



# **DNSWatch**

## **Deployment Guide**

---

---

## About This Guide

---

The *DNSWatchGO Deployment Guide* is a guide to help you set up the DNSWatchGO subscription service. Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc. Guide revised: 7/23/2019

## Copyright, Trademark, and Patent Information

---

Copyright © 1998 - 2019 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at <https://www.watchguard.com/wgrd-help/documentation/overview>.

---

## About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit [WatchGuard.com](http://WatchGuard.com).

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at [www.secplicity.org](http://www.secplicity.org).

## Address

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

## Support

[www.watchguard.com/support](http://www.watchguard.com/support)  
U.S. and Canada +877.232.3531  
All Other Countries +1.206.521.3575

## Sales

U.S. and Canada +1.800.734.9905  
All Other Countries +1.206.613.0895

# Contents

---

<b>DNSWatch Protects Your Assets On and Off Premise</b> .....	<b>1</b>
Components.....	1
DNSWatchGO Client.....	4
DNSWatchGO Client Process.....	4
Protect Your Networks with DNSWatch.....	5
<b>About DNSWatch Block Pages</b> .....	<b>5</b>
Customize DNSWatch Block Pages.....	8
Customize the Security Block Pages.....	8
Customize the Content Block Page.....	9
<b>Download and Install DNSWatchGO Client</b> .....	<b>10</b>
Download and Install on Each Device.....	10
Activate a DNSWatchGO Beta License.....	11
Extend Your DNSWatchGO Beta License.....	12
View Protected Devices.....	13
Content Filter Policies.....	14
Create a New Policy.....	15
Edit a Policy.....	16
Apply a Policy to a Network.....	17
Delete a Policy.....	17
Stop or Start DNSWatchGO.....	19
Stop or Start from Windows Services.....	19
Stop or Start from a Command Prompt.....	19
<b>Protect Your On-Premise Networks</b> .....	<b>21</b>
Add a New Network.....	21
<b>Test DNSWatchGo Client</b> .....	<b>24</b>
How to Test.....	24

Browse Normally.....	25
Verify DNSWatchGO Blocks Malicious or Filtered Content Domains.....	25
<b>View DNSWatch Content Filtering Reports.....</b>	<b>26</b>
View Filtered Requests.....	28
<b>Troubleshoot DNSWatchGO.....</b>	<b>29</b>
View Log Messages.....	29
View Log Messages Dynamically.....	30
<b>About DNSWatch Content Filter Categories.....</b>	<b>31</b>
Content Filter Categories.....	31
Abortion.....	31
Adult Material.....	31
Advocacy Groups.....	32
Bandwidth.....	32
Business and Economy.....	32
Collaboration - Office.....	32
Drugs.....	32
Education.....	33
Entertainment.....	33
Extended Protection.....	33
Gambling.....	33
Games.....	34
Government.....	34
Health.....	34
Illegal or Questionable.....	34
Information Technology.....	34
Internet Communication.....	35
Intolerance.....	35
Job Search.....	35

Militancy and Extremist .....	35
Miscellaneous.....	35
News and Media.....	35
Parked Domain.....	35
Productivity.....	35
Religion.....	36
Security.....	36
Shopping.....	37
Social Organizations.....	37
Social Web - Facebook.....	37
Social Web - LinkedIn.....	37
Social Web - Twitter.....	38
Social Web - YouTube.....	38
Society and Lifestyles.....	38
Special Events.....	38
Sports.....	38
Tasteless.....	39
Travel.....	39
Vehicles.....	39
Violence.....	39
Weapons.....	39

# DNSWatch Protects Your Assets On and Off Premise

---

DNSWatch protects your assets from malicious domains and provides the ability to filter the content your users can see. When a user tries to visit a malicious or filtered web domain, a *Block* page appears in the browser instead of the requested content.

DNSWatch offers two types of protection:

- **On-Premise Network Protection** – DNS protection and content filtering on your network (with or without a Firebox).
- **Off-Network Protection** – DNS protection and content filtering on portable assets with the DNSWatchGO client regardless of connection type, protocol, or port.

For example, a member of the sales team has a laptop with the DNSWatchGO Client installed. The salesperson is on the road most of the time and connects through a variety of networks. The DNSWatchGO off-network content filtering policy allows the social media, streaming media, and alcohol categories. If the salesperson tries to go to any filtered sites while not on the DNSWatch protected network, a standard content block page appears. If the salesperson accidentally clicks on a malicious link, a standard security block page appears.

At a branch office with a DNSWatch protected network, the on-network content filtering policy has the streaming media and alcohol categories blocked. When the salesman is in the office, he attempts to download movies for his next flight and receives the on-network customized content block page.

## Components

The DNSWatch subscription service has these components:

### *Account API Tokens*

Account API tokens connect your DNSWatchGO Clients with your DNSWatchGO account. These tokens are automatically created when you purchase a DNSWatchGO license. You need only one token for each account.



If you have merged accounts, you might see more than one API token listed. You can select any of the API tokens to use when you install DNSWatchGO.

### *DNSWatch*

A cloud-based service that monitors DNS requests to prevent connections to known malicious or filtered domains. The DNSWatch service can be enabled on a Firebox or configured on your network.

### *DNSWatch Dashboard*

Log in to your DNSWatch account on the WatchGuard Portal to get access to the DNSWatch Dashboard. From the dashboard you can manage your protected devices, configure network protection, change account settings, and monitor alerts that are generated when DNSWatch denies requests.

The dashboard is also the place to add domains to the blacklist or whitelist. You also have the option to submit domains you add to your blacklist to the DNSWatch Support team. The team analyzes submitted domains for inclusion in the Threat Intelligence Domain Feed for everyone.

### *DNSWatchGO Client*

A client-based application installed on host computers, such as laptops, to enforce your policy when a device is not connected to your network. The client submits DNS requests to both the DNSWatch server and the upstream DNS server.

- If the domain is considered malicious or suspicious, DNSWatchGO returns the Block page from the DNSWatch server
- If no issues are found by the DNSWatch server, DNWatchGO returns the requested content from the upstream DNS server

### *Content Filter Policy*

Sometimes you want to filter content that users can access both on and off your network. With DNSWatch, you can create a content filter policy to block domains in specific content categories, such as gambling, alcohol, or adult content. When a user tries to go to a web site in a filtered category, DNSWatch replaces the requested content with the Block page. You can have one policy for off-network and different policies for each on-premise network. For more information about how to filter content, see [Content Filter Policies](#).

### *Block Page*

When DNSWatch determines that a requested domain is malicious or filtered, users see the Block page instead of the requested content. DNSWatch also attempts to gather more information about the source of the blocked DNS request and the type of threat. The collected information appears in an alert for administrators that DNSWatch generates when it denies a DNS request.

Instead of blocking malicious information, DNSWatch also educates users about the hazards of clicking unknown links and how people can be tricked into disclosing information. The DNSWatch Block page provides a link to a short exercise to help educate the user about how to avoid phishing attacks. There are two Block pages:

- Customized Block page – The Block page can be customized for on-premise users. Users on a device with the DNSWatchGO Client installed who are on a protected network will also see the customized Block page. For more information about how to customize the Block page, see [Customize DNSWatch Block Pages](#).
- Standard Block page – The standard Block page appears when a device with the DNSWatchGO Client is not a protected network and tries to access a malicious domain.

### *Threat Intelligence*

To protect your network, DNSWatch uses a complex set of heuristics to identify requests to malicious domains or domains with suspicious certificates. DNSWatch polls a variety of commercial threat intelligence feeds daily to identify new malicious domains and update the *Domain Feeds*. To help improve DNSWatch for all users, you can share the domains you manually add to the block list with WatchGuard. You can see a list of the threat intelligence feeds in the [DNSWatch Dashboard](#).



## DNSWatchGO Client

DNSWatchGO Client is an application that you install on portable computers that leave your network, such as employee laptops. The client simultaneously forwards DNS requests to both DNSWatch servers and the upstream DNS resolvers. DNSWatch servers compare the requested domain to the lists of malicious domains in the Domain Feed and to domains in filtered categories.

If the requested domain is not on the known malicious domains list or on the filtered domains list, the requested content appears.

If the domain is a known threat or filtered content:

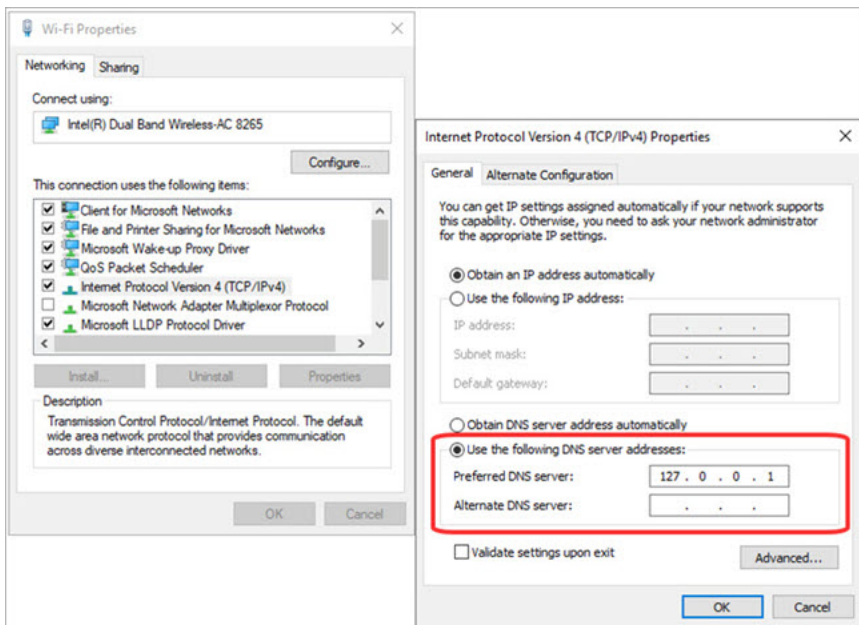
- DNSWatchGO Client returns the Block page content
- If the requested content links to a malicious domain, DNSWatchGO gathers more information about the threat

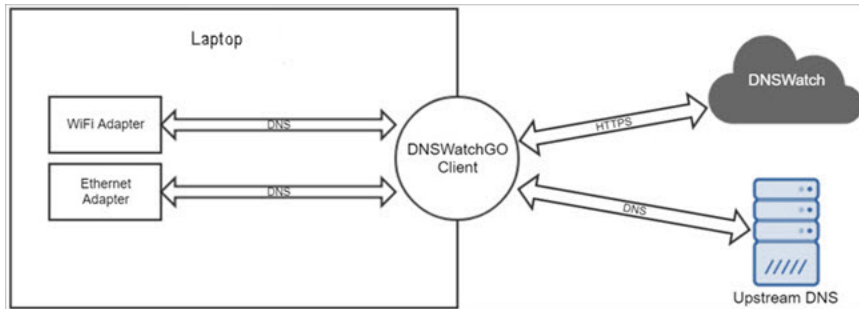


When a computer is connected to your network, your network policies and protections take priority over DNSWatchGO settings.

## DNSWatchGO Client Process

As part of the DNSWatchGO installation, all Internet Protocol (IP) enabled adapters on the host have their DNS servers configured to localhost. The original configured DNS settings are saved in the DNSWatchGO Client as the upstream DNS servers.





The DNSWatchGO Client listens on localhost port 53 (both TCP and UDP) and intercepts DNS requests. When a DNSWatchGO Client receives a DNS request:

- A query is sent to DNSWatch to determine if the domain is blocked
- A request for the IP address for the domain is sent to the upstream DNS servers based on the original DNS server configuration on the host (dynamic or manually configured DNS servers)

After DNSWatch sends the response:

- If the response is Block or Filter, the DNSWatchGO Client returns the Block page
- If the response is Allow or Whitelist, the DNSWatchGO Client returns the requested content provided by the upstream DNS server

## Protect Your Networks with DNSWatch

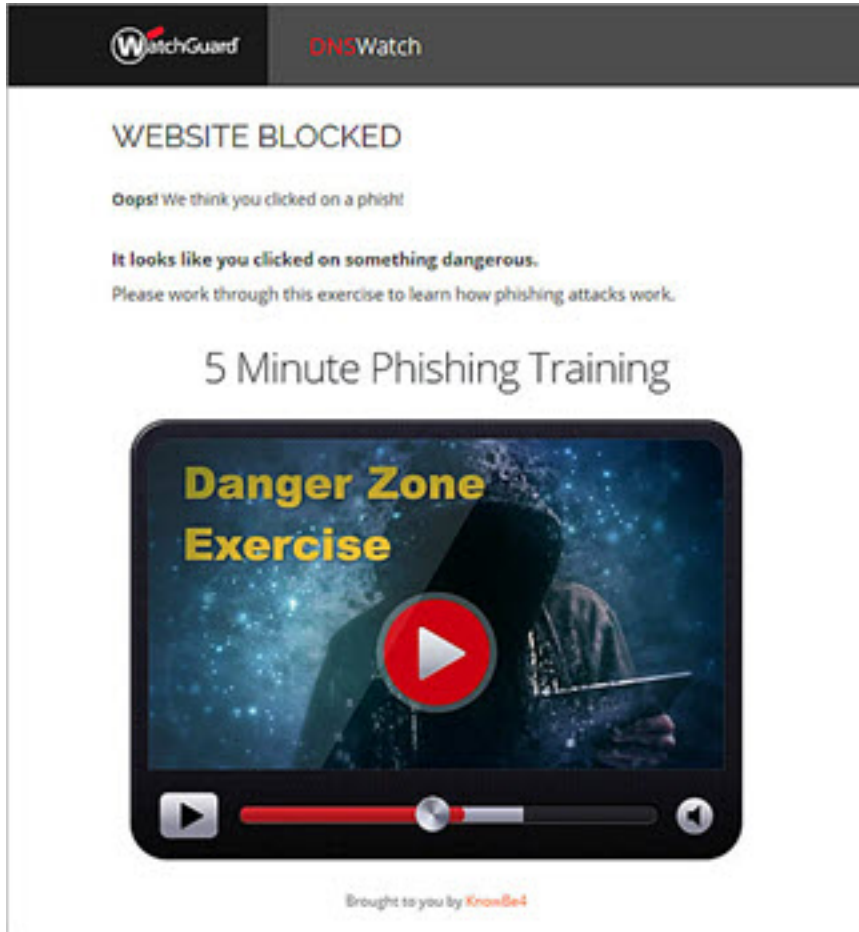
Configure DNSWatch as your DNS resolver to protect your network from malicious sites and phishing attempts. You can also filter access based on content such as alcohol, gambling, and online dating. When your network appliance or firewall receives a DNS query on a protected network, it uses DNSWatch as the DNS resolver. If the request is to a domain on the Domain Feeds list or Filtered Content list, then DNSWatch returns a Block page instead of the requested content. If the domain is not on the lists, DNSWatch returns the requested content to the user.

## About DNSWatch Block Pages

When DNSWatch denies the connection to a website at a suspicious domain, a block page appears in the browser. There are two block page types:

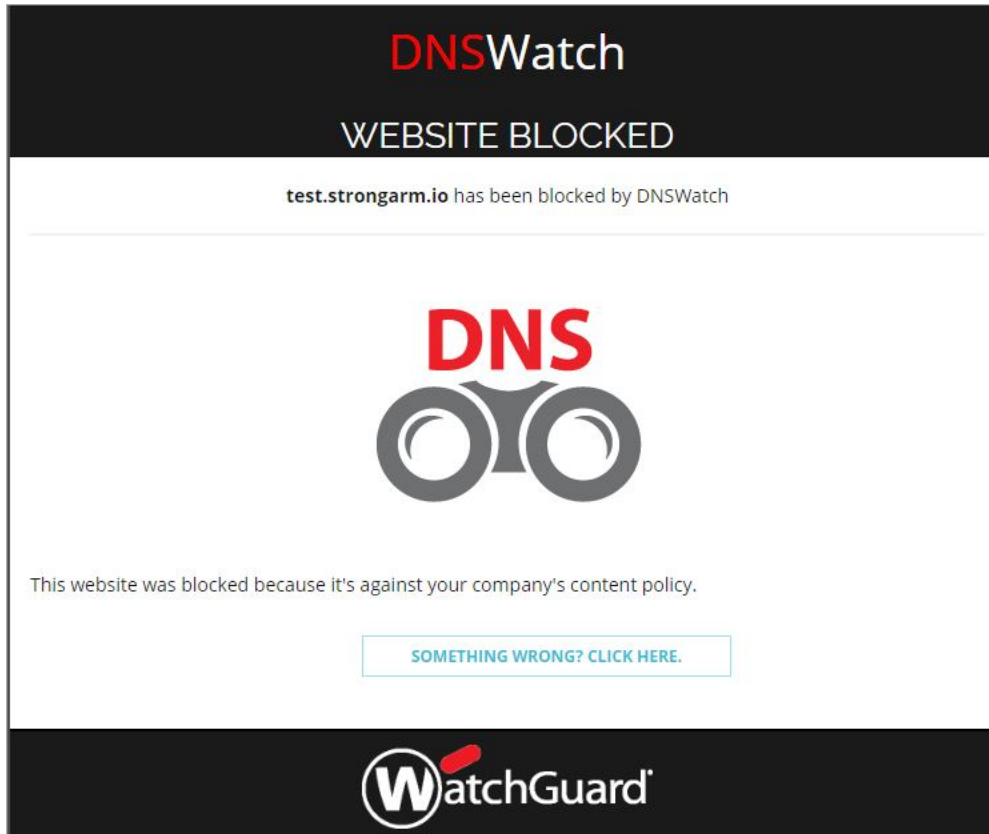
### Security Block Page

The security block page appears when a user tries to get access to a malicious domain. The block page informs the user that the website was blocked and provides a short training exercise to help educate the user about how to avoid phishing attacks.



### Content Block Page

The content block page appears when a user tries to get access to a domain that is not considered malicious but is filtered based on policy.



You can add custom messages to block pages that appear when the user tries to get access to malicious or filtered content on site. When a user is off site, the standard Block page appears.

### Block Page Overview

DNSWatchGOClient Installed	Location	Blocked Domain	Block Page Type	Where to Configure
Yes	On Site	Malicious	Security	Block Page Content
		Filtered content	Content	Content Filtering > Block Page tab
No	On Site	Malicious	Security	Block Page Content
		Filtered content	Content	Content Filtering > Block Page tab
Yes	Off Site	Malicious	Security	Not configurable
		Filtered content	Content	Not configurable

## Customize DNSWatch Block Pages

Customize your block pages to provide information that explains to users why content is blocked. This information should include contact information so that users can contact you if they believe they have been incorrectly blocked from a site.

### Customize the Security Block Pages

The customized security block page only appears when a user attempts to access a malicious domain while on site. The block page can be customized with your corporate message, colors, and logo.

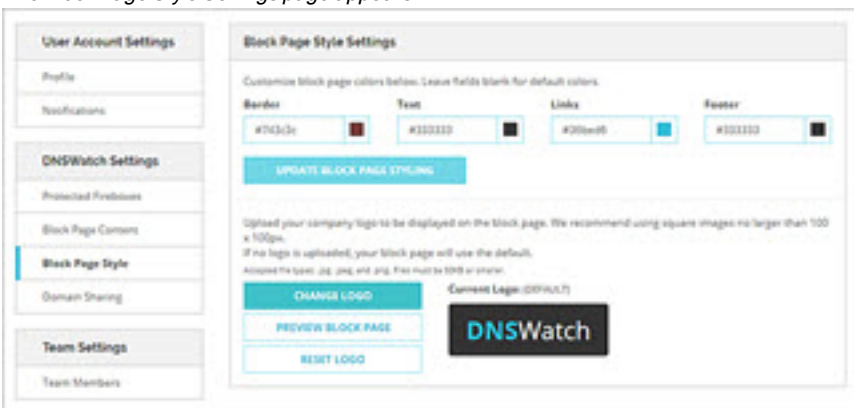
You can add a custom logo to replace the default logo that appears at the top of the page. We recommend that you select a square image that is no larger than 100 x 100 pixels. Select a .JPG, .JPEG, or .PNG file with a maximum size of 100 x 100 pixels. The maximum file size for the logo is 50 KB.

To customize the message on the security block page content for malicious domains:

1. [Log in](#) to your DNSWatch account.
2. Select your user name and select **Settings**.
3. From the navigation menu, select **Block Page Content**.  
*The Block Page Content Settings page appears.*
4. Select the **Content** tab.
5. Edit the content in the window in Markdown format. Click **Styling with Markdown is supported** to see tips on how to use Markdown.
6. To preview the content as it will appear on the block page, select the **Preview** tab.

To customize the security block page style:

1. [Log in](#) to your DNSWatch account.
2. Select your user name and select **Settings**.
3. From the navigation menu, click **Block Page Style**.  
*The Block Page Style Settings page appears.*



4. To customize the colors of a page element.

- To specify a color, type the hexadecimal value of the color in the text box.
  - To select a new color from a color palette, click the current color.
5. To change the logo, click **Change Logo**, browse to select the image, then click **Open**. To reset the logo to the DNSWatch logo, click **Reset Logo**.
- To preview the block page, click **Preview Block Page**.

## Customize the Content Block Page

The Content block page appears when a user attempts to get access to content that is filtered. You can customize the message text with Markdown.

To customize the text that appears on the Content block page:

1. [Log in](#) to your DNSWatch account.
2. Select your user name and select **Settings**.
3. From the navigation menu, click **Content Filtering**.  
*The Content Filtering page appears.*
4. Select the **Block Page** tab.
5. Select the **Content** tab.
6. Edit the content in the window in Markdown format. Click **Styling with Markdown is supported** to see tips on how to use Markdown.
7. To specify an email address for feedback, type the email address in the **Send user feedback to this email address (optional)** text box.
8. Click **Update Block Page**.

To reset the text back to the default:

1. At the bottom of the **Content** tab, click **Reset**.  
*The Reset Block Page confirmation dialog box appears.*
2. To confirm that you want to reset the content, click **Reset**.

## Download and Install DNSWatchGO Client

---

For each device you want to protect, follow the download and install instructions for the DNSWatchGO Client.


DNSWatchGO Client is supported on these operating systems:

- Windows 7
- Windows 8 and 8.1
- Windows 10

### Download and Install on Each Device

1. Log in to the [DNSWatch Dashboard](#).
2. Select your user name and select **Settings**.



3. From the navigation menu, select **DNSWatchGO Client**.
4. Click **Download DNSWatchGO Installer** or **Download Unified Installer**.
5. If prompted, save the installer package to an appropriate location.
6. In the **Account API token for DNSWatchGO Client** section, click  to copy the token to your clipboard.  
*If you have more than one token, it does not matter which token you copy.*
7. Navigate to the saved location and double-click the **DNSWatchGO\_Client** or **DNSWatchGO\_TDR** executable to begin the installation.
8. If you ran the unified **DNSWatchGO\_TDR** installer, select the **DNSWatchGO** check box. Click **Install**.  
*The DNSWatchGO Client Setup wizard opens.*
9. In the **DNSWatchGO Client Setup** wizard:
  - a. Click **Next**.  
*The Client Configuration screen appears.*
  - b. Use **Ctrl+V** to paste the account API token in the text box.
  - c. Click **Next**.  
*The Ready to Install DNSWatchGO Client screen appears.*
  - d. Click **Install** to begin the installation.
  - e. When setup is complete, click **Finish** to close the setup wizard.

The computer is now protected by DNSWatchGO. It can take up to 30 minutes for the device to appear in the DNSWatchGO Client Devices list. If you stop the client, DNSWatchGO automatically restarts when you restart the computer.

## Activate a DNSWatchGO Beta License

To participate in the Beta, request a beta license from the [WatchGuard DNSWatchGO Beta Site](#), activate the license on the WatchGuard Portal, and install the DNSWatchGO client on any Windows 7 or newer device you want to protect.



It is not necessary to have a Firebox or use DNSWatch in order to use DNSWatchGO. It can be used as a standalone product to protect your users both on and off the network, regardless of other WatchGuard products you may use.

Follow these steps to participate in the beta release for DNSWatchGO:

1. Log the [WatchGuard DNSWatchGO Beta Site](#).
2. In the left menu, click **Beta Licenses**. The Beta Licenses page appears with your Beta License Key.
3. Copy the Beta License Key.
4. In the [Activate Products](#) page on the WatchGuard Portal, paste the license key in the text box.

### Enter Serial Number or License Key

- To activate a new device, type the serial number exactly as it appears (include any hyphens). You can find the serial number on a label on your device or on the fulfillment email for your virtual device.
- To activate an add-on license, service, or renewal, type the license key from your fulfillment email or online store receipt.

**CONTINUE** ▶

5. In the **Activate a Product** dialog box, verify the information is correct and accept the end-user license agreement.

**Activate a Product**

Activating: DNSWatchGO Beta 25 users for Lisa DNSWatchGO

**Review the End-User License Agreement**

I accept the **End-User License Agreement**.

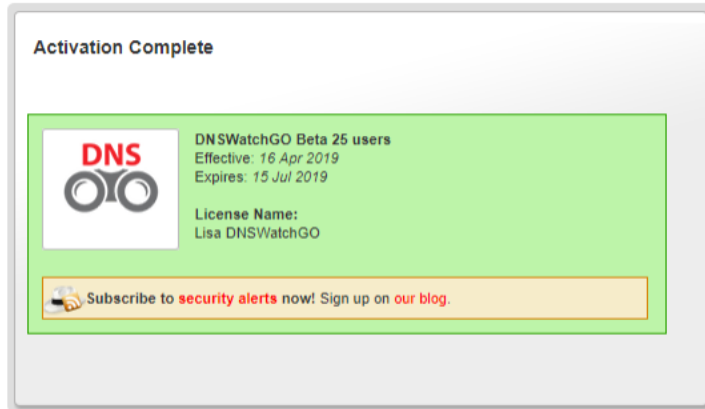
« Previous
Next »



6. Click **Next** to activate your license.

The *Activation Complete* page appears.

#### Activate a Product



You now have an active DNSWatchGO beta license.

To connect to the cloud-based DNSWatch Dashboard, click **DNSWatch Dashboard**.



Your DNSWatch credentials are the same credentials you use to log in to the WatchGuard Support Center.

For information on how to download and install the DNSWatchGO Client, see [Download and Install DNSWatchGO Client](#).

## Extend Your DNSWatchGO Beta License

To extend your DNSWatchGO Beta License, request a new Beta License on the [WatchGuard DNSWatchGO Beta Site](#), and activate the license on the WatchGuard Portal.

To extend your beta license:

1. Log the [WatchGuard DNSWatchGO Beta Site](#).
2. In the left menu, click **Beta License Extension**. The Beta License Extension page appears with your Beta License key. The license key appears at the bottom of the page.
3. Copy your new Beta License Key.

- In the [Activate Products](#) page on the WatchGuard Portal, paste the license key in the text box.

**Enter Serial Number or License Key**

- To activate a new device, type the serial number exactly as it appears (include any hyphens). You can find the serial number on a label on your device or on the fulfillment email for your virtual device.
- To activate an add-on license, service, or renewal, type the license key from your fulfillment email or online store receipt.

[CONTINUE >](#)

- In the **Activate a Product** dialog box, verify the information is correct and accept the end-user license agreement.
- Click **Next** to activate your license.  
*The Activation Complete page appears.*

You now have an extension for your DNSWatchGO beta license.

## View Protected Devices

View the status of devices with DNSWatchGO installed on the DNSWatchGO Client Devices page.

DNSWatchGO synchronizes with hosts approximately every 30 minutes. It can take up to 30 minutes for a new host to appear on the list.

Information included on this page:

- **Domain** – The Active Directory domain configured on the device.
- **User Name** – The name of the primary user of the device, often in domain\username format
- **Hostname** – The name of the device or laptop
- **Version** – The DNSWatchGO version currently installed
- **Registered** – The period of time the host has been registered with DNSWatchGO
- **Last Sync** – The last time DNSWatchGO synced the client
- **OS** – The operating system installed on the computer
- **Addresses** – The addresses associated with the computer
- **On Site** – A red X indicates the device is not connected to a protected network on the same DNSWatch account. A green check mark indicates the device is connected to a protected network on the same DNSWatch account.
- **Protected** – A green check mark indicates the device is protected by DNSWatchGO and a red X indicates protection is paused or disabled

To see DNSWatchGO client devices:

- Log in to the [DNSWatch Dashboard](#).
- Select **Reports > DNSWatchGO**.  
*The DNSWatchGO Client Devices page appears.*

DNSWatchGO Client Devices 3

USER NAME	HOSTNAME	VERSION	REGISTERED	LAST SYNC	OS	ADDRESSES	ON SITE	PROTECTED
WGTV	LAP-	0.10.1	1 week, 5 days ago	2 hours ago	Windows 10	Seattle, WA, US	✗	✓
WGTV	LAP-	0.10.1	2 months, 3 weeks ago	4 days, 11 hours ago	Windows 10	Seattle, WA, US	✗	✓
LAP-	LAP-	0.9.3	3 months, 3 weeks ago	2 months, 3 weeks ago	Windows 10	Seattle, WA, US	✗	✓

**FILTER** ▾

Username

Hostname

Version

OS Name

On Site

Protected

**APPLY FILTERS**

**CLEAR FILTERS**

3. To show the filter options, click **Filter**.
4. Make your selections then click **Apply Filter**.  
*The table populates with requests that meet the selected criteria.*

## Content Filter Policies



By default, content filtering is not turned on. If you want to filter content available to users, you must create a new policy. If you delete a policy used by a network or DNSWatchGO client, content filtering is turned off.

In addition to DNSWatch protection from malicious clickjacking and phishing domains based on intelligence feeds, you can use policies to block domains in selected content categories. You can create a multiple policies to meet the various needs of your networks. Each protected network can have a different policy. However, only one policy can be applied to devices using DNSWatchGO.

For example, you have two branch offices with separate protected networks and all of the laptops have the DNSWatchGO client installed. You can create a different policy for each branch office network or assign the same policy to all networks. Select one policy, or create a separate policy, for DNSWatchGO client enforcement off-network.

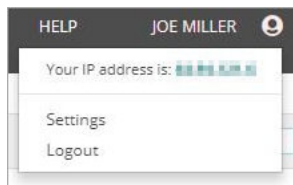
- DNSWatchGO client policy – This policy is used by DNWatchGO client when not connected to a DNSWatch protected network. You may want to allow domains categorized as Social Media and Streaming Media for users who are traveling and off network while blocking those domains for users who are on-premise. Only one policy can be designated as the DNSWatchGO client policy.
- Protected network policy – This policy is assigned to a protected network to filter content requests to the specified domain types. If Marketing and Sales are on a separate network, you may want to allow them to access Social Media and Streaming Media while restricting those categories for other users on a different network.

The available categories have both top-level and subcategories. Categories that can be fine-tuned with subcategories are indicated by an arrow. Click the arrow to select subcategories. Top-level categories are more than a summation of the subcategories they contain. Top-level categories include websites that fit the description of the category, but do not fit the description of any subcategory. For a complete list of available categories and descriptions, see [About DNSWatch Content Filter Categories](#).

## Create a New Policy

By default, content filtering is not turned on. If you want to filter content available to users, you must create a new policy. You can create multiple DNSWatch policies to use with your protected networks. Policies can be created based on functionality or location. For example, on the network used by marketing and sales, you can allow social media domains while excluding them on all other networks.

1. Select your user name and select **Settings**.



2. From the navigation menu, select **Content Filtering**.

*The Content Filtering Policies page appears.*

3. In the **Policies** tab, click **Create New Policy**.

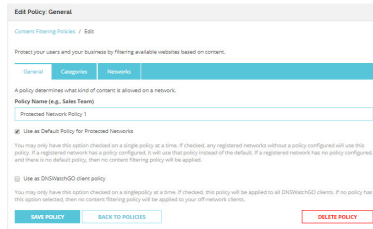
*The Create Policy page appears.*

 A screenshot of the 'Create Policy' form. The title is 'Create Policy'. Below it, there's a breadcrumb 'Content Filtering Policies / Add'. A note says 'A policy determines what kind of content is allowed on a network.' There's a 'Policy Name (e.g., Sales Team)' field with the value 'DNSWatchGO client policy'. Below that are two checkboxes: 'Use as Default Policy for Protected Networks' and 'Use as DNSWatchGO client policy'. There are 'SAVE POLICY' and 'CANCEL' buttons at the bottom.

4. In the **Policy Name** field, type a descriptive name for the policy.
5. To enable the policy as the default policy for protected networks, select the **Use as Default Policy for Protected Networks** check box.
6. To enable the policy as the DNWatchGO client policy, select the **Use as DNSWatchGO client policy** check box. You can only have one DNSWatchGO client policy at a time.

7. Click **Save Policy**.

*The Edit Policy: General page appears.*



8. Select the **Categories** tab.

*The Edit Policy: Categories page appears.*

9. Select the check boxes for the categories you want to filter. When you select the top-level category, the subcategories are automatically selected. Expand the top-level categories by clicking the arrow to the right of the category name to select subcategories.
10. To save your changes, click **Save Categories**.

## Edit a Policy

You can edit policies as your needs change.

To edit a policy:

1. Select your user name and select **Settings**.

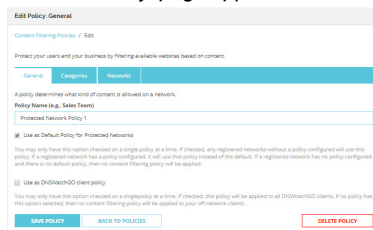


2. From the navigation menu, select **Content Filtering**.

*The Content Filtering Policies page appears.*

3. In the **Policies** tab, click **Edit Policy** policy for the policy you want to edit.

*The Edit Policy: page appears.*



4. Select the **Categories** tab.

*The Edit Policy: Categories page appears.*

5. Select the check boxes for the categories you want to filter. When you select the top-level category, the subcategories are automatically selected. Expand the top-level categories by clicking the arrow to the right of the category name to select subcategories.

- To save your changes, click **Save Categories**.
- Click **Back to Policies**.

## Apply a Policy to a Network

It is easy to apply a policy to a network from the policy page. This allows you to apply a single policy to multiple networks at one time. You can also choose the policy when you first configure the network.

To apply a policy to a network:

- Select your user name and select **Settings**.

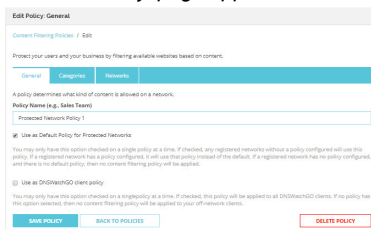


- From the navigation menu, select **Content Filtering**.

*The Content Filtering Policies page appears.*

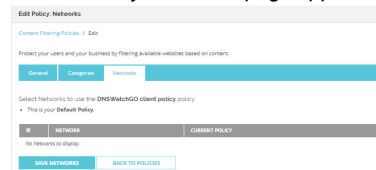
- In the **Policies** tab, click **Edit Policy** policy for the policy you want to edit.

*The Edit Policy: page appears.*



- To choose which networks use the policy, select the **Networks** tab.

*The Edit Policy: Networks page appears.*



- Select the check boxes for the appropriate networks.
- Click **Save Networks**.
- Click **Back to Policies**.

## Delete a Policy

If you do not use a policy, you can delete it.



If you delete a default policy, you need to apply another policy to the DNSWatchGO client or to the protected network if you want to continue content filtering.

1. Select your user name and select **Settings**.

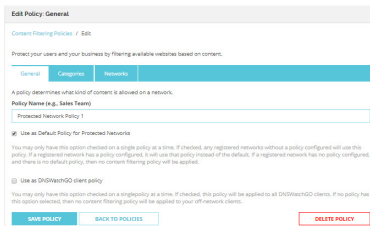


2. From the navigation menu, select **Content Filtering**.

*The Content Filtering Policies page appears.*

3. In the **Policies** tab, click **Edit Policy** policy for the policy you want to edit.

*The Edit Policy: page appears.*



4. Click **Delete Policy**.

*The Delete Policy confirmation page appears.*



5. Click **Delete Policy**.

## Stop or Start DNSWatchGO

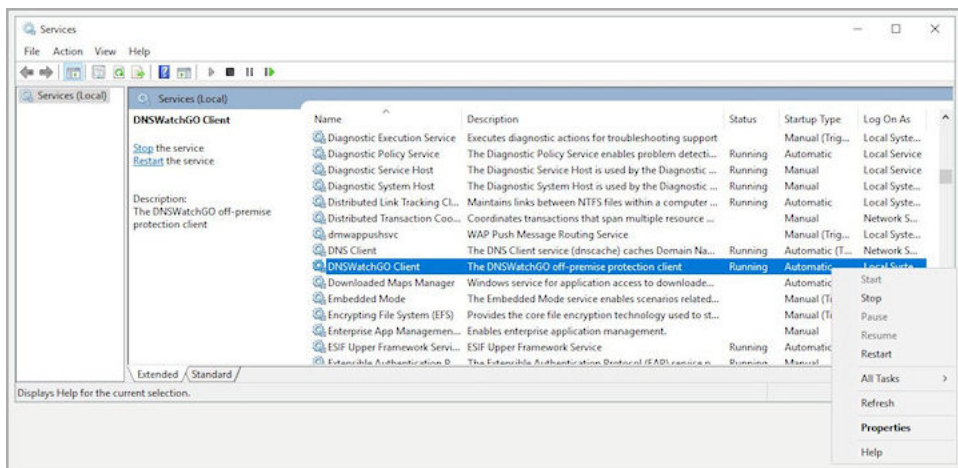
If you run into any issues, you can manually stop and start the DNSWatchGO Client on the device from the Windows Services control panel utility or Command Prompt.



The DNSWatchGO Client is configured to automatically start when the device starts. If you stop the client, it will automatically restart when the device is restarted.

## Stop or Start from Windows Services

From Windows Services, search the **Services (Local)** list for DNSWatchGO Client.



To start or stop the client, right-click **DNSWatchGO Client** and select **Stop** or **Start**.

## Stop or Start from a Command Prompt



You must run Command Prompt as an administrator.

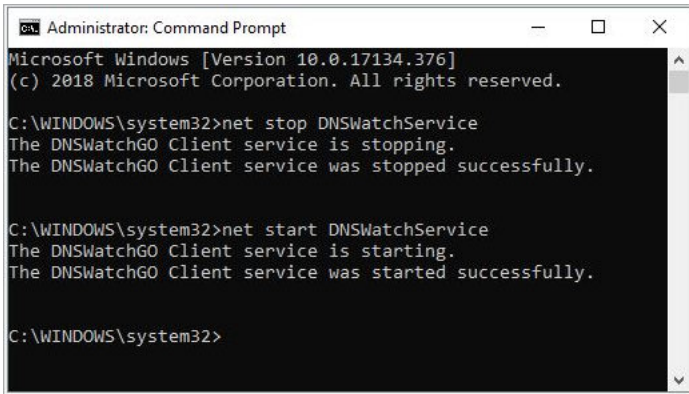
To stop DNSWatchGO, type the stop command:

```
net stop DNSWatchService
```



To start DNSWatchGO, type the start command:

```
net start DNSWatchService
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.376]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net stop DNSWatchService
The DNSWatchGO Client service is stopping.
The DNSWatchGO Client service was stopped successfully.

C:\WINDOWS\system32>net start DNSWatchService
The DNSWatchGO Client service is starting.
The DNSWatchGO Client service was started successfully.

C:\WINDOWS\system32>
```

# Protect Your On-Premise Networks

You can protect your on-premise networks by blocking malicious sites and filtering requests sites based on content even if you don't have Firebox. All you need to do is to configure your network to use DNSWatch as your DNS server. Your DNS traffic will be evaluated and any requests to known malicious or filtered domains are denied.

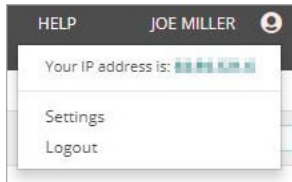


This is intended to be used with static on-premise networks as part of your overall network protection plan, not as a temporary, portable solution at multiple locations. That is what DNSWatchGO client will do for you.

If you plan to protect multiple networks with different content filter policies, it is easier to create the policies before you add the network. See [Content Filter Policies](#) for information about policies.

## Add a New Network

1. Log in to the [DNSWatch Dashboard](#).
2. Select your user name and select **Settings**.



3. From the left menu, select **Protected Networks**.

*The Protected Networks page appears.*

ADDRESS	DESCRIPTION	PROTECTED	POLICY	ACTIONS
You don't have any protected networks. To protect a network, login from that network or <a href="#">contact support</a> for assistance.				

4. Click **Add Network**.

The *Add New Network* page appears.

The screenshot shows a web form titled "Add New Network". At the top, there is a breadcrumb trail: "Protected Networks / Add". Below this is a light blue informational box that says "Your current IP address has been automatically populated below." The form contains several fields: "IP Address" with a text box containing a blurred IP address; "Description (e.g. 'Boston Office')" with a text box containing the placeholder "Add a description"; and "Policy" with a drop-down menu currently showing "--Default Policy--". At the bottom of the form, there are two unchecked checkboxes: "Enable Custom Block Page" and "Enable Dynamic DNS". A prominent blue button labeled "SAVE NETWORK" is located at the bottom left of the form area.

5. Your current IP address appears in the **IP Address** text box automatically. If you want to protect a different network, type the IP address of the network in the text box.
6. Type a descriptive name for the network in the **Description** text box.
7. From the **Policy** drop-down list, select a content filter policy to apply to the network. For information about policies, see [Content Filter Policies](#).
8. To create a custom page for this network, select the **Enable Custom Block Page** check box. If you do not customize the page, the network uses the default DNSWatch Block page.
  - a. Type the Markdown content in the **Content** text box.
  - b. To preview the Block page, click the **Preview** tab.

### Add New Network

[Protected Networks](#) / [Add](#)

Your current IP address has been automatically populated below.

**IP Address**

**Description (e.g. "Boston Office")**

**Policy**

--Default Policy--

Enable Custom Block Page

**Custom block page specific to this address**

Content
Preview
Styling with Markdown is supported ⓘ

Add a message...

Enable Dynamic DNS

SAVE NETWORK

9. If your network uses dynamic DNS, select the **Enable Dynamic DNS** check box.
10. Click **Save Network**.  
*The Protected Networks page appears.*
11. Your network is not protected until you configure your network appliance to use the DNSWatch resolvers. Follow the instructions for your appliance to change the DNS resolvers to the addresses on the Protect Networks page.

### Protected Networks Need help configuring networks?

DNSWatch makes it easy to protect and manage many networks. You can also view [past changes to your Protected Networks](#).

For help with adding a large number of networks, please [contact support](#).

Primary DNS Resolver

Second DNS Resolver

ADDRESS	DESCRIPTION	PROTECTED	POLICY	ACTIONS
<input type="text" value="192.168.1.100"/>	Seattle Office	<b>x</b> ⓘ	Default Policy	<a href="#">EDIT</a>

ADD NETWORK

Your network is now registered with DNSWatchGO.

**Protected Networks** Need help configuring networks?

DNSWatch makes it easy to protect and manage many networks. You can also view [past changes to your Protected Networks](#).

For help with adding a large number of networks, please [contact support](#).

ADDRESS	DESCRIPTION	PROTECTED	POLICY	ACTIONS
[Redacted]	Seattle Office	✓	Default Policy	<a href="#">EDIT</a>

[ADD NETWORK](#)

## Test DNSWatchGo Client

DNSWatchGO protects your devices when they are off your protected network. After you test the application in several scenarios, report the results on the WatchGuard beta management platform.

To gather the best data for the test, we ask that you repeat the test scenarios on DNSWatchGO Client devices in a variety of locations. Some suggested locations:

- Home
- Active Directory controlled network
- Coffee shops
- Mobile hotspot
- On a network behind a firewall while connected with VPN
- Airport – Include the airport and the name of the service used
- Airplane – Include the airline and name of the service used
- Hotels – Include the hotel chain name



It is important to test the client on networks that are not protected by your Firebox and DNSWatch configuration.

## How to Test

There are two tests to confirm the DNSWatchGO Client functions correctly:

- Verify you can browse to non-malicious or regular domains without issues
- Verify DNSWatchGO blocks malicious or filtered content domains

## Browse Normally

Browse the Internet and verify common domains operate correctly.

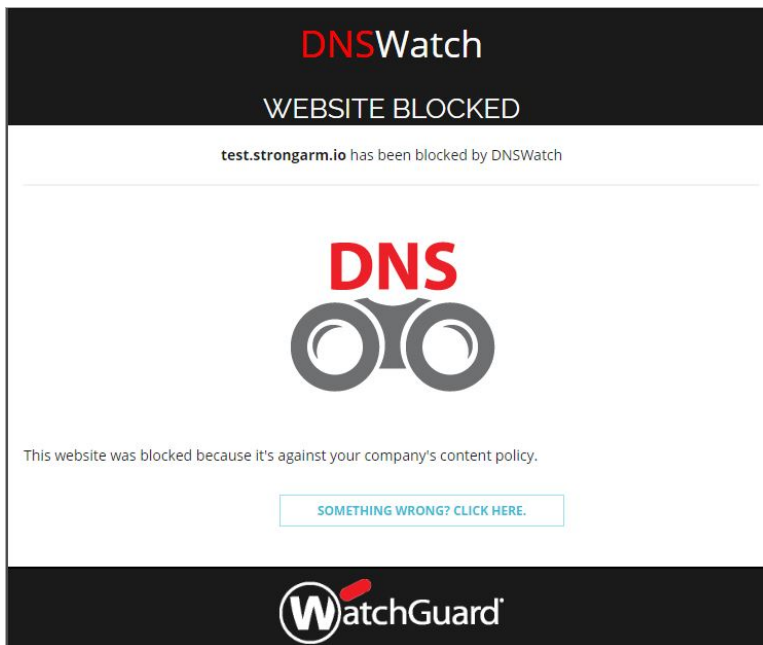
For example, browse to <https://www.watchguard.com/>. Confirm the page loads correctly.

## Verify DNSWatchGO Blocks Malicious or Filtered Content Domains

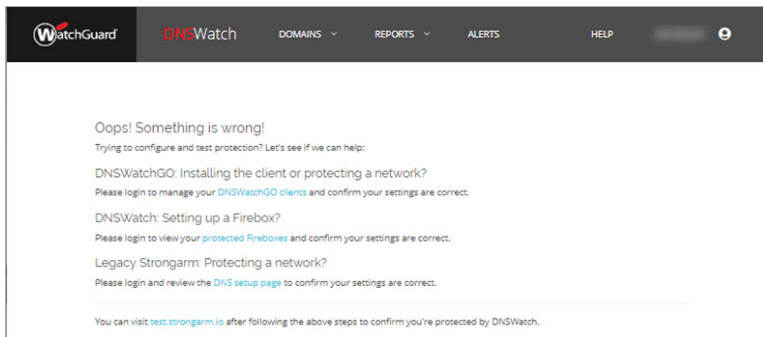
Browse to a domain in a category currently blocked by DNSWatchGO.

1. In your browser, go to [test.strongarm.io](https://test.strongarm.io).
2. Confirm the correct Block Page appears. If the client does not block malicious domains, submit the issue on the WatchGuard beta management platform.

If DNSWatchGO correctly blocks the test domain, you see this Block Page:



If DNSWatchGO does not operate correctly, you see this message:



## View DNSWatch Content Filtering Reports

---



While reports and alerts for connected Fireboxes that use DNSWatch are available, reports and alerts related to DNSWatchGO usage are not yet available. This functionality will be added later in the beta cycle.

DNSWatch stores summary information about the top 20 domains blocked and the number of domains blocked each hour from all your protected addresses. You can choose to see the blocked domains individually or grouped by category.

The available content filtering reports are:

- **Top 20 Domains Blocked** – This chart shows the top 20 domains blocked in the selected week
- **Top 20 Categories Blocked** – This chart shows the top 20 categories of domains blocked in the selected week
- **Blocked Requests per Hour** – This chart shows the number of blocked DNS requests for each hour in the selected week

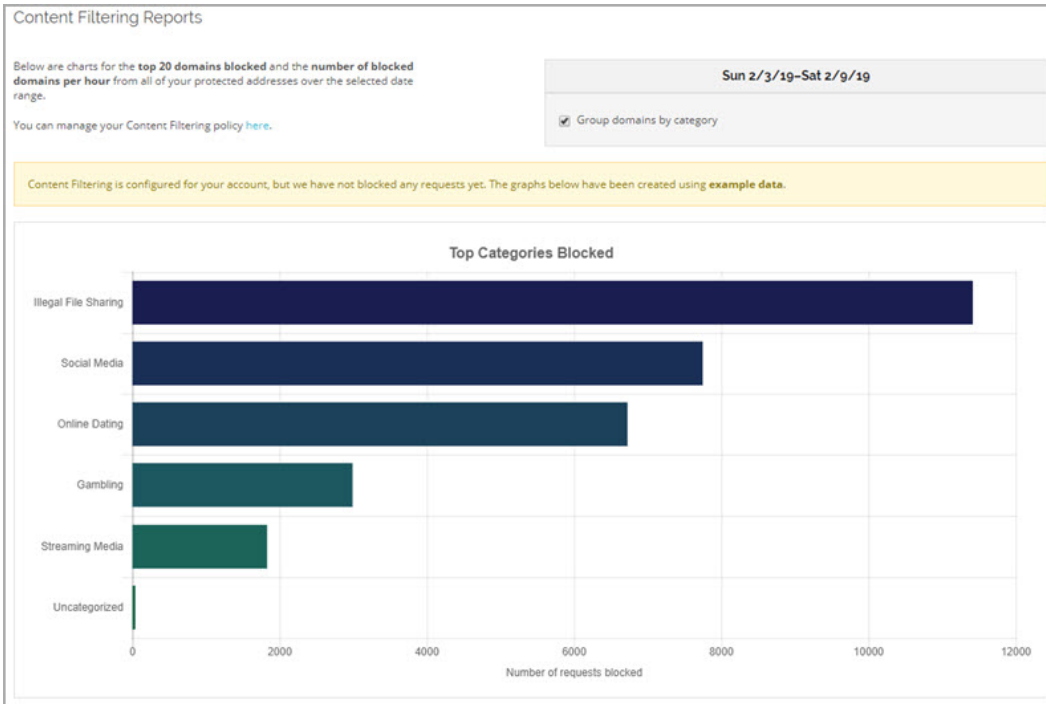
By default, the **Top 20 Domains Requested** report combines domains into categories. If a domain does not match a category, the report shows the domain ranked separately. You can choose whether to combine domains into groups in weekly reports.

To see DNSWatch content filtering reports:

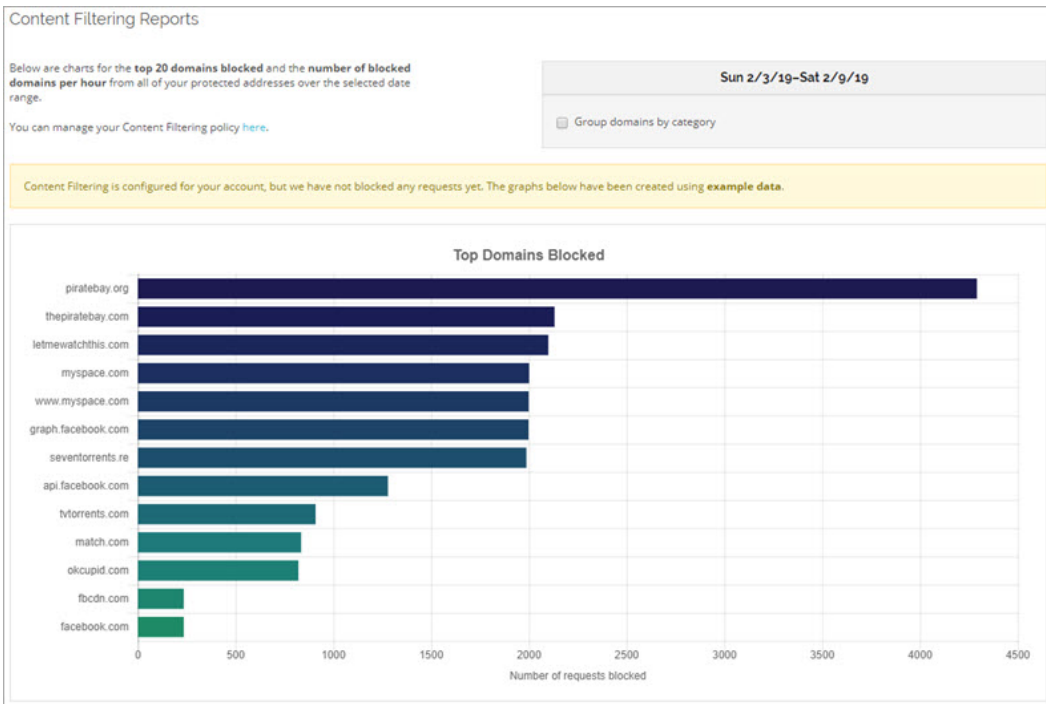
1. Log in to the [DNSWatch Dashboard](#).
2. Select **Reports > Content Filtering Reports**.  
*The Content Filter Reports page appears. By default the reports show Top Categories Blocked for the current week.*
3. To see Top Domains Blocked for the week, clear the **Group domains by category** check box.
4. To see reports for a specific network, from the **Filter by Network** drop-down list, select the name of the network.



DNSWatch reports are available after several hours of DNS requests from your protected networks. For a new DNSWatch account without protected networks, the reports show example data.

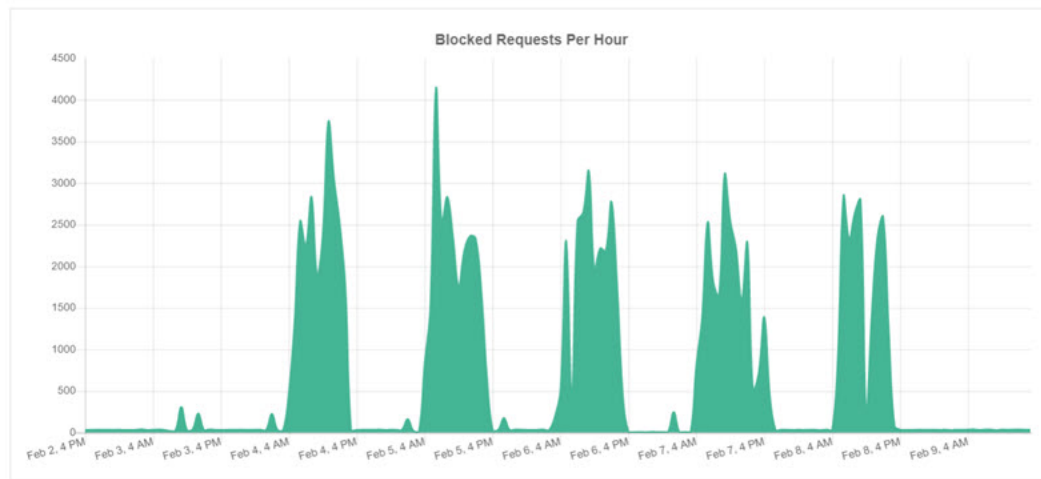


The DNSWatch Top 20 Categories Blocked report with example data



The DNSWatch Top 20 Domains Blocked report with example data





The DNSWatch Blocked Requests Per Hour report with example data

DNSWatch content filtering reports show only the top 20 domains or domain categories. See [View Filtered Requests](#) to search for a specific domain.

## View Filtered Requests

You can view a detailed activity report filtered by these items:

- **Domain Name** – Select a domain to view
- **Category** – Select the content category you want to view
- **Network** – Select which network activity you want to view
- **Time Period** – Select from past week, past 24 hours, or past hour

To see filtered Requests from content filtering:

1. Log in to the [DNSWatch Dashboard](#).
2. Select **Reports > Filtered Requests**.

The Filtered Requests from Content Filtering page appears. Details of all filtered requests in the past week appear in the table.

Filtered Requests from Content Filtering FILTER ▾

Filtered requests are captured when an employee on one of your protected networks tries to visit a website that violates your content filtering policies. This page shows your organization's filtered requests from the past week. You can easily filter this data by category, domain, protected network, and time period.

DOMAIN NAME	LAST SEEN	FIRST SEEN	REQUESTS
<i>No filtered requests to display.</i>			

Domain Name

Category  
..... ▾

Network  
..... ▾

Time Period  
Past week ▾

**APPLY FILTERS**

CLEAR FILTERS

3. To show the filter options, click **Filter**.
4. Make your selections then click **Apply Filter**.  
*The table populates with the requests that meet the selected criteria.*

## Troubleshoot DNSWatchGO

- If you experience issues with DNSWatchGO Client, often the simplest fix is to restart the client service. See [Stop or Start DNSWatchGO](#) for the steps to restart the client.
- Run `nslookup` in Command Prompt to verify your DNS server is localhost 127.0.0.1

If you are on DNSWatchGO v0.10.2 or higher, run diagnostics to get a snapshot of the state of the device when the issue occurred:

1. In the computer's system tray, right-click the DNSWatchGO icon.
2. Select **Show Diagnostics**.  
*The DNSWatchGO Diagnostic application opens.*
3. In the **Domain to test** box, type a domain or leave it blank to test the default domain.
4. Click **Run Tests**.

The diagnostic report currently provides three types of information.

The current client configuration:

- The DNS servers the client uses to resolve DNS
- The network configuration of the device

The network configuration on the client with protection turned on. This information will confirm:

- The adapters have been properly configured to point DNS to the client
- The device is able to properly resolve DNS with protection turned on

The device's network configuration when the client is turned off or paused:

- Ensure the adapters are properly configured to their original configuration
- That DNS query responses are the same as with protection turned on

## View Log Messages

DNSWatchGO Client saves log messages in the `dnswatchgo_client_log.txt` file located in:

```
\ProgramData\WatchGuard\DNSWatch\Logs
```

The **ProgramData** directory is hidden by default. To show the directory:

1. In Windows Explorer, select **Windows (C:)**.
2. In the ribbon, select **View > Options > Change folder and search options**.  
*The Folder Options dialog box appears.*
3. Select the **View** tab.

4. In **Advanced Settings > Files and Folders**, select **Show hidden files, folders, and drives**.
5. Click **Apply**.
6. Click **OK**.

*The ProgramData directory appears on the root of the C: drive.*

## View Log Messages Dynamically

To see the log messages dynamically, use this PowerShell command:

```
Get-Content -Path \ProgramData\WatchGuard\DNSWatch\dnswatchgo_client_log.txt -wait
```

# About DNSWatch Content Filter Categories

DNSWatch uses content categories to group different websites. A website is added to a category when the content of the website meets the criteria for the content category.

If you think a website is not included or is miscategorized, you can send feedback. Submit the website URL and a suggested category, separated by a space, comma, or semicolon. Type each suggestion on a separate line. For example:

```
http://www.seattletimes.com, News and Media
```

```
http://www.soccer.com, Sports
```

To send site categorization feedback:

1. Open a web browser and go to <https://www.watchguard.com/securityportal/UrlCategorization.aspx>.
2. If you are not already logged in to the WatchGuard website, type your **Username** and **Password**. Click **Log in**.  
*The WatchGuard Security Portal appears.*
3. In the text box at the bottom of the page, type the URL of the website and the suggested category, separated by a space, comma, or semicolon.
4. To submit multiple suggestions, type them on separate lines.
5. Select the **I'm not a robot** check box.
6. Complete the reCAPTCHA task, if requested.
7. Click **Submit**.

## Content Filter Categories

### Abortion

Sites with neutral or balanced presentation of the issue.

- **Pro-Choice:** Sites that provide information about or are sponsored by organizations that support legal abortion or that offer support or encouragement to those seeking the procedure.
- **Pro-Life:** Sites that provide information about or are sponsored by organizations that oppose legal abortion or that seek increased restriction of abortion.

### Adult Material

Parent category that contains adult-oriented categories; may also contain age-restricted content.

- **Adult Content:** Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses including clubs, nightclubs, escort services; and sites supporting the online purchase of such goods and services.
- **Lingerie and Swimsuit:** Sites that offer images of models in suggestive but not lewd costume, with semi nudity permitted. Includes classic 'cheesecake,' calendar and pinup art and photography. Includes sites offering lingerie or swimwear for sale.

- **Nudity:** Sites that offer depictions of nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect.
- **Sex:** Sites that depict or graphically describe sexual acts or activity, including exhibitionism; sites offering direct links to such sites.
- **Sex Education:** Sites that offer information about sex and sexuality, with no pomographic intent.

## Advocacy Groups

Sites that promote change or reform in public policy, public opinion, social practice, economic activities and relationships.

## Bandwidth

Sites that use a large amount of bandwidth.

- **Educational Video:** Sites that host videos with academic or instructional content.
- **Entertainment Video:** Sites that host videos with entertainment-oriented content.
- **Internet Radio and TV:** Sites that provide online radio or television programming.
- **Internet Telephony:** Sites that enable users to make phone calls via the Internet or to obtain information or software for that purpose.
- **Peer-to-Peer File Sharing:** Sites that provide client software to enable peer-to-peer file sharing and transfer.
- **Personal Network Storage and Backup:** Sites that store personal files on web servers for backup or exchange.
- **Streaming Media:** Sites that enable streaming of media content.
- **Surveillance:** Sites that enable real-time monitoring of various operations via network cameras, webcams and other video recording devices.
- **Viral Video:** Sites that host videos with high or rapidly rising popularity.

## Business and Economy

Sites sponsored by or devoted to business firms, business associations, industry groups or general business.

- **Financial Data and Services:** Sites that offer investment advice and news and quotations on stocks, bonds and other investment vehicles, but not online trading. Includes banks, credit unions, credit cards and insurance.
- **Hosted Business Applications:** Sites that provide access to business-oriented web applications and allow storage of sensitive data, excluding those for web collaboration.

## Collaboration - Office

Office Category used to manage the Office domain, and includes these functions:

- **Office - Apps:** Office function that enables a user to collaborate via various applications.
- **Office - Documents:** Office function that enables a user to collaborate via document applications.
- **Office - Drive:** Office function that enables a user to collaborate via virtual storage.
- **Office - Mail:** Office function that enables a user to collaborate via email and messaging.

## Drugs

The parent category that contains the following categories:

- **Abused Drugs:** Sites that promote or provide information about the use of prohibited drugs, except marijuana, or the abuse or unsanctioned use of controlled or regulated drugs; also, paraphernalia associated with such use or abuse.
- **Marijuana:** Sites that provide information about or promote the cultivation, preparation or use of marijuana.
- **Nutrition:** Sites that provide information about nutrition.
- **Prescribed Medications:** Sites that provide information about approved drugs and their medical use.

## Education

The parent category that contains the following categories:

- **Cultural Institutions:** Sites sponsored by museums, galleries, theaters (but not movie theaters), libraries and similar institutions; also, sites whose purpose is the display of artworks.
- **Educational Institutions:** Sites sponsored by schools and other educational facilities, by non-academic research institutions, or that relate to educational events and activities.
- **Educational Materials:** Sites that provide information about or that sell or provide curriculum materials or direct instruction; also, learned journals and similar publications.
- **Reference Materials:** Sites that offer reference-shelf content such as atlases, dictionaries, encyclopedias, formularies, white and yellow pages, and public statistical data.

## Entertainment

Sites that provide information about or promote motion pictures, non-news radio and television, books, humor and magazines.

- **Media File Download:** Sites that enable download of media content.

## Extended Protection

The parent category that contains the following categories:

- **Dynamic DNS:** Sites that mask their identity using Dynamic DNS services, often associated with advanced persistent threats (APTs).
- **Elevated Exposure:** Sites that camouflage their true nature or that include elements suggesting latent malicious intent.
- **Emerging Exploits:** Sites found to be hosting known and potential exploit code.
- **Newly Registered Websites:** Scans for newly registered websites on an ongoing basis. The default criteria for classification under the associated category Newly Registered Websites involves unknown (Uncategorized) websites registered within the last 41 days. Exception is given to websites known to pose a live security risk; such websites are assigned security classification regardless of the registration attribute. A website classified under the category Newly Registered Websites may acquire a granular content-based category at any time.
- **Suspicious Content:** Sites found to contain suspicious content.

## Gambling

Sites that provide information about or promote gambling or support online gambling, involving a risk of losing money.

## Games

Sites that enable a user to play or download a game.

## Government

Sites sponsored by branches, bureaus or agencies of any level of government, except for the armed forces.

- Military: Sites sponsored by branches or agencies of the armed services.
- Political Organizations: Sites sponsored by or providing information about political parties and interest groups focused on elections or legislation.

## Health

Sites that provide information or advice on personal health or medical services, procedures, or devices, but not drugs. Includes self-help groups.

## Illegal or Questionable

Sites that provide instruction in or promote nonviolent crime or unethical or dishonest behavior or the avoidance of prosecution.

## Information Technology

Sites sponsored by or providing information about computers, software, the Internet and related business firms, including sites supporting the sale of hardware, software, peripherals and services.

- Computer Security: Sites that provide information about or free downloadable tools for computer security.
- Hacking: Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software or databases.
- Proxy Avoidance: Sites that provide information about how to bypass proxy server features or to gain access to URLs in any way that bypasses the proxy server.
- Search Engines and Portals: Sites that support searching the web, news groups or indices or directories thereof.
- Unauthorized Mobile Marketplaces: Protects against websites that may distribute applications unauthorized by the mobile OS manufacturer, the handheld device manufacturer or the network provider. (Traffic visiting websites in this category may indicate jail-broken or rooted phones.)
- Web Analytics: Sites that are associated with web traffic analysis.
- Web and Email Marketing: Sites that are associated with online marketing.
- Web and Email Spam: Sites whose links are sent in unsolicited commercial email, either as part of campaigns to promote products or services or to entice readers to click through to surveys or similar sites. Also includes sites that display comment spam.
- Web Collaboration: Sites that provide virtual workspace for purposes of collaboration and conferencing, which may include sites that enable authorized access to a computer or network from a remote location.
- Web Hosting: Sites of organizations that provide hosting services, or top-level domain pages of web communities.
- Website Translation: Sites that enable translation of website text.

## Internet Communication

The parent category that contains the following categories:

- General Email: Sites that provide email services open to general use.
- Organizational Email: Log in sites for corporate or institutional email systems.
- Text and Media Messaging: Sites that enable the sending of messages and other content via SMS, EMS, MMS or similar protocols.
- Web Chat: Sites that host web chat services or that support or provide information about chat via HTTP or IRC.

## Intolerance

Sites that condone intolerance towards any individual or group.

## Job Search

Sites that offer information about or support the seeking of employment or employees.

## Militancy and Extremist

Sites that offer information about or promote or are sponsored by groups advocating antigovernment beliefs or action.

## Miscellaneous

The parent category that contains the following categories:

- Content Delivery Networks: Commercial hosts that deliver content to subscribing websites.
- Dynamic Content: URLs that are generated dynamically by a web server.
- File Download Servers: Web servers whose primary function is to deliver files for download.
- Network Errors: URLs with hosts that do not resolve to IP addresses.
- Private IP Addresses: IP addresses defined in RFC 1918, 'Address Allocation for Private Intranets.'
- Web Images: Sites that deliver image content.
- Web Infrastructure: Sites that are associated with website architecture.

## News and Media

Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines or other media.

- Alternative Journals: Online equivalents to supermarket tabloids and other fringe publications.

## Parked Domain

Sites that are expired, offered for sale, or known to display targeted links and advertisements.

## Productivity

The parent category that contains the following categories:



- Advertisements: Sites that provide advertising graphics or other ad content files.
- Application and Software Download: Sites that enable download of software, applications.
- Instant Messaging: Sites that enable instant messaging.
- Message Boards and Forums: Sites that host message boards, bulletin boards and other unaffiliated discussion forums.
- Online Brokerage and Trading: Sites that support active trading of securities and investment management.
- Pay-to-Surf: Sites that reward users for online activity such as viewing websites, advertisements or email.

## Religion

The parent category that contains the categories:

- Non-Traditional Religion: Sites that provide information about non-traditional religious beliefs and practices.
- Traditional Religions: Sites that provide information about or promote Bahai, Buddhism, Christian Science, Christianity, Hinduism, Islam, Judaism, Mormonism, Shinto and Sikhism, as well as atheism.

## Security

Security-related website categories that allow you to develop policies to deny access to sites associated with spyware, phishing, keylogging and malicious mobile code.

- Advanced Malware Command and Control: Protects against outbound transmissions from a compromised machine to a malicious command-and-control center.
- Bot Networks: Sites that host the command-and-control centers for networks of bots that have been installed onto users' computers. (Excludes web crawlers.)
- Compromised Websites: Sites that are vulnerable and known to host an injected malicious code or unwanted content.
- Keyloggers: Sites that download programs that record all keystrokes, and which may send those keystrokes (potentially including passwords or confidential information) to an external party.
- Malicious Embedded Link: Sites infected with a malicious link.
- Malicious Embedded Iframe: Sites infected with a malicious iframe.
- Malicious Websites: Sites containing code that may intentionally modify users' systems without their consent and cause harm.
- Mobile Malware: Protects against malicious websites and applications designed to run on mobile devices.
- Phishing and Other Frauds: Sites that counterfeit legitimate sites to elicit financial or other private information from users.
- Potentially Unwanted Software: Sites using technologies that alter the operation of a user's hardware, software or network in ways that diminish control over the user experience, privacy or the collection and distribution of personal information.
- Spyware: Sites that download software that generate HTTP traffic (other than simple user identification and validation) without a user's knowledge.
- Suspicious Embedded Link: Sites suspected of being infected with a malicious link.

## Shopping

Sites that support the online purchase of consumer goods and services except: sexual materials, lingerie, swimwear, investments, medications, educational materials, computer software or hardware, alcohol, tobacco, travel, vehicles and parts, weapons.

- Internet Auctions: Sites that support the offering and purchasing of goods between individuals.
- Real Estate: Sites that provide information about renting, buying, selling or financing residential real estate.

## Social Organizations

The parent category that contains the following categories:

- Professional and Worker Organizations: Sites sponsored by or that support or offer information about organizations devoted to professional advancement or workers' interests.
- Service and Philanthropic Organizations: Sites sponsored by or that support or offer information about organizations devoted to doing good as their primary activity.
- Social and Affiliation Organizations: Sites sponsored by or that support or offer information about organizations devoted chiefly to socializing or common interests other than philanthropy or professional advancement.

## Social Web - Facebook

Category used to manage the Facebook domain, and includes these functions:

- Facebook Posting: Facebook function that enables a user to share a post, status or link.
- Facebook Commenting: Facebook function that enables a user to comment or like.
- Facebook Friends: Facebook function that enables a user to add a connection.
- Facebook Photo Upload: Facebook function that enables a user to upload a photo.
- Facebook Mail: Facebook function that enables a user to send an email within the Facebook community.
- Facebook Events: Facebook function that enables a user to create, modify or respond to an event within the Facebook community.
- Facebook Apps: Facebook function that enables a user to access or utilize an app.
- Facebook Chat: Facebook function that enables a user to chat within the Facebook community.
- Facebook Questions: Facebook function that enables a user to ask a question within the Facebook community.
- Facebook Video Upload: Facebook function that enables a user to upload a video.
- Facebook Groups: Facebook function that enables a user to create, modify or join a group within the Facebook community.
- Facebook Games: Facebook function that enables a user to access or play a game.

## Social Web - LinkedIn

Category used to manage the LinkedIn domain, and includes these functions:

- LinkedIn Updates: LinkedIn function that enables a user to edit a profile or post an update.
- LinkedIn Mail: LinkedIn function that enables a user to send an email within the LinkedIn community.

- LinkedIn Connections: LinkedIn function that enables a user to add a connection.
- LinkedIn Jobs: LinkedIn function that enables a user to perform activities related to job search.

## Social Web - Twitter

Category used to manage the Twitter domain, and includes these functions:

- Twitter Posting: Twitter function that enables a user to post an update.
- Twitter Mail: Twitter function that enables a user to send an email within the Twitter community.
- Twitter Follow: Twitter function that enables a user to add a connection.

## Social Web - YouTube

Category used to manage the YouTube domain, and includes these functions:

- YouTube Commenting: YouTube function that enables a user to comment, like or dislike.
- YouTube Video Upload: YouTube function that enables a user to upload a video.
- YouTube Sharing: YouTube function that enables a user to share a video within and outside of the YouTube community.

## Society and Lifestyles

Sites that provide information about matters of daily life, excluding entertainment, health, hobbies, jobs, sex and sports.

- Alcohol and Tobacco: Sites that provide information about, promote, or support the sale of alcoholic beverages or tobacco products or associated paraphernalia.
- Blogs and Personal Sites: Sites that host blogs and personal sites.
- Gay or Lesbian or Bisexual Interest: Sites that provide information about or cater to gay, lesbian, or bisexual lifestyles, but excluding those that are sexually or issue oriented.
- Hobbies: Sites that provide information about or promote private and largely sedentary pastimes, but not electronic, video or online games.
- Personals and Dating: Sites that assist users in establishing interpersonal relationships, excluding those intended to arrange for sexual encounters.
- Restaurants and Dining: Sites that list, review, advertise or promote food, dining, or catering services.
- Social Networking: Sites of web communities that provide users with means for expression and interaction.

## Special Events

Sites devoted to a current event that requires separate categorization.

## Sports

Sites that provide information about or promote sports, active games, and recreation.

- Sport Hunting and Gun Clubs: Sites that provide information about or directories of gun clubs and similar groups, including war-game and paintball facilities.

## **Tasteless**

Sites with content that is gratuitously offensive or shocking, but not violent or frightening. Includes sites devoted in part or whole to scatology and similar topics or to improper language, humor or behavior.

## **Travel**

Sites that provide information about or promote travel-related services and destinations.

## **Vehicles**

Sites that provide information about or promote vehicles, including those that support online purchase of vehicles or parts.

## **Violence**

Sites that feature or promote violence or bodily harm, including self-inflicted harm; or that gratuitously display images of death, gore or injury; or that feature images or descriptions that are grotesque or frightening and of no redeeming value.

## **Weapons**

Sites that provide information about, promote, or support the sale of weapons and related items.

