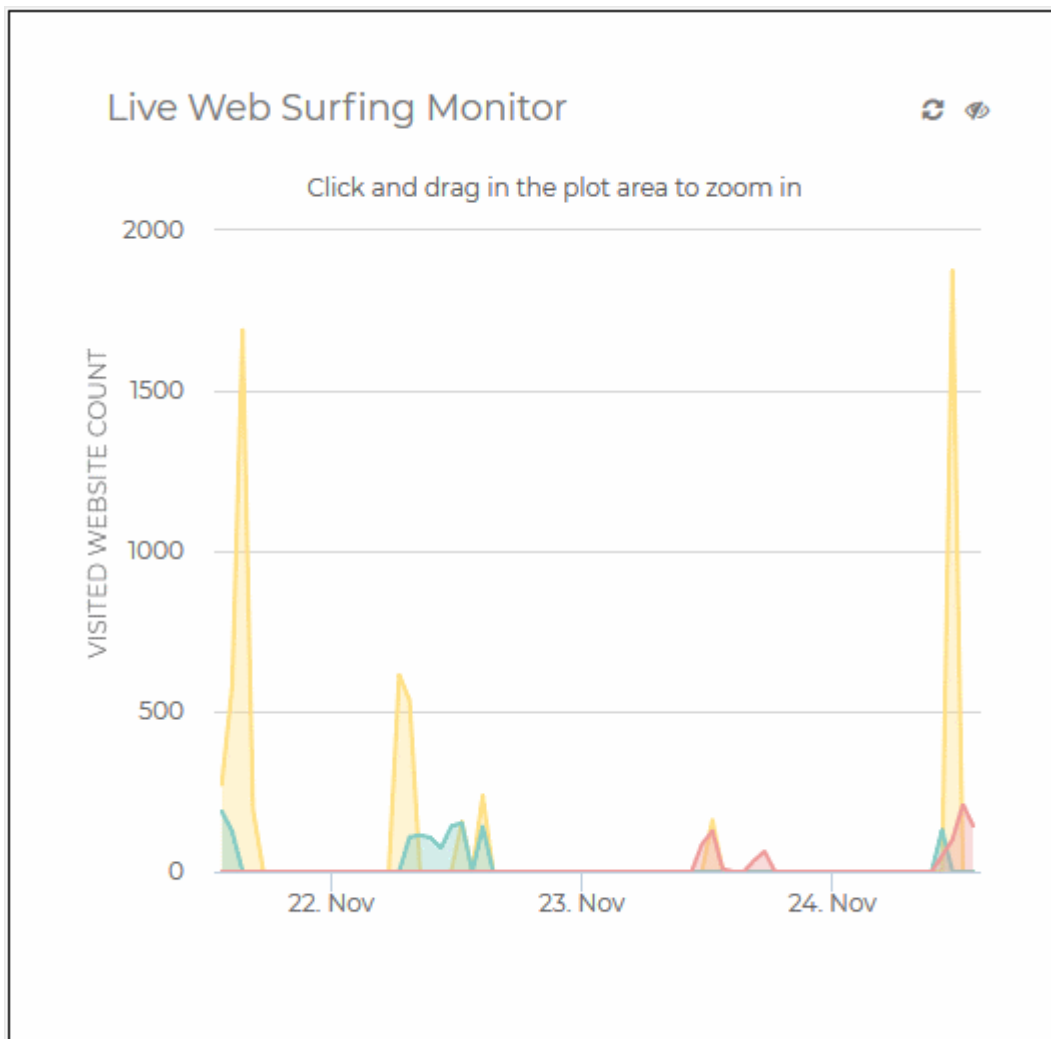
Protected Devices List							
#	Device Name	Status	Protected	OS	Version	Last Seen	Action
1	SM-G600FY	Connected	✓	Android 6.0.1	N/A	2 days ago	
2	DESKTOP-HI950BN	Connected	✓	Windows 10	1.10.3	2 days ago	
3	AND0428	Disconnected	✗	Windows 10	1.10.3	4 days ago	
4	SM-G930F	Disconnected	✗	Android 7.0	N/A	6 days ago	

Protected Devices List - Column Descriptions

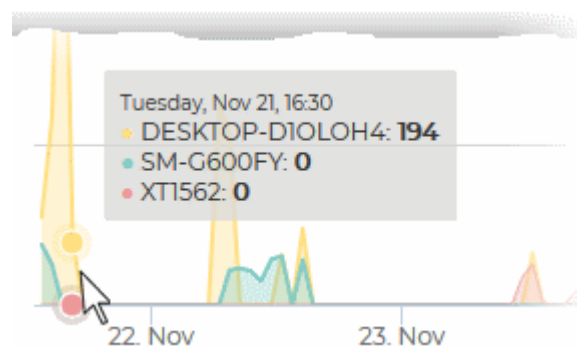
Column Header	Description
Device Name	The label of the enrolled device
Status	Whether or not the device is currently connected to cWatch Office. A device must first be connected for it to become protected.
Protected	Whether or not the device is currently protected by cWatch Office.
OS	The operating system version of the device
Version	The version number of the cWatch Office agent. This applies to Windows devices only.
Last seen	The most recent web browsing activity recorded for the device.
Action	Remove the device from cWatch Office. <ul style="list-style-type: none"> Click the trashcan icon to delete the device

Live Web Surfing Monitor

Shows the number of websites visited by each enrolled device during the selected time-period.



- Each device is shown in a different color.
- Select a portion of the graph to zoom-in.
- Place your mouse over a point in the chart to view the number of websites visited by a device at that time-point.



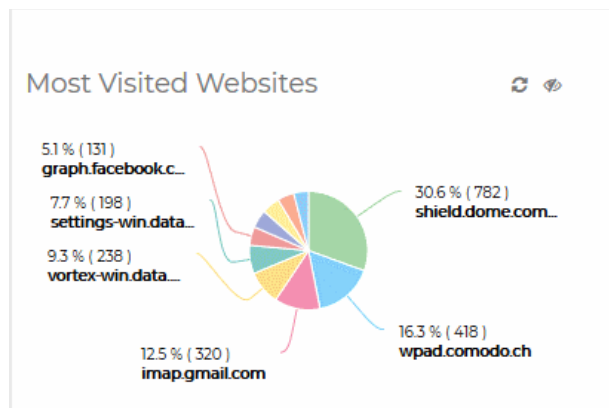
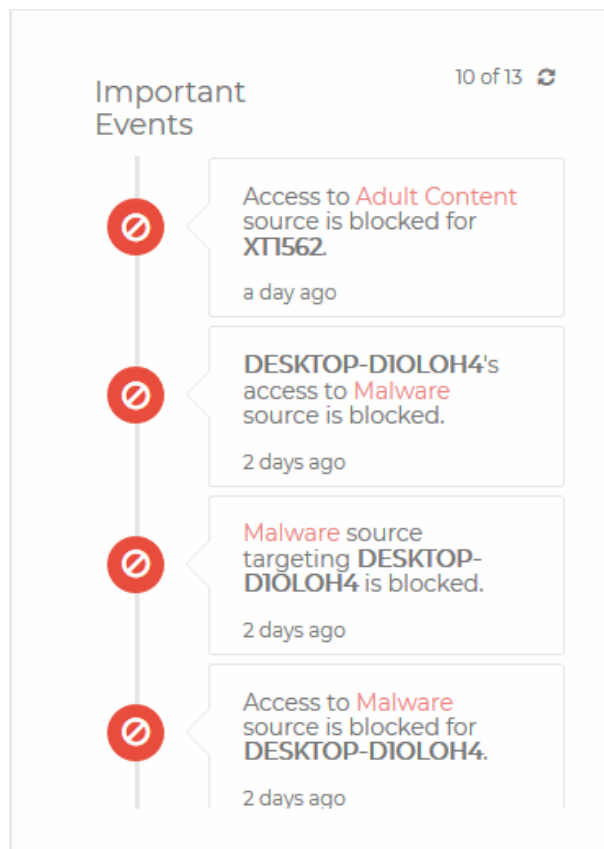
Important Events

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.



- Click  to refresh the data

Tip: The 'Default Protection Settings' page lets you view the types of attacks that cWatch blocks. See '**Attack Categories and Threats**' in **View Default Protection Settings** for more details.



Most Visited Websites

The ten websites visited most often by all devices in your cWatch network.



- Place your mouse on a sector to view the precise number of times the website was accessed.
- Click  to refresh the data
- Click  to view the legends used in the graph

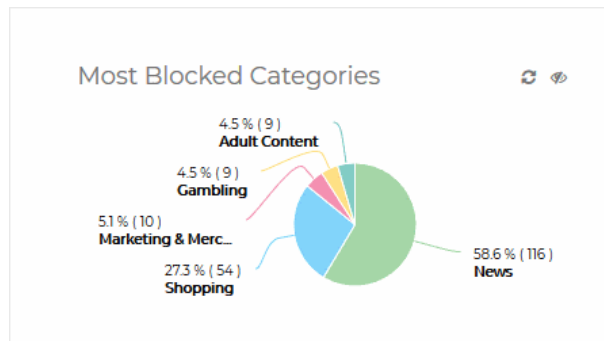
Most Blocked Categories

The ten website categories which were most often visited and blocked in your cWatch network.

The categories blocked depends on the protection settings active on your devices/networks.

See **Manage Protection Settings for a Network/Device** for more details on protection settings.

- Place your mouse on a sector to view the precise number websites blocked in that category.
- Click  to refresh the data
- Click  to view the legends used in the graph



Last Visited Websites



#	Web Site Name	Last Seen
1	analytics.ff.avast.com	2 hours ago
2	wpad.comodo.ch	2 hours ago
3	shield.dome.comodo.com	2 hours ago
4	api.media.jio.com	2 hours ago
5	settings.crashlytics.com	2 hours ago
6	update.googleapis.com	2 hours ago
7	ad.doubleclick.net	2 hours ago
8	b-graph.facebook.com	2 hours ago
9	wzrkt.com	2 hours

Last Visited Websites

The 100 websites most recently visited by devices in your cWatch network.

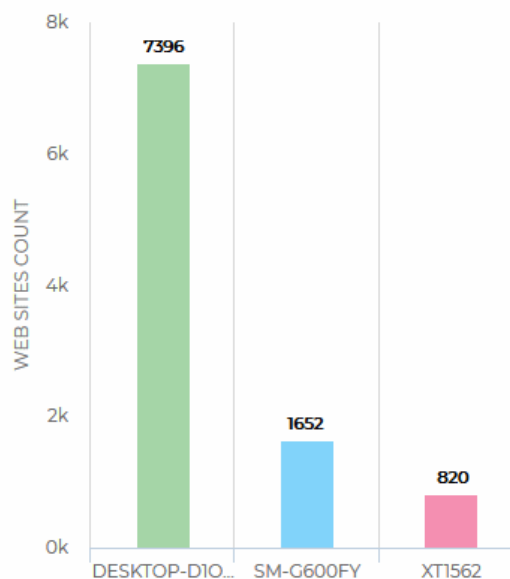
- Click to refresh the list.

Top Devices

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

- Place your mouse on a bar to view the precise number websites visited by that device.
- Click to refresh the data
- Click to view the legends used in the graph

Top Devices




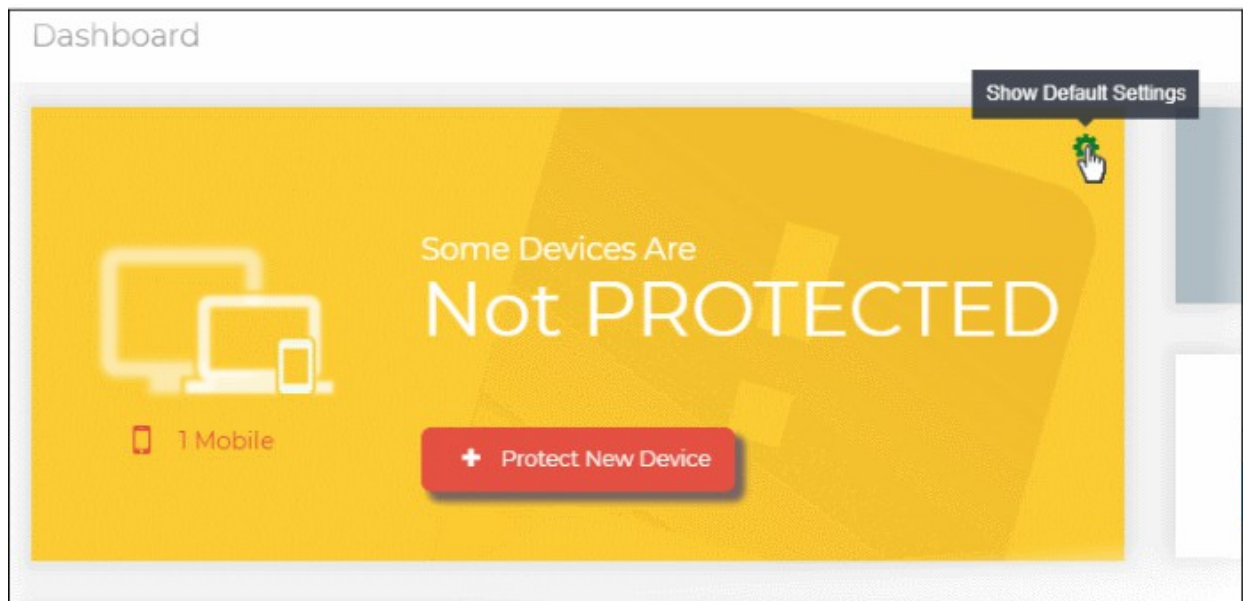
3.1 View Default Protection Settings

- Click 'Dashboard' in the left-hand menu
- Click the gear icon in the corner of the main, protection summary tile
- This will open a page that lists the default protection settings which are applied to newly enrolled devices
- You can view the default settings here, but cannot edit them
- You can change the settings on a particular device as follows:
 - Click the device name you wish to modify on the left
 - Click the gear icon in the corner of the main, protection summary tile
 - Modify the protection settings as required

- Click 'Save' to apply your changes. You can also apply these settings to other devices.

Web site categories

- 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.
- You can add or remove categories from a device or whitelist/blacklist specific websites
 - A whitelisted website is always allowed regardless of the category to which it belongs
 - A blacklisted website is always blocked regardless of the category to which it belongs
- To view global defaults, click 'Dashboard' then the gear icon  in the corner of the main, protection summary tile:



- Scroll down to view website categories which are blocked or allowed:

Device Default Settings

← Back

Default Office Web Browsing Settings

These are the Default Settings for the Internet traffic in your office. These settings are applied to **all devices** registered to this account.

If you want to define specific rules for any device;

1. Click on the device you want to change settings of,
2. Click **Change Settings** button on that device's page,
3. Select any categories you want to block or allow,
4. Click **Save**.


Default Protection Settings

cWatch Office by default secures your internet traffic by blocking below threat types. All added devices will be applied by this policy. You can track blocked threats in your Dashboard under Important Events tab.

Phishing attacks **BLOCKED**

Marketing-Merchandising	ALLOWED
Intimate Apparel & Swimwear	ALLOWED

[Reset Device Specific Rules](#)

- You can modify categories/create whitelists/blacklists for a particular device as follows:
 - Click the device name you wish to modify on the left
 - Click the gear icon  in the corner of the main, protection summary tile
 - Modify website categories as required. Create whitelists/blacklists as required.
 - Click 'Save' to apply your changes. You can also apply these settings to other devices.

Attack Categories and Threats:

- The top of the 'Default Protection Settings' page shows the types of threats that are blocked by cWatch.
- Websites which host these threat types are permanently blocked on all protected devices.
 - Note - You cannot disable or modify protection against these threat types on a per-device basis (like you can with website categories).

- The list includes: Phishing attacks
- Botnet, C&C Servers, Bot Infected Sources
- Malicious & Malware Domains
- Webspam, Spam Sources
- Spyware
- Drive-by Downloads
- TOR Nodes, Bitcoin Miners, Blackhole Systems, Fake AV/PUA Sources
- Brute Force attack sources, Port Scanners, Known DDOS Sources, Remote Access Services

The **'Important Events'** tile in the dashboard shows the log of events at which these threats were blocked on the protected devices and networks.

Default Web Surfing Settings

The 'Default Web Surfing Settings' area displays a list of website categories that can be selectively blocked/allowed. The table below shows the default settings for these categories:

Website Category	Status
Adult Content	Blocked
Social Networks	Allowed
News Websites	Allowed
Sports Related Websites	Allowed
Gambling Websites	Allowed
Shopping Websites	Allowed
Personal and Dating Services	Allowed
Chat Services	Allowed
Gaming Sites	Allowed
Advertising and PopUps	Allowed

- You can change these settings for specific devices or websites if required. See **Manage Protection Settings for a Network/Device** for more details.

Additional Categories Summary

This area displays a list of miscellaneous website categories that can be selectively blocked/allowed. The table below shows the categories that are allowed or blocked by default:

Website Category	Status
Job Search and Career Development	Allowed
Entertainment	Allowed
Hosted Personal Pages	Allowed
Instant Moderated Forums	Allowed
Blogs and Wikis	Allowed

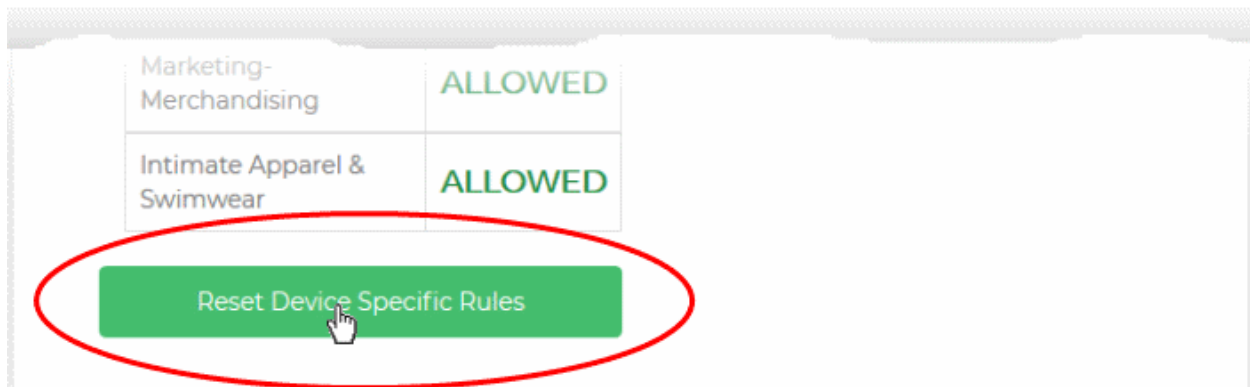
Advocacy - NGO	Allowed
Health	Allowed
Marketing and Merchandising	Allowed
Intimate Apparel & Swimwear	Allowed

- You can change these settings for specific devices or websites if required. See [Manage Protection Settings for a Network/Device](#) for more details.

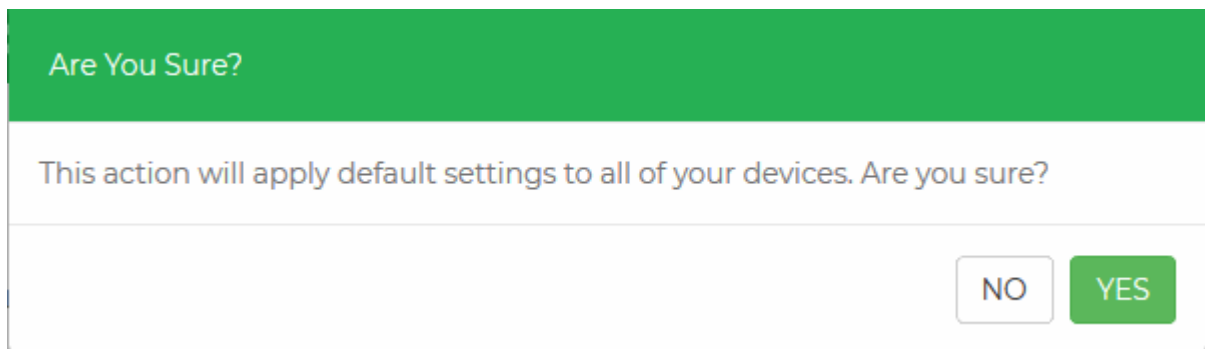
Revert Protection Settings of Devices and Networks

The 'Default Protection Settings' page also lets you reset to default any custom settings on your devices.

- To reset settings on all devices, click 'Reset Device Specific Rules' at the bottom of the page



A confirmation dialog will appear:



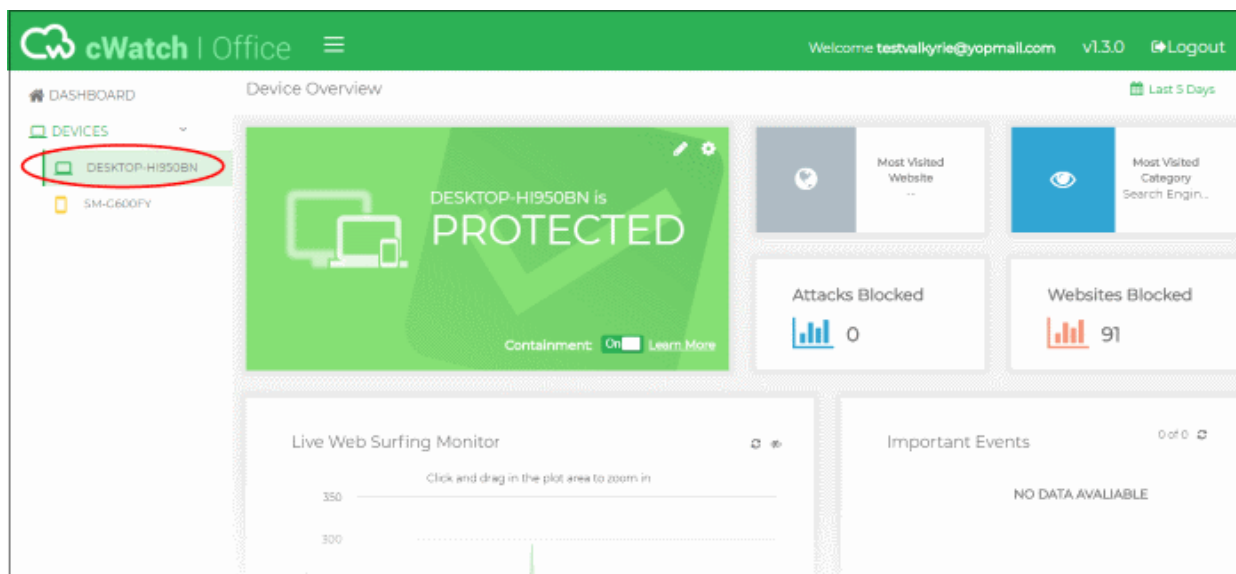
- Click 'Yes'

All enrolled devices will be applied with the default settings, overwriting the existing settings.

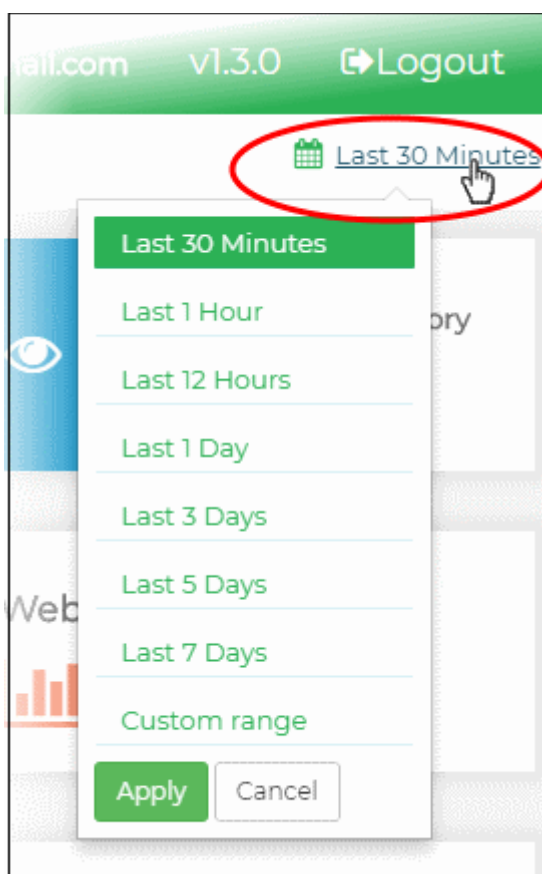
4 Device Overview

- The 'Device Overview' page shows the web browsing activities of a selected device.
- Statistics include websites visited, domains and attacks blocked, and more.
- This allows you to quickly identify harmful websites visited by users and effectively track the risks associated with the device.
- You can also configure device-specific protection settings and website blacklist/whitelists from this page. See [Manage Protection Settings for a Network/Device](#) for more guidance on this.

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**
- **Most visited website**
- **Most visited category**
- **Attacks blocked**
- **Websites blocked**

- **Live web surfing monitor**
- **Important events**
- **Most visited websites**
- **Most blocked categories**
- **Last visited websites**

Device Protection Status

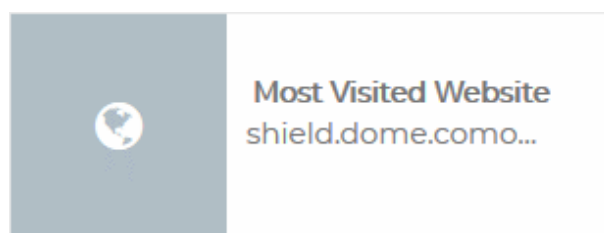
- The color of the protection summary tile indicates the device protection level:
 - Green - The device is connected and protected
 - Yellow - The device is not connected to cWatch Office and therefore not protected. The message at bottom left indicates when the device last connected.
- Click the cog icon in the top-right corner to view and manage protection settings on the device.
- Click the pencil icon to change device name. Please note, the device name will be updated in the cWatch console only. It doesn't actually change the name on the device itself.

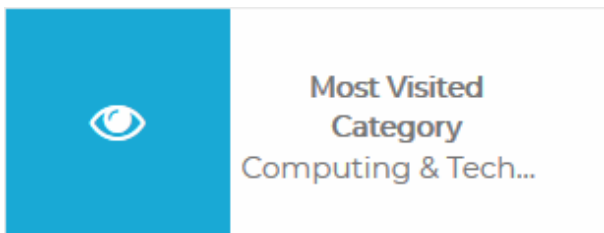


- Containment – (Windows devices only). If enabled:
 - Files with an 'unknown' trust-rating will be run in a secure virtual environment, isolated from the underlying file system and user data.
 - This prevents potentially malicious files from damaging the host computer. Unknown files which are harmless will operate without loss of functionality while in the container.
 - Only white-listed files that are known to be safe are allowed to run on the host.
- Click the gear icon  at top-right to view and change the protection settings applied to the device.
 - See **Manage Protection Settings for a Network/Device** for more details on these settings.

Most Visited Website

The website most often visited by the device.





Most Visited Category

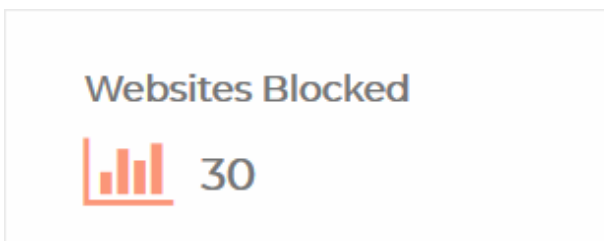
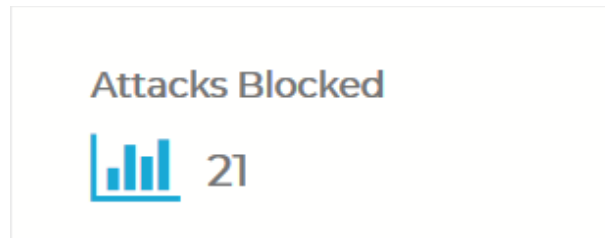
The website category visited most often by the device within the selected period. Blocked categories can be managed by clicking the cog icon -

Attacks Blocked

The total number of attacks blocked on the device within the selected period.

Tip: Click the cog icon to view the types of attacks that cWatch blocks.

See '**Attack Categories and Threats**' in **View Default Protection Settings** for more details.



Websites Blocked

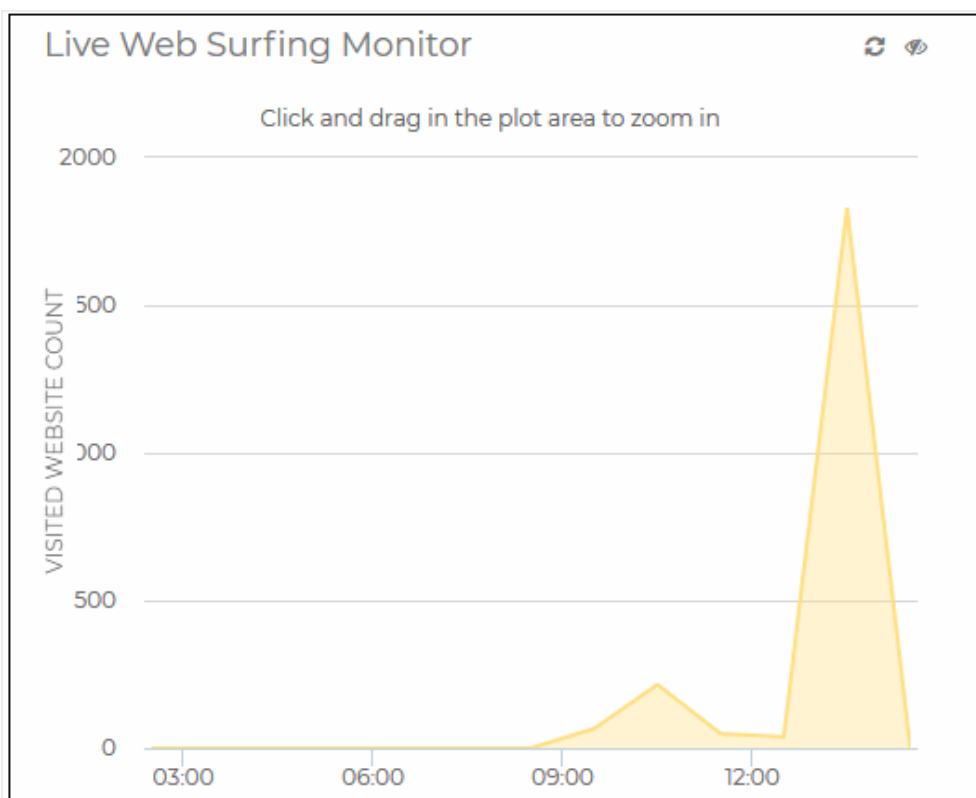
The total number of website access attempts that were intercepted and blocked on the device.

The number of sites blocked depends on the protection settings active on the device.

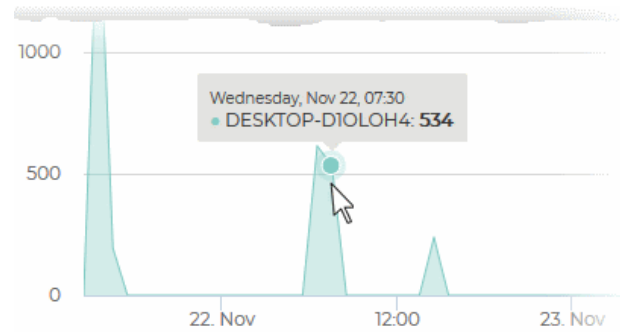
Click the cog icon to view the website categories that cWatch blocks.

Live Web Surfing Monitor

Shows the number of websites visited by the device during the selected time-period.



- Select a portion of the graph to zoom-in
- Place your mouse over a point in the chart to view the number of websites visited by the device at that time point.



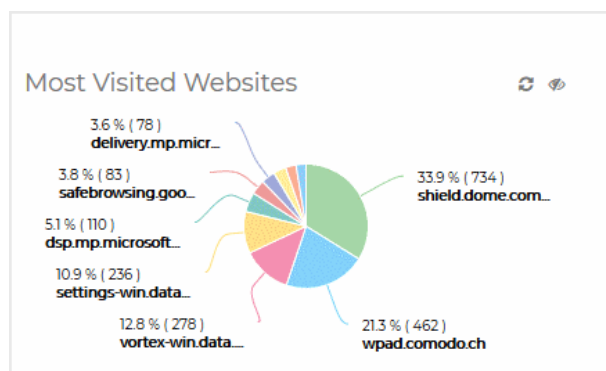
Important Events

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.

- Click to refresh the data

Tip:: The 'Default Protection Settings' page lets you view the types of attacks that cWatch blocks. See '**Attack Categories and Threats**' in **View Default Protection Settings** for more details.



Most Visited Websites

The ten websites visited most often by the device.



- Place your mouse on a sector to view the precise number of times the website was accessed.
- Click to refresh the data
- Click to view the legends used in the graph

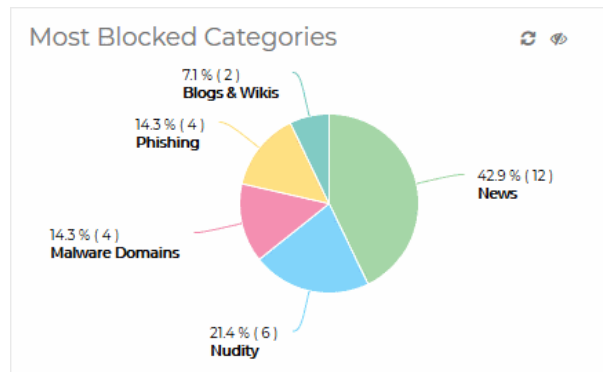
Most Blocked Categories

The ten website categories which were most often visited and blocked on the device.

The categories blocked depends on the protection settings active on the device.

See **Manage Protection Settings for a Network/Device** for more details on protection settings.

- Place your mouse on a sector to view the precise number websites blocked in that category.
- Click  to refresh the data
- Click  to view the legends used in the graph



#	Web Site Name	Last Seen
1	e10883.g.akamaiedge.net	an hour ago
2	e5077.g.akamaiedge.net	an hour ago
3	imgd.aeplcdn.com	an hour ago
4	sb.scorecardresearch.com	an hour ago
5	e1879.e7.akamaiedge.net	an hour ago
6	connect.facebook.net	an hour ago


Last Visited Websites

The 100 websites most recently visited by the device.

- Click  to refresh the list.

4.1 Manage Protection Settings on a Network/Device

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. You can use the default cWatch settings or you can apply custom settings to particular devices.

- Click on the device you wish to modify on the left
- You can enable / disable containment feature for a Windows device. If enabled, unknown files are isolated in a secure, virtual environment.
- Click the gear icon  in the corner of the the main, protection tile
- You can add/remove categories from a device or whitelist/blacklist specific websites
 - A whitelisted website is always allowed regardless of the category to which it belongs
 - A blacklisted website is always blocked regardless of the category to which it belongs
- Modify the protection settings as required

- Click 'Save' to apply your changes. You can also apply these settings to other devices.

Click the links below for more details:

- [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.
 - Click 'Open Valkyrie Portal' in the explanation to login to Valkyrie.


What is Containment ?

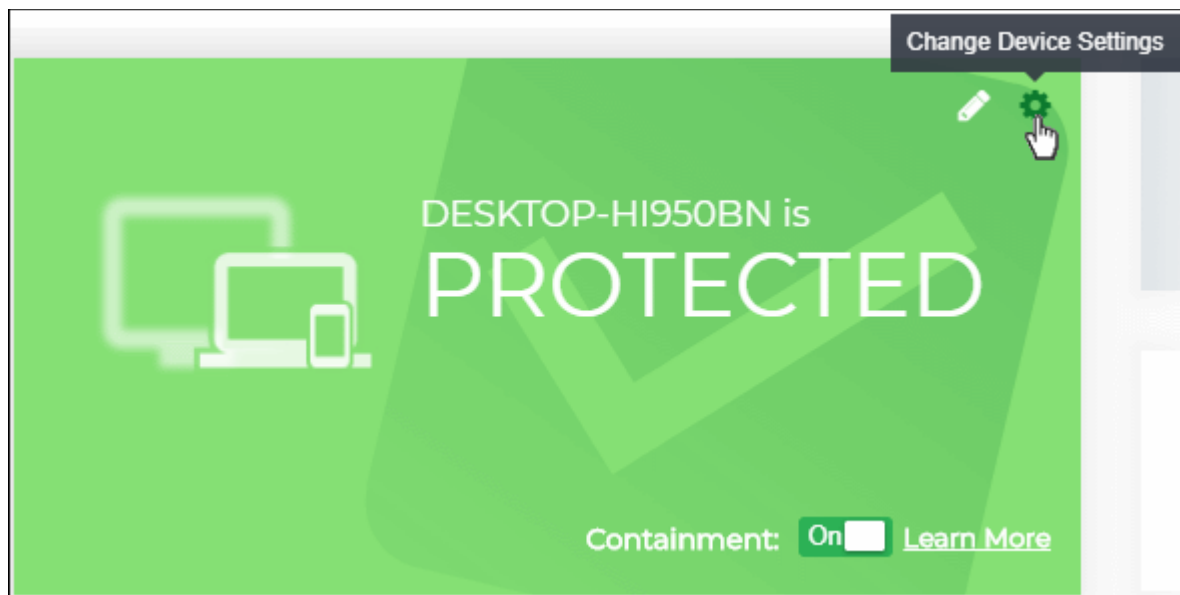
Containment service protects you against bad files and automatically contains unknown files in a virtual container using Default Deny Platform and containerization technology, which are provided by Comodo Cloud Antivirus installed on your device along with cWatch Office Agent. The unknown "contained" file is analyzed and an accelerated verdict is obtained through the Valkyrie cloud-based advanced malware analysis platform, delivering 100% protection against Zero-Day Malware.

[Open Valkyrie Portal.](#)

Close

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



Intimate Apparel &
Swimwear



Do you want to whitelist any websites?

example.com



Do you want to blacklist any websites?

example.com



Discard


Save

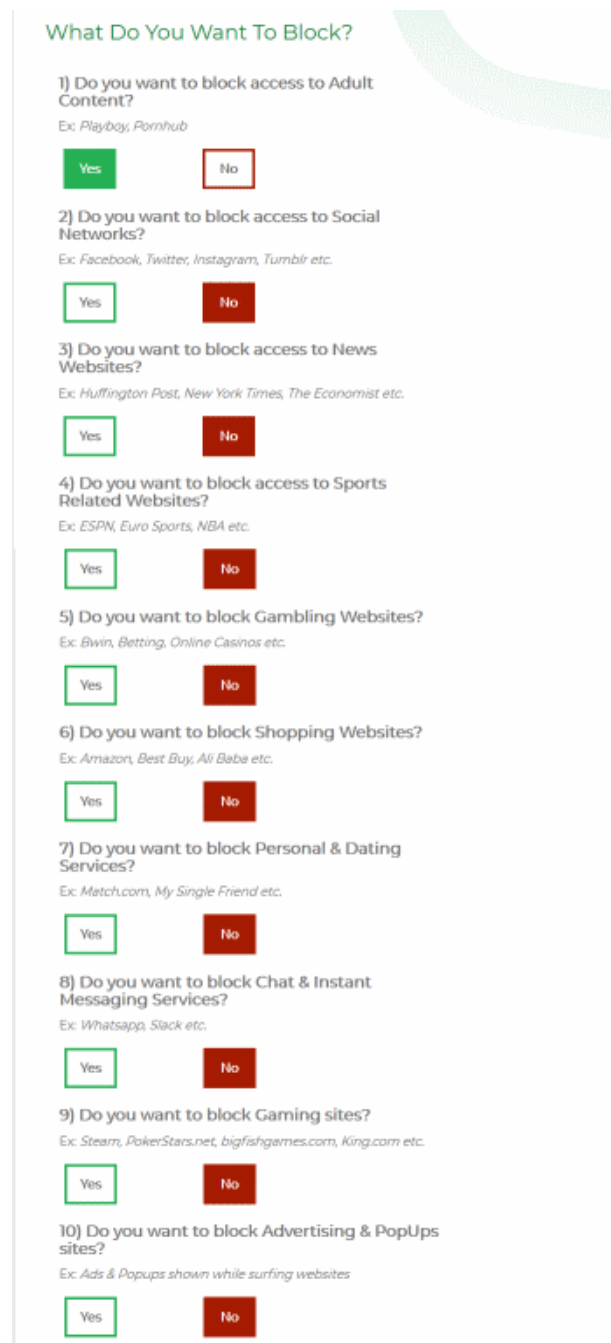
Apply to Other Dev

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

- Click the gear icon  at top-right of the protection status tile.
- 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' under 'What Do You Want To Block' but decide to white-list 'example-shop.com', then 'example-shop.com' will be allowed.
- You can add as many websites 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, hover 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

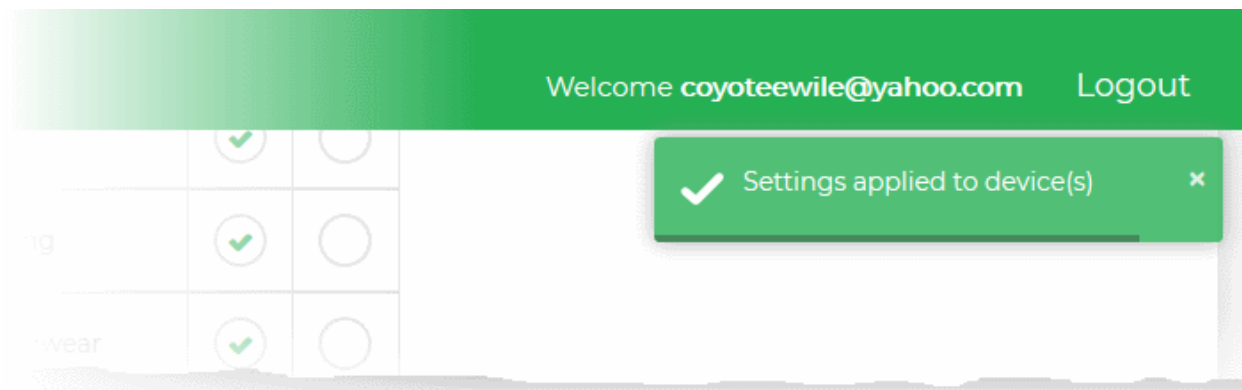
pokersample.com

Discard

Save

Apply to Other Devices

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

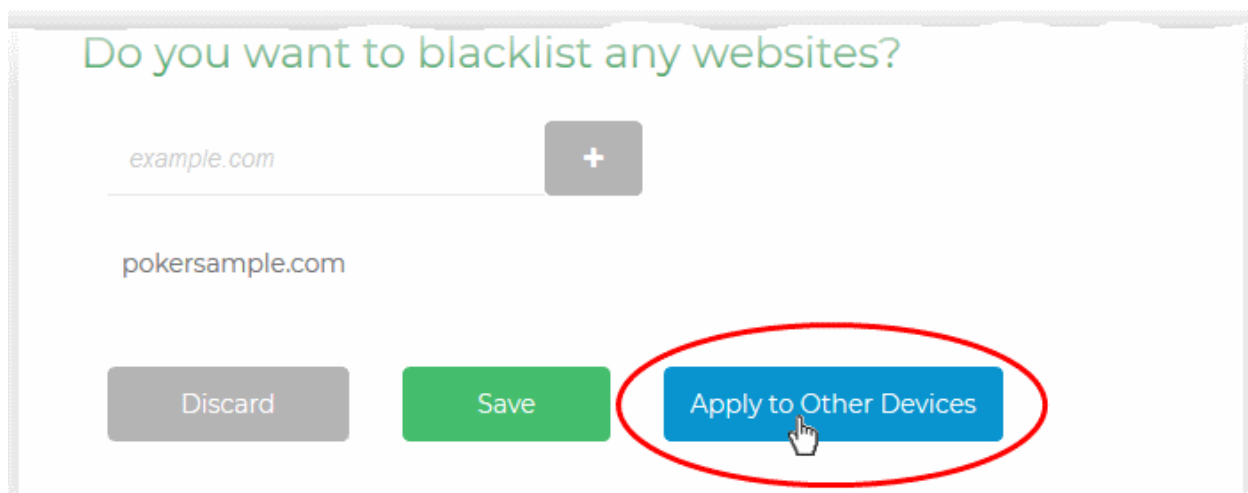


4.2 Manage Protection Settings for Several Devices

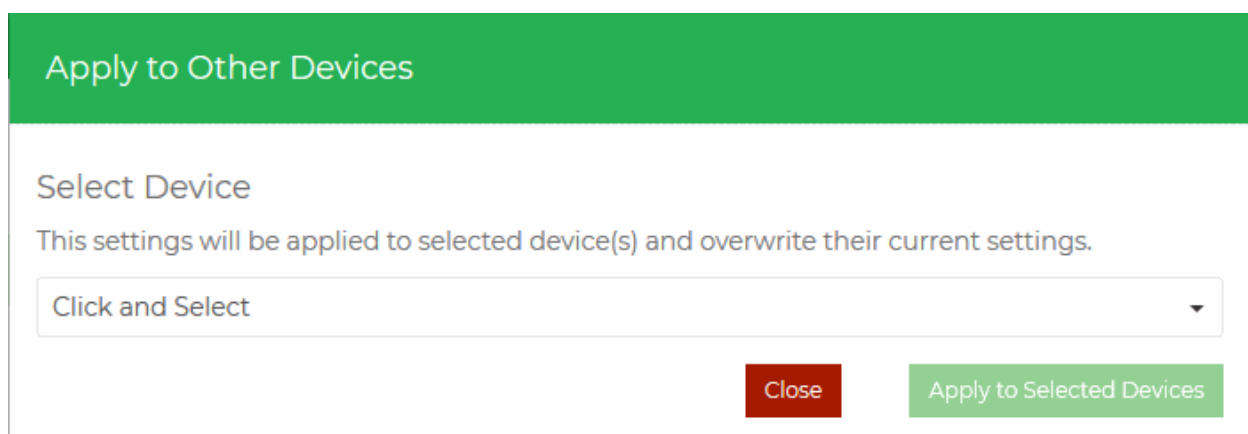
cWatch allows you to apply protection settings configured for one device to other devices. This is useful if you want to roll out the same protection settings to a group of devices.

To deploy the same protection settings to several devices:

- Click on a device on the left then click the gear icon at top-left.
- Configure the protection settings for the device as required. See [Manage Protection Settings for a Network/Device](#) for detailed guidance on this.
- After saving the settings, click 'Apply to Other Devices'.



The 'Apply to Other Devices' dialog will appear.



- Select the devices one-by-one from the drop-down

Apply to Other Devices

Select Device

This settings will be applied to selected device(s) and overwrite their current settings.

DESKTOP-D1OLOH4

Search... x

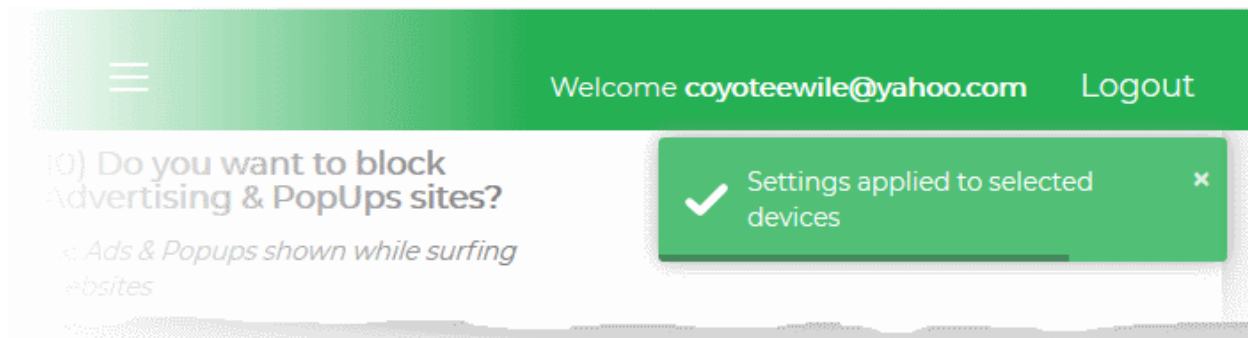
DESKTOP-D1OLOH4 ✓

SM-G600FY

Tip: You can use the search bar at the top to search for specific devices. Start typing the name of the device in the search box and select the device from the options.

- Click 'Apply to Selected Devices'

The settings will be applied to all selected devices at once.



- Please note that containment settings will not be applied. You have to configure this setting for each Windows device.

5 The cWatch Mobile Admin Console

The management console can be accessed by administrators from the cWatch mobile device app. This provides visibility and control over enrolled devices even when the administrator is on the move.

Notes:

- You must be an administrator to view the console from the mobile app.
- Admin rights are assigned by selecting 'Is Admin' when enrolling the device.
- To assign admin rights to an existing, non-admin device, you should first remove the device then re-enroll it. Remember to select 'Is Admin' when re-enrolling.

The console can be accessed as follows:

- Open the cWatch app on your smart device to view the mobile console

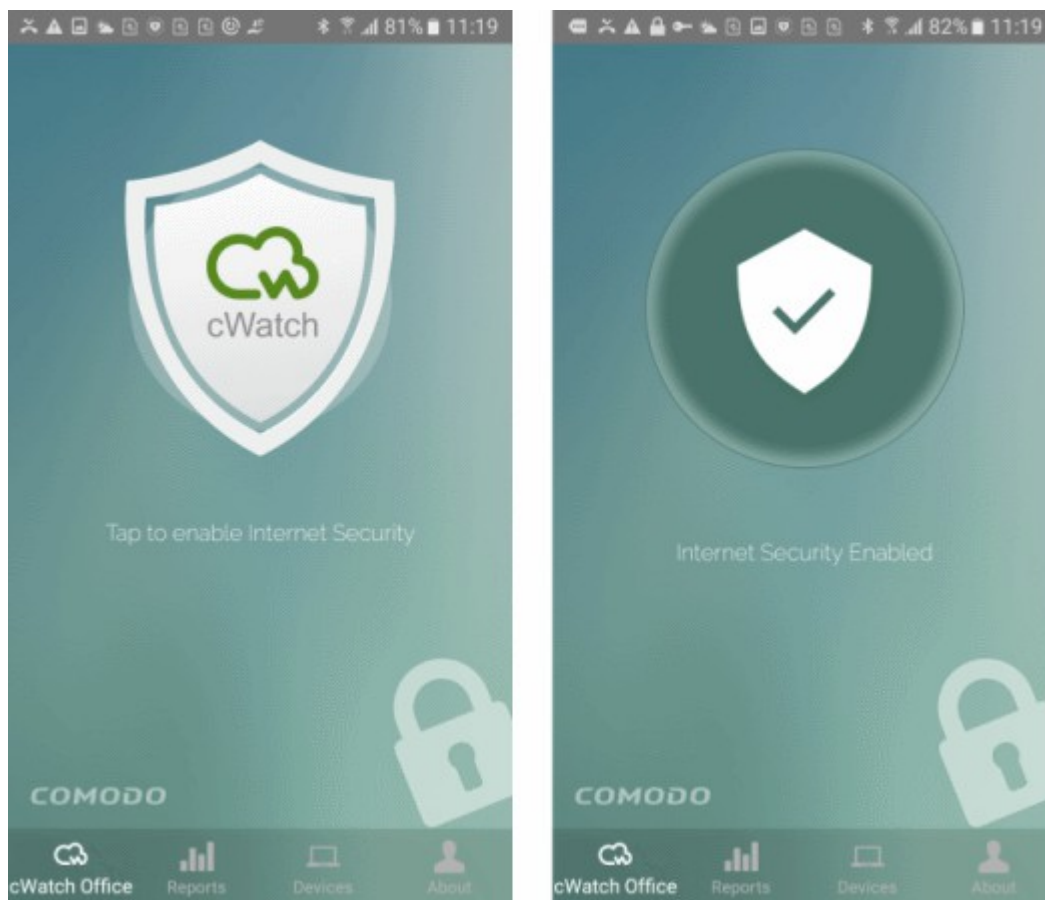


The options at the bottom of the screen let you to view different reports and screens:

- **cWatch Office** - Opens the cWatch app home screen. See [The Home Screen](#) for more details.
- **Reports** - View reports on browsing trends, attacks, websites blocked and more .See [View cWatch Office Reports](#) for more details.
- **Device** - View the protection status of enrolled devices in your network. See [View Device Summaries](#) for more details.
- **About** - View details about the cWatch app. Also contains a link to login to the cWatch Web Console. See [About](#) for more details.

5.1 The Home Screen

The home screen displays the connection status of the device:



- Tap the cWatch Office shield logo to connect to the console.

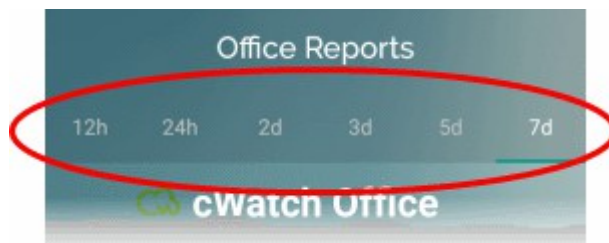
5.2 View cWatch Office Reports

- Tap the 'Reports' icon on the launch bar to open this section

The 'Reports' screen shows overall and device specific charts on browsing trends, attacks blocked, websites visited, websites blocked and more:



- The options at the top allows you to choose the time period of the statistics:



- The 'Device Name' drop-down lets you choose the device/network whose statistics you want to see:



- Choose 'All Devices' to view overall statistics for all devices in your network
- Select a device name if you want to view stats for a specific device

The total websites blocked, total websites visited and total attacks blocked will be displayed at the top of the page for the selected item:

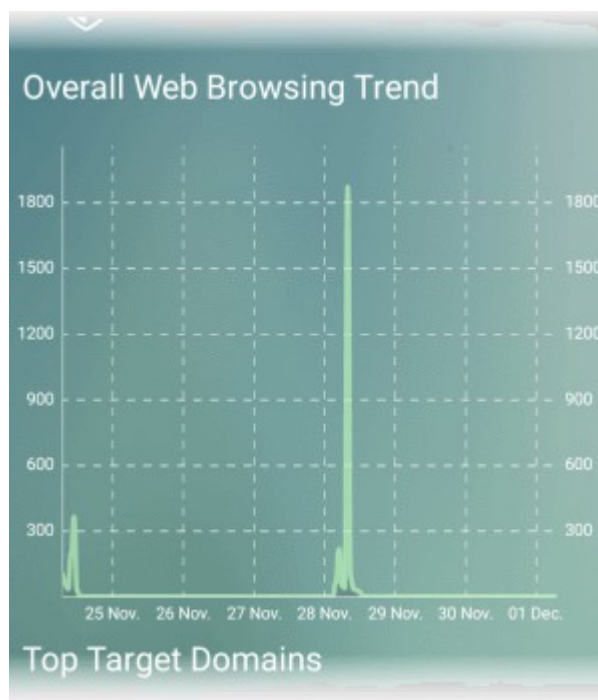


The following charts are displayed for the chosen device.

- **Overall Web Browsing Trend**
- **Top Target Domains**
- **Top Blocked Domains**
- **Overall Advanced Threats**
- **Top URL Categories**

Overall Web Browsing Trend

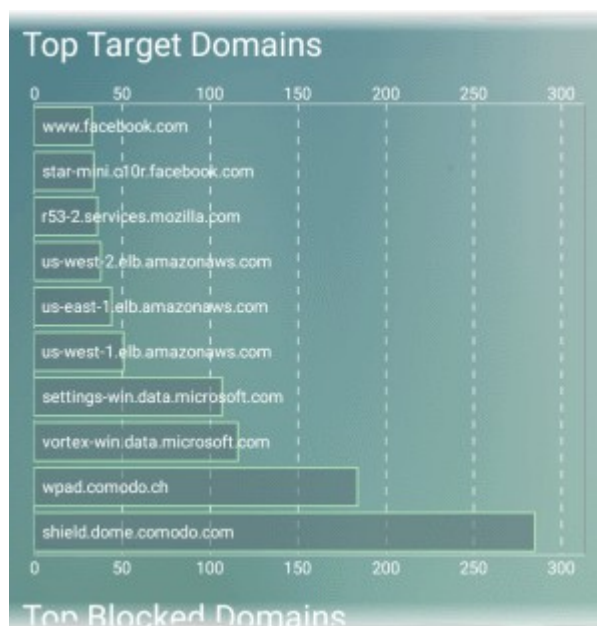
- The chart shows the number of websites visited by the device during the selected time-period.
- The X-axis shows the time period and the Y-axis shows the number of websites visited
- An example is shown below:



Top Target Domains

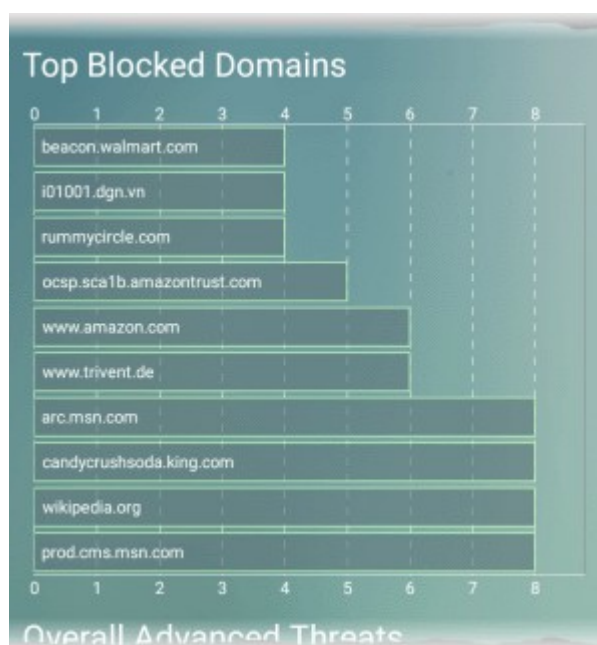
- Shows the ten websites visited most often by the device within the selected period.
- The number of visits to each website is shown in the X-axis.

- An example is shown below:



Top Blocked Domains

- Shows the top-ten websites blocked on the device within the selected period.
- The number of access attempts to each website is shown in the X-axis.
- An example is shown below:

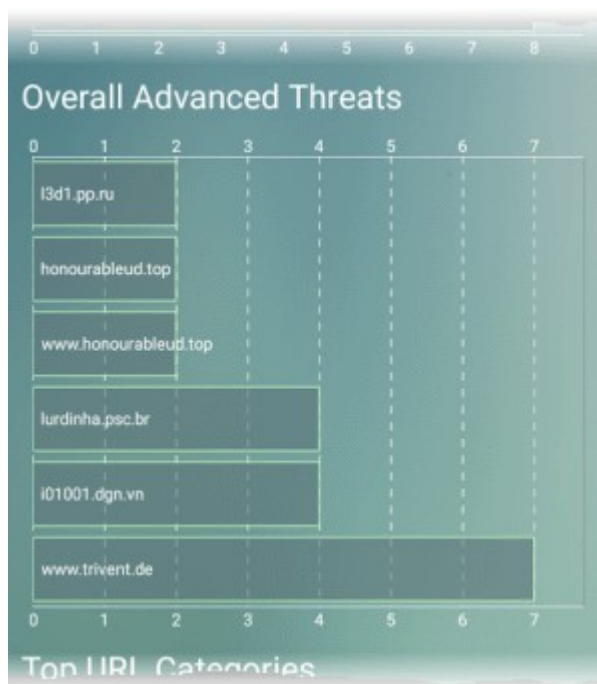


Overall Advanced Threats

- Shows the top-ten types of attacks blocked on the device within the selected period.
- The number of times each attack was blocked is shown in the X-axis.

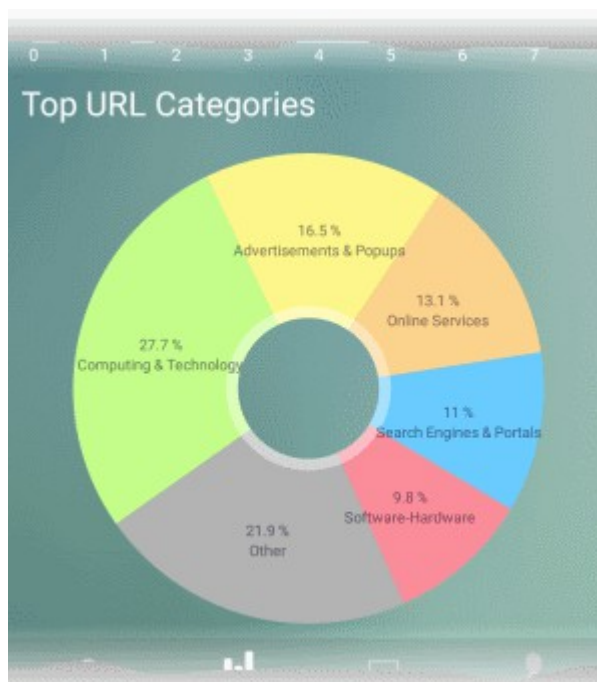
Tip: You can view the types of attacks that cWatch blocks in the 'Default Protection Settings' page of the web console. See '**Attack Categories and Threats**' in **View Default Protection Settings** for more details.

- An example is shown below:



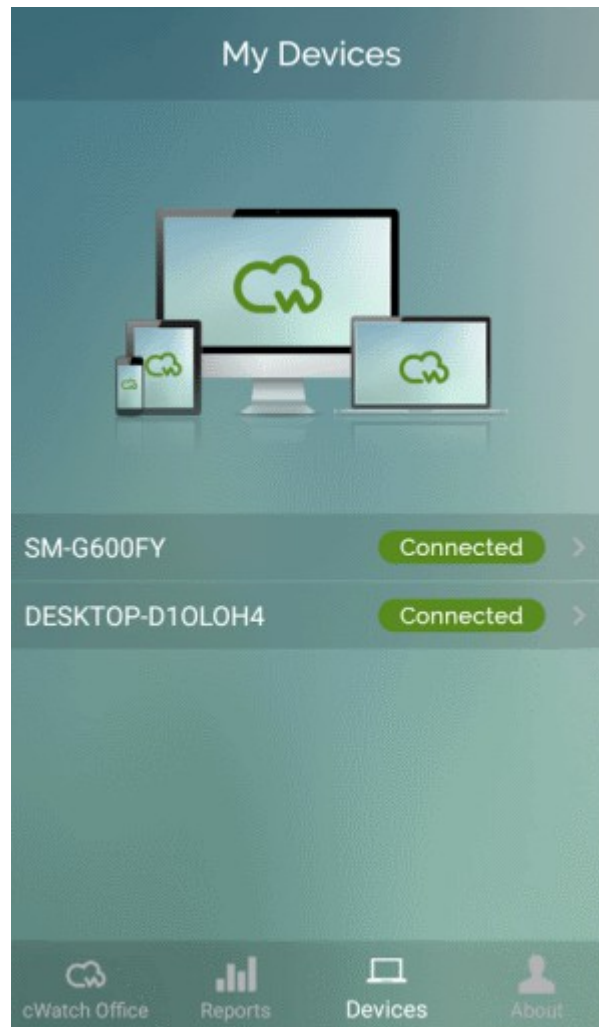
Top URL Categories

- Shows the ten website categories which were most often visited on the device.
- An example is shown below:

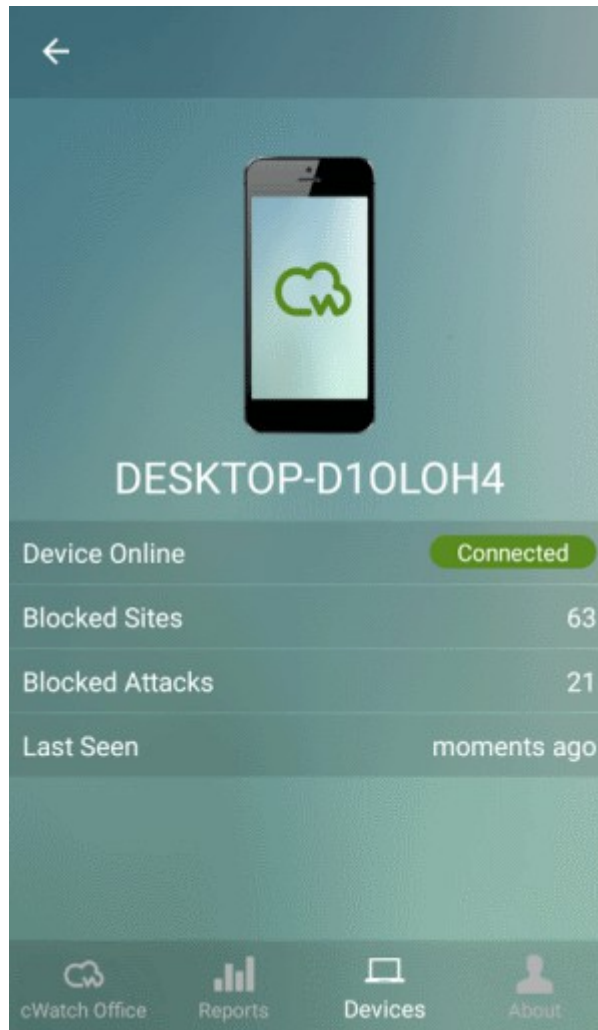


5.3 View Device Summaries

The 'My Devices' page shows a list of enrolled networks and devices.

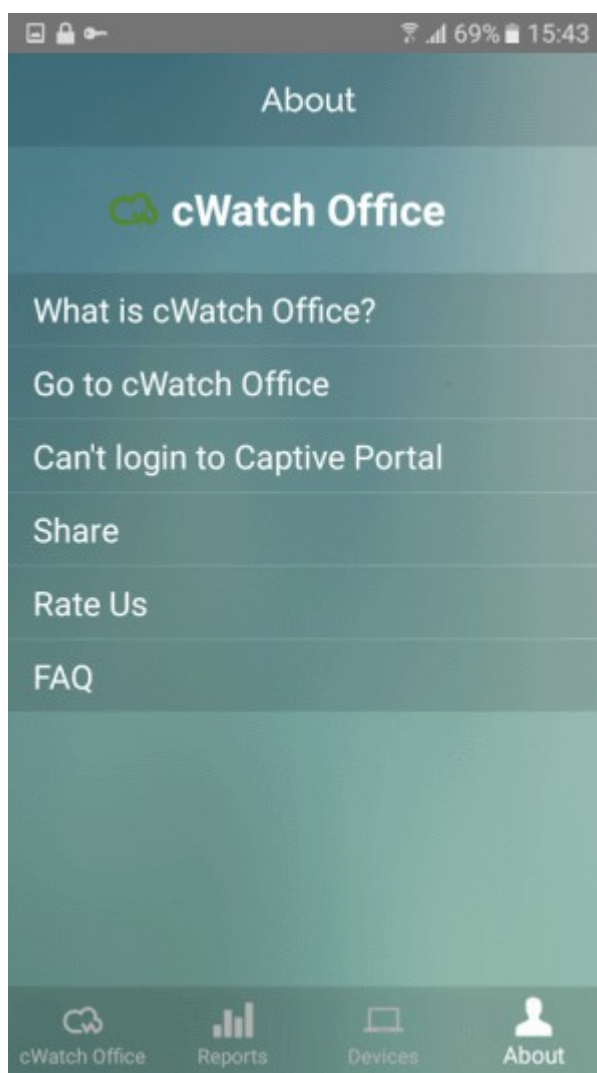


- Tap a device name to view its status summary:



5.4 About

The 'About' page contains links to support information and a link to login to the Office web console.



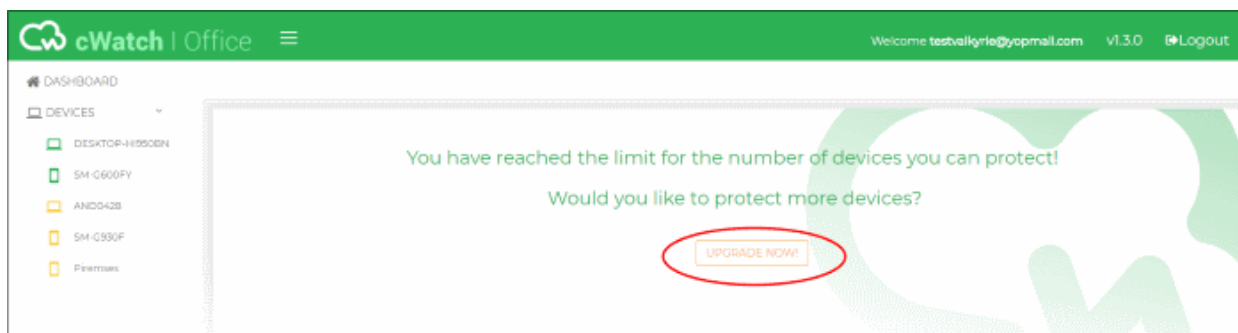
- **What is cWatch Office** - cWatch Office information page.
- **Go to cWatch Office** - Opens the cWatch Office web console login page.
- **Can't login to Captive Portal** - Opens a help page with advice if your device can't connect to the cWatch Office server.
- **Share** - Allows you to share the cWatch Office app with other users.
- **Rate Us** - Opens the Google Play or Apple App store where you can rate and provide feedback on the app. Your feedback is much appreciated for the continual improvement of the service.
- **FAQ** - Opens the cWatch Office frequently asked questions page.

6 Upgrade Your License

You should upgrade your license if you wish to protect more devices than covered by your existing license.

There are two ways to upgrade your license:

- You can purchase additional licenses using the order form at <https://secure.comodo.net/home/purchase.php?pid=210>.
- cWatch displays an 'Upgrade Now' message if you attempt to add more devices than allowed by your license:



- Click the 'Upgrade Now' button.

You will be taken to the cWatch license purchase page.

- Complete the purchase process. Make sure you choose 'Existing Customer' under 'Enter Customer Details' and enter your Comodo Account username and password. See [Purchase a License](#) if you need help with this.
- The new license will be automatically added to your account once your order has been processed.
- Login in cWatch and enroll your new devices as required. See [Add Networks and Devices](#) if you need help with this.

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