

WEBROOT®

an **opentext™** company

DNS Protection Admin Guide

Copyright

Copyright 2019 Webroot. All rights reserved.

DNS Protection Admin Guide

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Webroot.

Table of Contents

Chapter 1: DNS Protection Admin Guide	1
DNS Protection Overview	2
Getting Started	3
Trial Expired?	3
Trial Expiration Behavior	3
Chapter 2: Configuring the Web Console Overview	4
Beginning to Setup DNS Protection	5
Servers	5
Workstations	5
Configuring Sites	6
Network Settings	6
Domain Bypass List (Intranet)	7
Defining Filters	8
Chapter 3: Installing the Agent Overview	9
Installing the Agent	10
Managing DNS Through Groups	11
Advanced Group Management	14
Moving Systems Between Groups	15
DNS Agent Behavior - Loopback	16
About Supported VPNs	18
Policy Enforcement through the Webroot DNS Protection Agent	18
Policy Enforcement through Webroot Network DNS Protection	18
Uninstalling the Agent	19
Chapter 4: Configuring the Network	21
Updating Network Settings	22
Testing Network DNS Resolution - Network Only	23
Configuring Local DNS Servers	24
Installing Certificates	26
Chapter 5: Working With Block Pages And Overrides	27
Web Block Page Settings	28
Configuring Web Overrides	29
Web Overrides	29
Filtering Exceptions – Web Block / Allow List	29
Adding Exceptions	29

Viewing Exceptions	30
Creating DNS Protection Web Overrides	31
Chapter 6: Working With Reports	37
DNS Protection Reports Overview	38
Generating DNS Protection Reports	39
Exporting CSV Files	45
Chapter 7: Configuring Firewalls	48
Configuring Firewalls	49
Chapter 8: Accessing Usage Data	50
About Accessing Usage Data	51
Chapter 9: DNS Protection Support	52
Accessing Technical Support	53
Chapter 10: Appendix	54
Domain Groups and Categories Overview	55
Webroot Domain Groups	55
Security Risk Domain Group	56
Human Resources Protections Domain Group	58
Questionable and Legal Domain Group	61
Social Media and Internet Communication Domain Group	64
Shopping Domain Group	67
Entertainment Domain Group	68
Lifestyle Domain Group	70
Business / Government Services Domain Group	72
General Information Domain Group	76
Uncategorized Domain Group	79
Index	i

Chapter 1: DNS Protection Admin Guide

To get started using the DNS Protection Admin Guide, see the following topics:

DNS Protection Overview	2
Getting Started	3
Trial Expired?	3
Trial Expiration Behavior	3

DNS Protection Overview

This document is designed as an admin guide for deploying and using Webroot DNS Protection. It is intended as a technical resource for network administrators and those that will be configuring or managing DNS Protection.

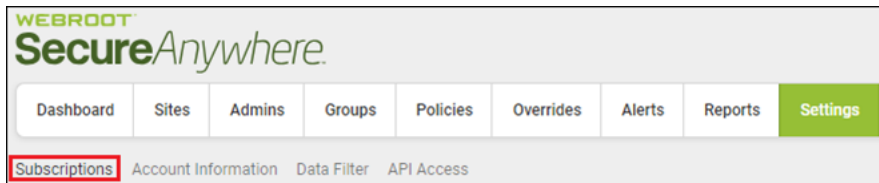
For step-by-step deployment information, please see the [Webroot DNS Protection Getting Started Guide](#).

Getting Started

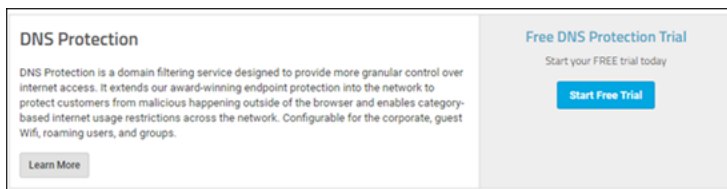
In order to use DNS Protection and for the DNS settings to be available in your console, it must first be licensed. If you have not already signed up to trial or purchased DNS Protection, you can easily do so from the Settings tab in the GSM console.

To trial or purchase DNS Protection:

1. From the Settings tab, click the **Subscriptions** tab.



2. Here you can initiate a trial by clicking the **Start Free Trial** button. Once the trial is active or once you have purchased, you can use the Subscriptions tab to reference the remaining days on your trial or your subscription status.



Trial Expired?

If you have already trialed DNS protection and want to do so again, [please reach out to your sales representative](#).

Trial Expiration Behavior

- **DNS Agent** – If your trial expires, any DNS Protection agents that have been deployed will automatically uninstall and the DNS settings will revert to their original settings. For more information see [Installing the Agent](#).
- **DNS Network Protection** – If you are using the Network version of DNS Protection, please revert the DNS settings on your router and DNS Forwarders. The Webroot DNS servers will only respond to accounts that have purchased or have active trials. For more information, see [Configuring the Network](#).

Chapter 2: Configuring the Web Console

Overview

To configure DNS Protection, the following settings need to be configured:

Beginning to Setup DNS Protection	5
Servers	5
Workstations	5
Configuring Sites	6
Network Settings	6
Domain Bypass List (Intranet)	7
Defining Filters	8

Beginning to Setup DNS Protection

DNS Protection has two components: An agent-based solution that allows granular control of DNS independent of the network and a network solution designed to protect your network as a whole. Although it is possible to run each component individually, they are designed to complement each other and work in parallel to comprehensively protect the network and attached systems.

In each instance, you will need to define a filter (policy).

- [Configuring Sites on page 6](#)
- [Defining Filters](#)

Servers

The most effective way to protect servers with Webroot DNS Protection is to use the Network version.

This is done by registering the WAN IP address associated with the network you want to protect and then by adding the Webroot DNS Protection servers as the forwarders for external resolution on your AD DNS Servers. For more information, see [Configuring the Network](#).

Note: In some instances, you may find the need for granular control of DNS for specific servers, depending on their role. The DNS Protection Agent is not supported on DNS or RDS (Terminal) Servers. For more information on installing the agent, see [Installing the Agent Overview](#).

Workstations

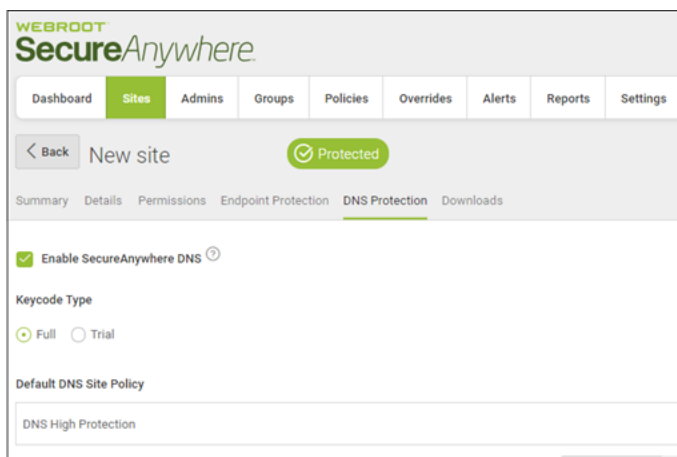
The DNS Protection Agent is designed to filter DNS requests on workstations. Active Directory DNS requests will be fielded by the local servers, but internet DNS requests will be filtered based on the applied Webroot DNS filter. This allows for granular control and reporting regardless of the network to which they are connected. For more information on installing the agent, see [Installing the Agent Overview](#).

Configuring Sites

Each Site can be individually configured for DNS Protection. The DNS Protection column shows the status of each site.

To configure DNS Protection for a site:

1. Do either of the following:
 - Click the **Gear** icon.
 - Click the **Manage** button, then go to the DNS tab.
2. Select whether the site is licensed or a trial.



Note: The Default DNS Policy is the default DNS Policy assigned when any new Endpoint or IP is added. Changing this setting will update the policy for any Endpoint configured to inherit its policy from the site. Alternate policies can be assigned to Groups, Endpoints and IP addresses under the Groups tab.

Network Settings

The most effective way to protect servers with Webroot DNS Protection is to use the Network version. This is configured by registering the WAN IP address associated with the network you wish to protect, and then to add the Webroot DNS Protection servers as the forwarders for external resolution on your AD DNS Servers.

Additionally, this can be used to control content on Wi-Fi and guest networks as well limit of content available over different circuit types. More information on setting up Network DNS filtering can be found [here](#).

Domain Bypass List (Intranet)

The Domain Bypass List (Intranet) applies only to the DNS Protection Agent. It is designed to accommodate Active Directory. Entries in the list are passed to your AD DNS server rather than filtered by the DNS Protection Agent. Be sure to include the wildcard to ensure you encompass all resources under this domain.



The screenshot shows a web interface for configuring the Domain Bypass List (Intranet). At the top, there is a title bar that reads "Domain Bypass List (Optional)" with a help icon. Below this is a button labeled "Add Row" with a plus icon. The main area is a table with a header row labeled "Domain". Below the header, there is a single row containing the text "*.companydomain.local". At the bottom of the table, there is a green button labeled "Save Changes".

Defining Filters

Policies for DNS Protection provide the ability to customize which categories are available or blocked. These Policies can be linked to Sites, Groups, or Endpoints to implement filtering. Policies for DNS Protection are managed under the DNS subtab under the Policies section of the console. If the DNS tab is not visible, [check that your DNS Subscription is current](#).

You will want to create custom Policies beyond the provided static policies (DNS High Protection and DNS Medium Protection). To do so, click the **Add** or **Copy** button, provide the Policy Name and Description, and a new policy will be created. This can then be configured by selecting from the 80 available categories. More information about each category can be found in the [appendix](#).

Dashboard Sites Admins Groups **Policies** Overrides Alerts Reports Settings

Endpoint DNS

+ Add Copy Delete Import

SecureAnywhere DNS Policies

- DNS High Protection
- DNS Medium Protection
- Demo Policy**

Demo Policy

Name
Demo Policy

Description
Demo Policy

Recommended

- ☒ Security Risk All selected
- ☒ Human Resource Protections All selected
- ☒ Questionable / Legal All selected

Chapter 3: Installing the Agent Overview

Once a Site has DNS Protection enabled, the settings inside the Endpoint Policy for DNS Protection become active. This controls whether the DNS Agent is installed. You can use the provided Recommended DNS Enabled Policy or create a custom Policy with Install DNS Protection set to On. It is recommend that a copy be made of your existing Endpoint Policy, and then to change Install DNS protection to On. Once complete, this Policy can be applied to endpoints for which the DNS Agent is to be installed.

To start deploying the agent, see the following topics:

Installing the Agent	10
Managing DNS Through Groups	11
Advanced Group Management	14
Moving Systems Between Groups	15
DNS Agent Behavior - Loopback	16
About Supported VPNs	18
Policy Enforcement through the Webroot DNS Protection Agent	18
Policy Enforcement through Webroot Network DNS Protection	18
Uninstalling the Agent	19

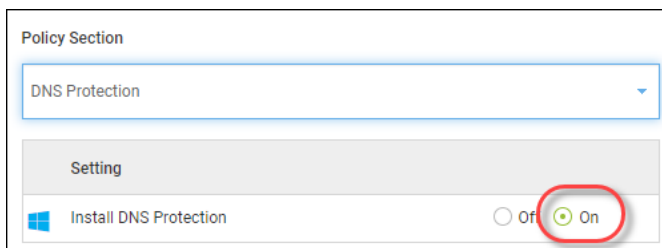
Installing the Agent

Once you have enabled DNS for a Site and have a filtering Policy, the next step is to install the DNS Protection Agent. The Endpoint Policy (Policies – Endpoint) controls whether the DNS agent is installed or uninstalled. You can use the provided Recommended DNS Enabled Policy or create a custom Policy with Install DNS Protection set to **On**.

Note: For Custom Policies for DNS Protection, it is recommend that a copy be made of your current in-use Endpoint Policy, and then to change Install DNS protection to On. Once complete, this Policy can be applied to endpoints for which the DNS Agent is to be installed.

To configure the policy:

1. Click **Global Settings** and click the **Endpoint** tab.
2. Select an appropriate Policy and click the **Copy** button. Save this as a new Endpoint Policy.
3. Enable **Install DNS Protection** for the new Policy.

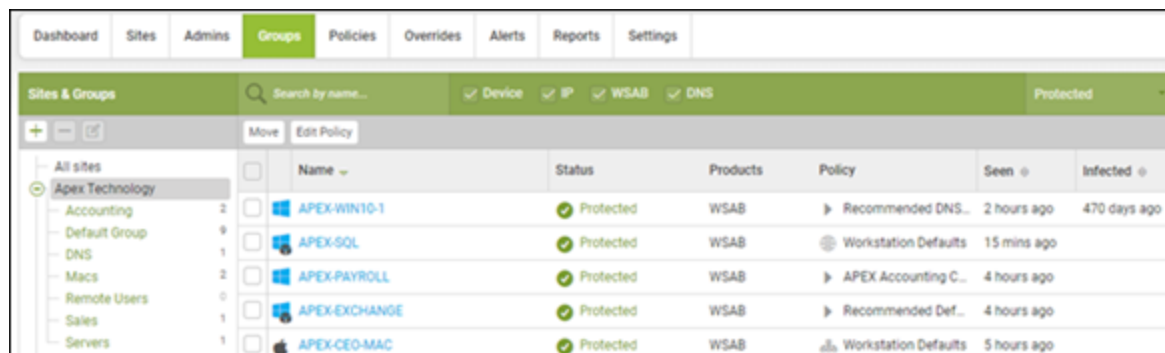


Managing DNS Through Groups

There are two types of Policies, one for Endpoint management and one for DNS management. These can both be managed by configuring Groups, either by selecting a device or IP from within a Group or by selecting the Group itself.

Groups are managed in the Groups tab. From here, you can see each configured Site:

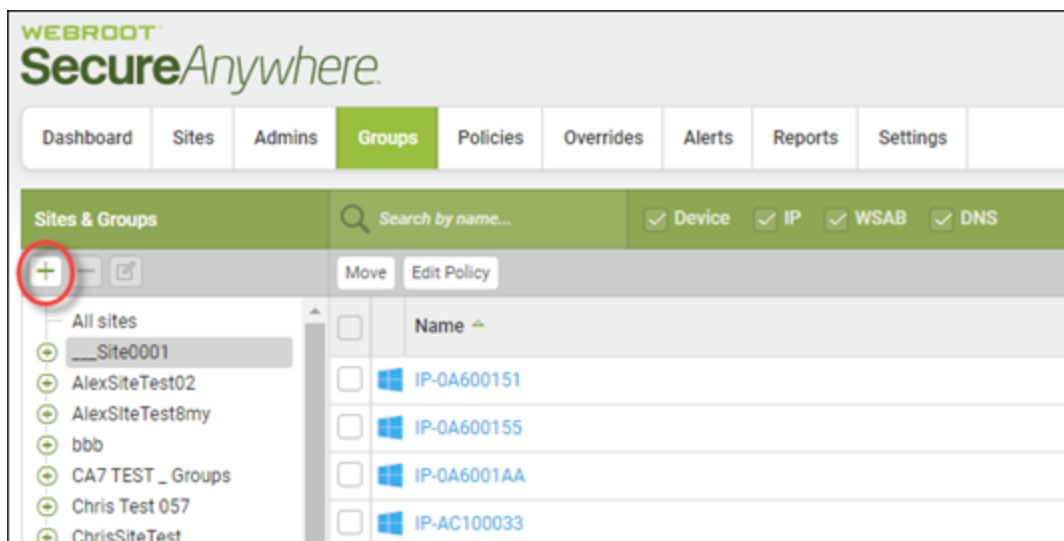
- Click the Site name to display a list of all devices in that Site.
- Click the **Plus (+)** sign next to the Site to display the associated Groups.



Sites & Groups							
Search by name...		Device	IP	WSAB	DNS	Protected	
	Move	Edit Policy					
All sites							
Apex Technology							
Accounting	2						
Default Group	9						
DNS	1						
Macs	2						
Remote Users	0						
Sales	1						
Servers	1						
Name	Status	Products	Policy	Seen	Infected		
APEX-WIN10-1	Protected	WSAB	Recommended DNS...	2 hours ago	470 days ago		
APEX-SQL	Protected	WSAB	Workstation Defaults	15 mins ago			
APEX-PAYROLL	Protected	WSAB	APEX Accounting C...	4 hours ago			
APEX-EXCHANGE	Protected	WSAB	Recommended Def...	4 hours ago			
APEX-CEO-MAC	Protected	WSAB	Workstation Defaults	5 hours ago			

To add a new Group under a Site:

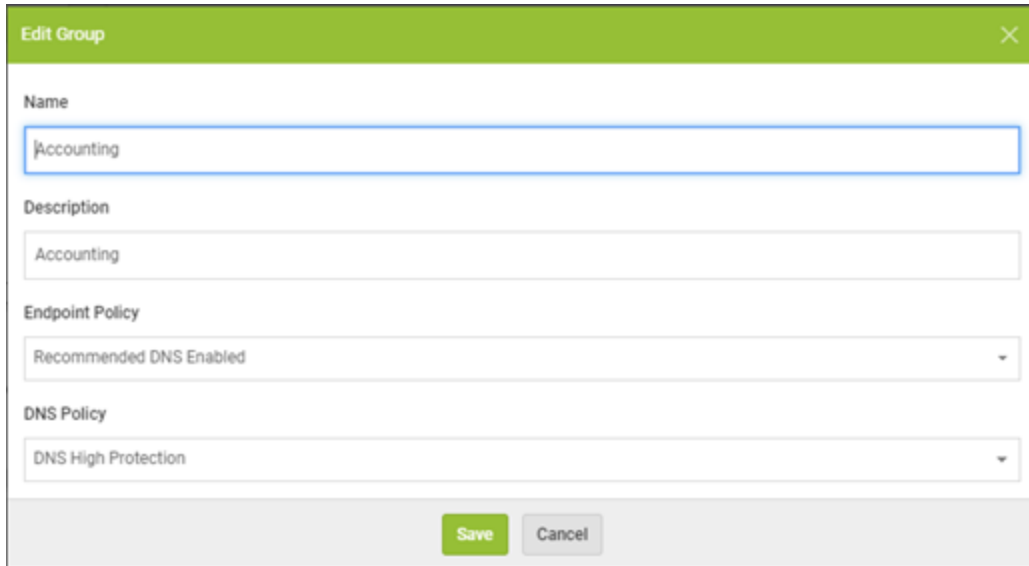
1. Select the Site and then click the **Plus (+)** button.



Sites & Groups							
Search by name...		Device	IP	WSAB	DNS		
	Move	Edit Policy					
All sites							
Site0001							
AlexSiteTest02							
AlexSiteTest8my							
bbb							
CA7 TEST _ Groups							
Chris Test 057							
ChrisSiteTest							
Name							
IP-0A600151							
IP-0A600155							
IP-0A6001AA							
IP-AC100033							

2. When prompted, enter a group name, description, and specify the corresponding Endpoint and DNS Policies.
3. As with specific systems, in order for the DNS Agent to install on systems within this Group, the Endpoint Policy must have Install DNS Protection set to **On**.

Any system you place in this Group will inherit these Policies and, assuming DNS is On, will install the Agent.



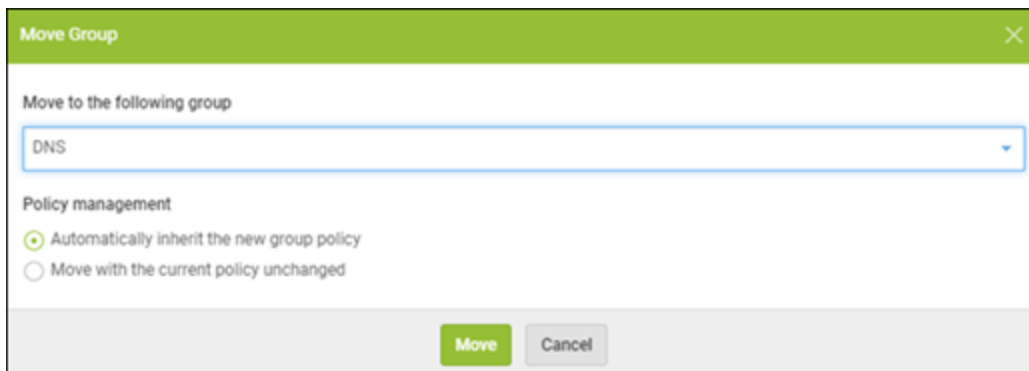
The 'Edit Group' dialog box has a green header bar with the title 'Edit Group' and a close button (X). The form contains the following fields:

- Name:** A text input field containing 'Accounting'.
- Description:** A text input field containing 'Accounting'.
- Endpoint Policy:** A dropdown menu showing 'Recommended DNS Enabled'.
- DNS Policy:** A dropdown menu showing 'DNS High Protection'.

At the bottom right, there are two buttons: a green 'Save' button and a grey 'Cancel' button.

To move a system to a different Group:

1. Select it and click the **Move** button.
2. A prompt will ask for the destination Group as well as whether to inherit that Group's Policy.

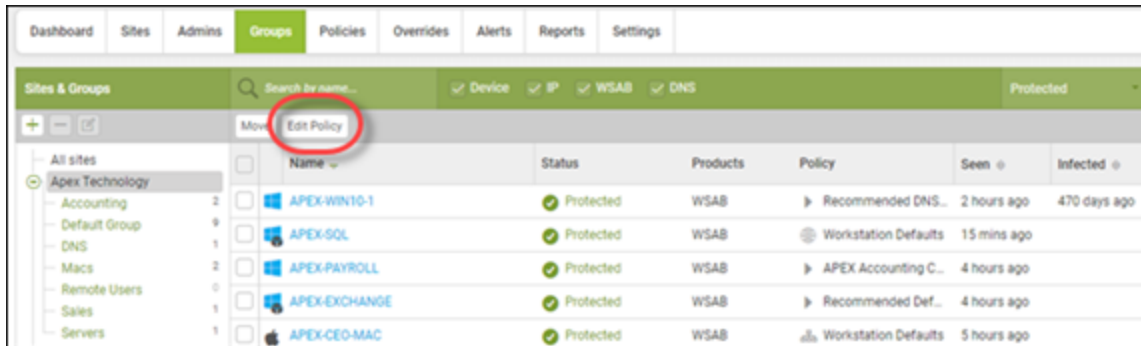


The 'Move Group' dialog box has a green header bar with the title 'Move Group' and a close button (X). The form contains the following fields:

- Move to the following group:** A dropdown menu showing 'DNS'.
- Policy management:** Two radio button options:
 - ☒ Automatically inherit the new group policy
 - ☐ Move with the current policy unchanged

At the bottom right, there are two buttons: a green 'Move' button and a grey 'Cancel' button.

3. Alternately you can select to copy the Policy setting with the device by selecting **Move with the current Policy unchanged**.
4. The DNS and Endpoint Policies can also be managed independently of the Group. Select the device or IP and click the **Edit Policy** button.



5. You can then specify what Policies apply.

The 'Edit Policy' dialog box has a green header with a close button. It contains two sections: 'Endpoint Policy' and 'DNS Policy', each with a dropdown menu set to 'Leave Unchanged'. At the bottom are 'Change' and 'Cancel' buttons.

Endpoint Policy
Leave Unchanged

DNS Policy
Leave Unchanged

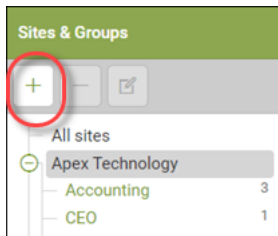
Change Cancel

Advanced Group Management

Groups can also be used as containers to group like systems both for Endpoint and DNS settings.

To add a new group under a site:

1. Select the site and then click the **Plus (+)** button.



2. When prompted, enter a group name, description, and specify the corresponding Endpoint and DNS Policies.

3. As with specific systems, in order for the DNS Agent to install on systems within this Group, the Endpoint Policy must have Install DNS Protection set to **On**.

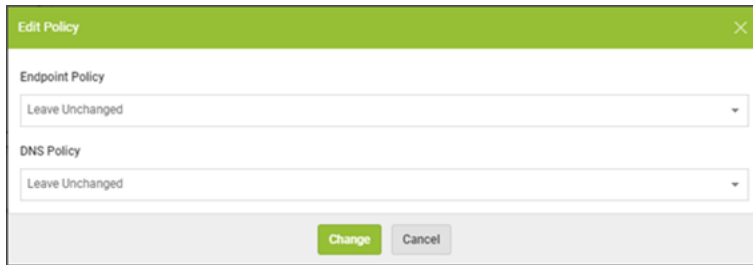
Any system you place in this group will inherit these policies and, assuming DNS is On, will install the Agent.

Moving Systems Between Groups

Follow this procedure to move a policy to a different group.

To move a system to a different group:

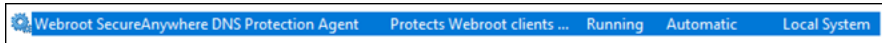
1. Select it and click the **Move** button. A prompt will ask for the destination group as well as whether to inherit that group's policy.
2. Alternately you can select to copy the policy setting with the device by selecting **Move** with the current policy unchanged.



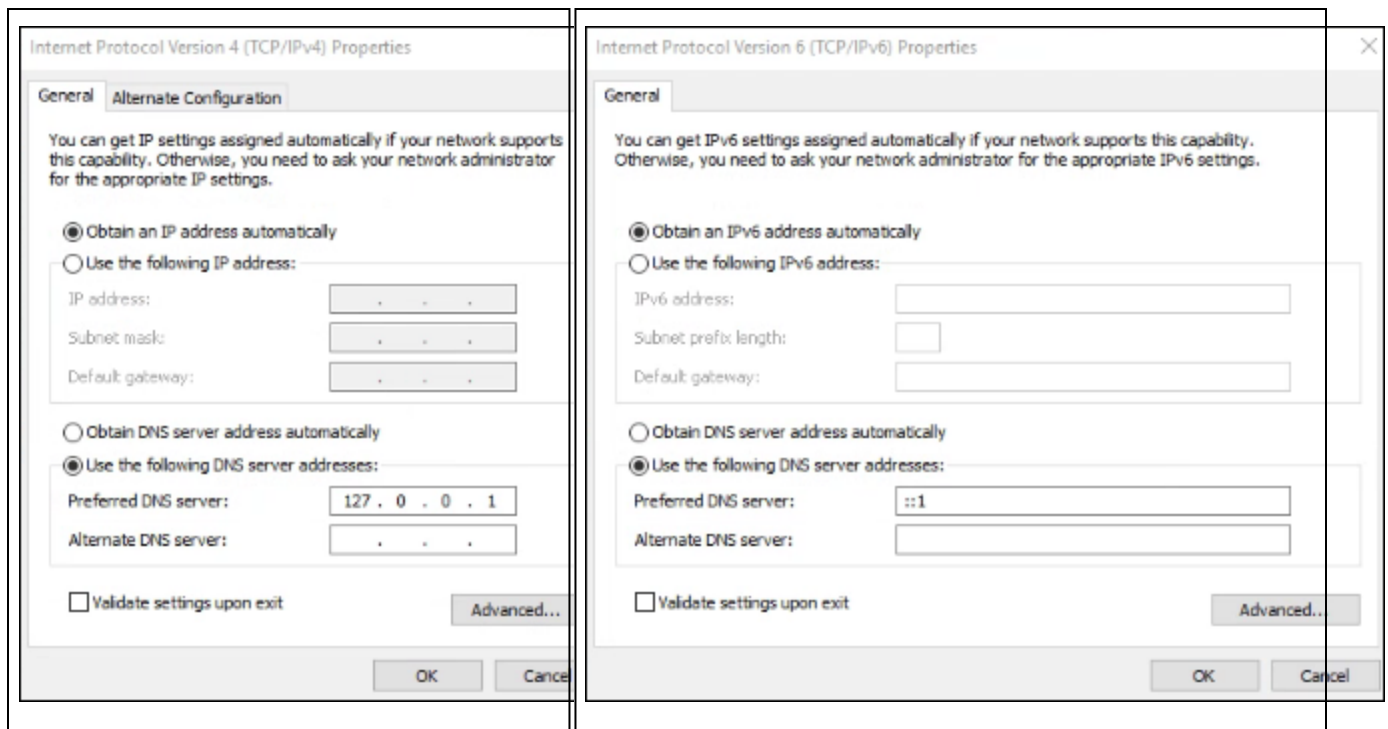
The screenshot shows a dialog box titled "Edit Policy" with a green header bar and a close button (X) in the top right corner. Inside the dialog, there are two sections: "Endpoint Policy" and "DNS Policy". Each section has a dropdown menu currently set to "Leave Unchanged". At the bottom of the dialog, there are two buttons: a green "Change" button and a grey "Cancel" button.

DNS Agent Behavior - Loopback

The DNS Protection agent, once installed, will setup a service, the Webroot SecureAnywhere DNS Protection Agent.



When the service starts, it inspects the active network adapters and notes the current settings for DNS, saving these settings. The IPv4 and IPv6 DNS settings for the adapters are then set to Loopback.



The Webroot SecureAnywhere DNS Protection Agent Service will await DNS requests, and, since the DNS settings are now set to loopback, any DNS requests initiated by the system can be answered by the agent. All internet DNS requests will receive a filtered response, and all AD or local DNS requests are sent to the original previously saved DNS settings. Note that these settings are updated whenever the service is restarted or the connection status of the network adapter changes.

DNS Settings

When the Webroot SecureAnywhere DNS Protection Agent Service starts, the DNS settings are set to loopback. When the service is stopped, the DNS settings are reverted to their previous state. While the service is running, any DNS changes, such as manually setting an alternate IP or changing DNS to DHCP, are disregarded and the settings are again set to loopback.

About Supported VPNs

The following VPNs are supported by the Webroot DNS Agent. Due to the different VPN configurations, some VPNs do not allow for the DNS requests to be filtered. In this instance, the system is protected by the DNS settings provided by the firewall or the network to which it is connected.

Policy Enforcement through the Webroot DNS Protection Agent

- Fortinet VPN
- PulseSecure
- SonicWall Mobile Connect

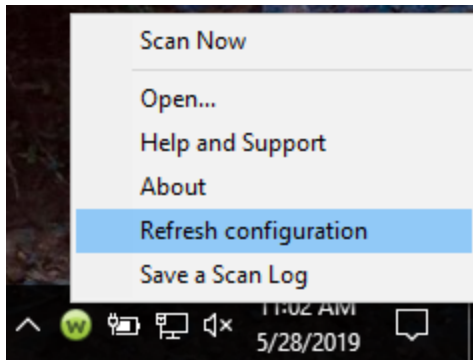
Policy Enforcement through Webroot Network DNS Protection

- Cisco AnyConnect
 - Pure VPN
 - Safer VPN
 - SonicWall NetExtender
 - WatchGuard VPN
-

Uninstalling the Agent

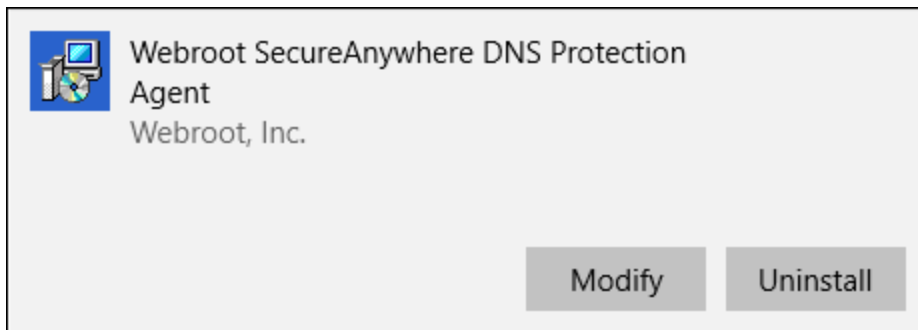
The Endpoint Agent controls both the install as well as the uninstall of the DNS Protection Agent. To uninstall the DNS Agent, apply a Policy that does not have DNS Protection set to on. For more information on setting this Policy, see [Installing the Agent on page 10](#).

The Endpoint Policy change takes effect at Agent Poll. To force the Agent to Poll, in the task bar, right click the **Webroot** icon and select **Refresh configuration**.



You can verify the DNS agent has been uninstalled by checking Programs and Features > Webroot Secure Anywhere DNS Protection Agent. If this application is not listed, the DNS Protection Agent is not installed.

Note: At uninstall, the DNS settings will also revert to their previous settings.



Note: The DNS Protection Agent can also be manually uninstalled from Programs and Features. However, if the Policy is set to install the Agent, it will be automatically reinstalled.

Chapter 4: Configuring the Network

Configuring the network to filter all DNS requests is recommended to strengthen security. This provides a foundation both from a threat perspective as well as content.

To start configuring the network, see the following topics:

Updating Network Settings	22
Testing Network DNS Resolution - Network Only	23
Configuring Local DNS Servers	24
Installing Certificates	26

Updating Network Settings

On your network, identify the public IPv4 address used for internet access (WAN IP). An internet search of My IP generally reveals the appropriate IP address.

Select Add Row to add an IP address to the Site. Once the IP has been added, associate a filtering Policy. Any DNS requests received from this WAN IP will receive a corresponding response based on this filter. Requests from unregistered IP addresses or from IP addresses under expired or disabled sites will not receive a response.



Network Settings (Optional) ?

+ Add Row

IP Address	Policy
22.33.44.55	DNS High Protection

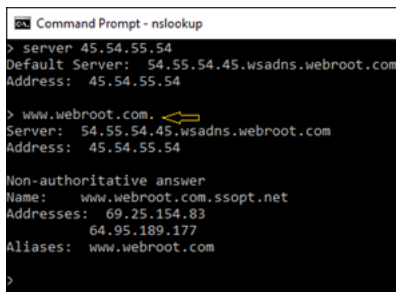
Testing Network DNS Resolution - Network Only

Once the IP addresses and the Policies have been configured, it needs to be confirmed that the DNS Protection Servers are responding with appropriate information *before* updating Forwarders. This can be done from an endpoint on the network to be protected.

To test resolution for the network:

1. Open a command prompt.
2. Run NSLookup.
3. Set the server to 45.54.55.54.
4. Check several Sites to confirm valid responses. Note, some network environments append a suffix to DNS Lookups. In the example, a '.' has been added to the end of `www.webroot.com` to avoid possible resolution problems.

A successful test looks like the following:



```
Command Prompt - nslookup
> server 45.54.55.54
Default Server:  54.55.54.45.wsadns.webroot.com
Address:  45.54.55.54

> www.webroot.com.
Server:  54.55.54.45.wsadns.webroot.com
Address:  45.54.55.54

Non-authoritative answer
Name:    www.webroot.com.ssopt.net
Addresses: 69.25.154.83
          64.95.189.177
Aliases: www.webroot.com
>
```


Configuring Local DNS Servers

Once you have successfully tested that the Webroot DNS Servers are responding correctly, you can then configure your network to use the Webroot DNS Protections servers. This setting should be managed on the router or, in the case of a Windows server, under the DNS forwarders.

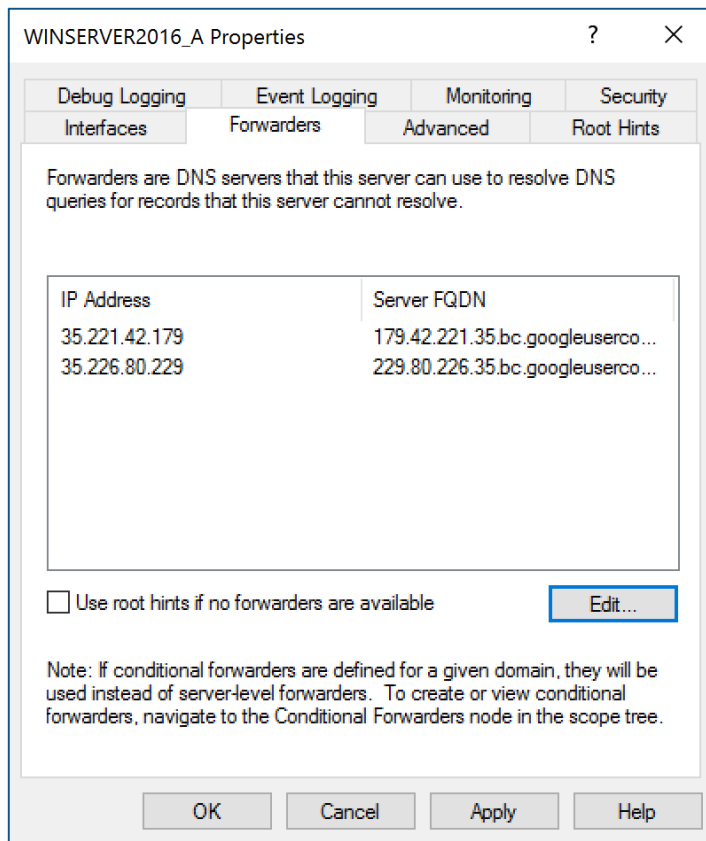
To find the best DNS servers for your location, click the **Manage** button next to the site for which you have enabled DNS, go to the DNS Protection tab, and select your region from the dropdown.

Site 
Apex Technology Manage 

The best primary and secondary DNS servers will be listed.

Network Location	
United States (East) 	
Webroot DNS Servers - United States (East)	
PRIMARY 35.221.42.179	SECONDARY 35.226.80.229

Once you have identified the best resolvers, your DNS forwarders need to be updated as in this example for a server in the United States (East).



Installing Certificates

The Agent automatically installs the certificates to the endpoint. If a system is running on a network protected by DNS Protection and is not using the agent, certificates need to be installed to avoid browser errors when https websites are blocked. Although skipping this step will not stop filtering, it does avoid certificate errors when an https Site is redirected.

Certificates can be downloaded from behind a registered IP address:

<http://45.54.55.55/download>

The certificate needs to be installed to Trusted Root Certification Authorities. This can be done on individual systems or, depending on your environment, pushed out automatically.

To install a certificate:

1. Click **Start**, click **Start Search**.
 2. In the Search field, type *mmc*, then press **Enter**.
 3. From the File menu, select **Add/Remove Snap-in**.
 4. Under Available snap-ins, click **Certificates**, then click **Add**.
 5. Under This snap-in will always manage certificates for, click **Computer account**, then click **Next**.
 6. Click **Local computer**, then click **Finish**, then click **OK**.
 7. In the console tree, double-click **Certificates**.
 8. Right-click **Trusted Root Certification Authorities**.
 9. Click **Import** to import the certificates and follow the steps in the Certificate Import Wizard to add the P7B certificate.
-

Chapter 5: Working With Block Pages And Overrides

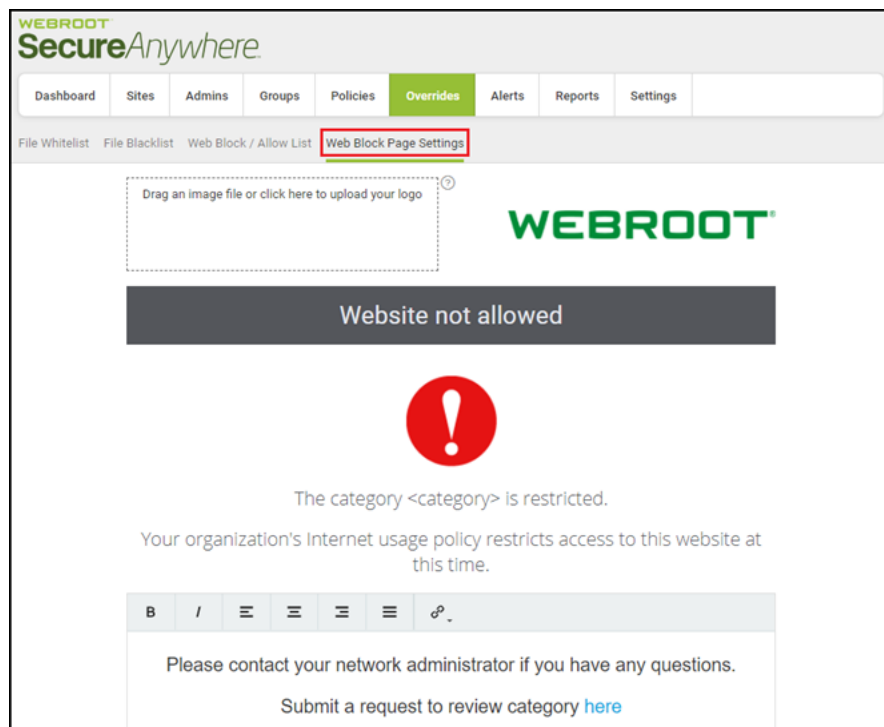
To work with block pages and overrides, see the following topics:

Web Block Page Settings	28
Configuring Web Overrides	29
Web Overrides	29
Filtering Exceptions – Web Block / Allow List	29
Adding Exceptions	29
Viewing Exceptions	30
Creating DNS Protection Web Overrides	31

Web Block Page Settings

The Block Page can be customized for each console. This allows the user to be provided with more information alongside the standard Webroot messaging to include a logo as well as custom text.

- The image size is restricted to 1 MB. Supported formats are PNG, GIF or JPG with a maximum height of 50 pixels.
- The Content field can be used to add support telephone numbers, links to ticketing systems, and communication guiding the user as to the intent of the page.



Configuring Web Overrides

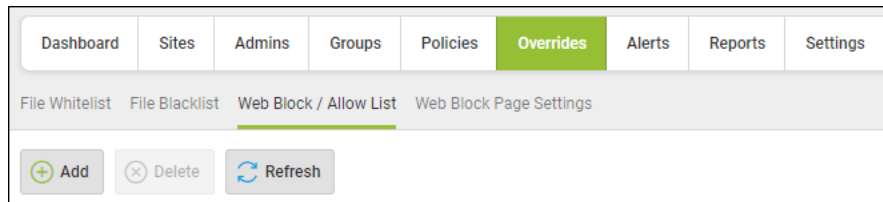
Web Overrides

Web Overrides and the Block Page configuration are managed under the Overrides tab. These are broken out into two subtabs.

- Web Block / Allow List
- Web Block Page Settings

Filtering Exceptions – Web Block / Allow List

If you need to make specific exceptions to the Policies, this can be managed domain by domain under the Overrides tab, Web Block / Allow List. These entries override the Policy for the Sites.



Adding Exceptions

When you click the **Add Button**, you can either do either of the following in the Scope area on the Create New Entry window:

- Select the **Global** radio button to apply the override to all sites
- Select the **Site** radio button and select a specific site from the drop-down menu for a targeted override.

The URL field is where you add the domain that needs to be allowed or blocked. Entries in this field may include a wildcard or can be specific to the domain or subdomain you wish to allow or block.

For example, if you wanted to block `www.webroot.com` and `vpn.webroot.com`, each would need to be entered as separate overrides. Alternately, both would be encompassed by `*.webroot.com`.

Note: Site Overrides take precedence over GSM Global Web Overrides.

Create New Entry

Domain(s) ?

goodwebsite.com, productivity.net...

Wild cards are supported within domain(e.g. *.subdomain.com)0 / 50 domain(s) entered

Scope ?

☐ Global

☒ Site

Select a site...

Policy ?

☒ Associated Policy

Select policy...

Block / Allow ?

☐ Block

☐ Allow

☒ Block Malicious URLs ?

Create

Cancel

For more information, see [Creating Web Overrides](#) in the [Global Site Manager Admin Guide](#).

Viewing Exceptions

Exceptions are visible based on the drop-down menu. Select Overrides to View:

- To see Overrides for all Sites, select **Global** radio button.
 - To see Overrides for a specific site, select the **Site** radio button and select the site from the drop-down menu.
-

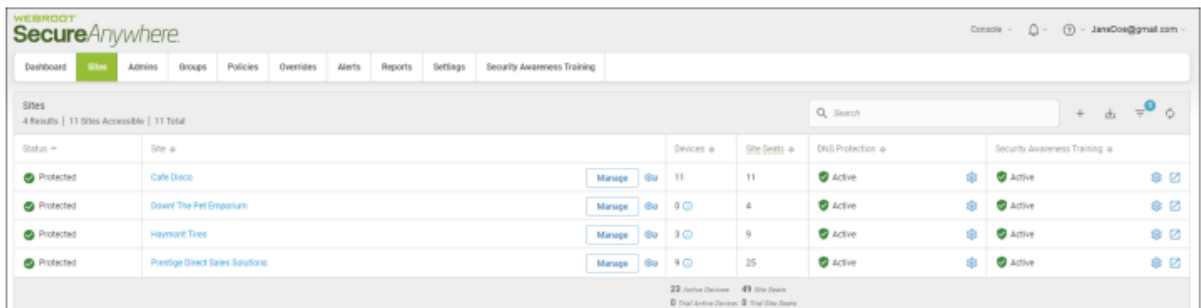
Creating DNS Protection Web Overrides

Follow this procedure to create a web override that will override the default classifications of the default Web Threat Shield Protection functionality.

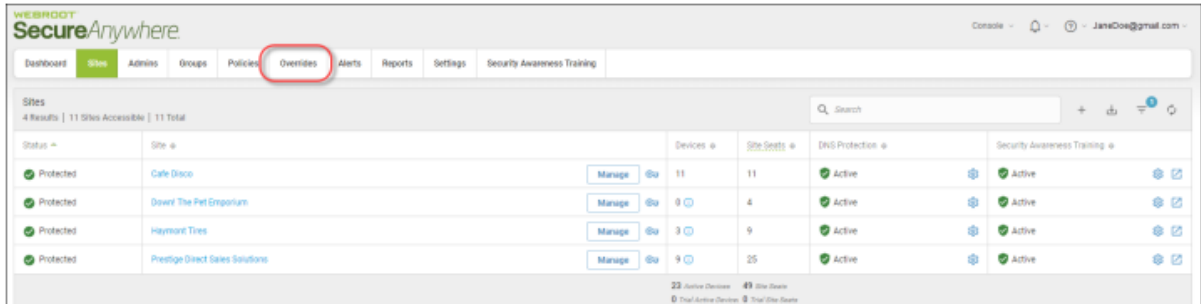
To create a web override:

1. Log in to the [management console](#).

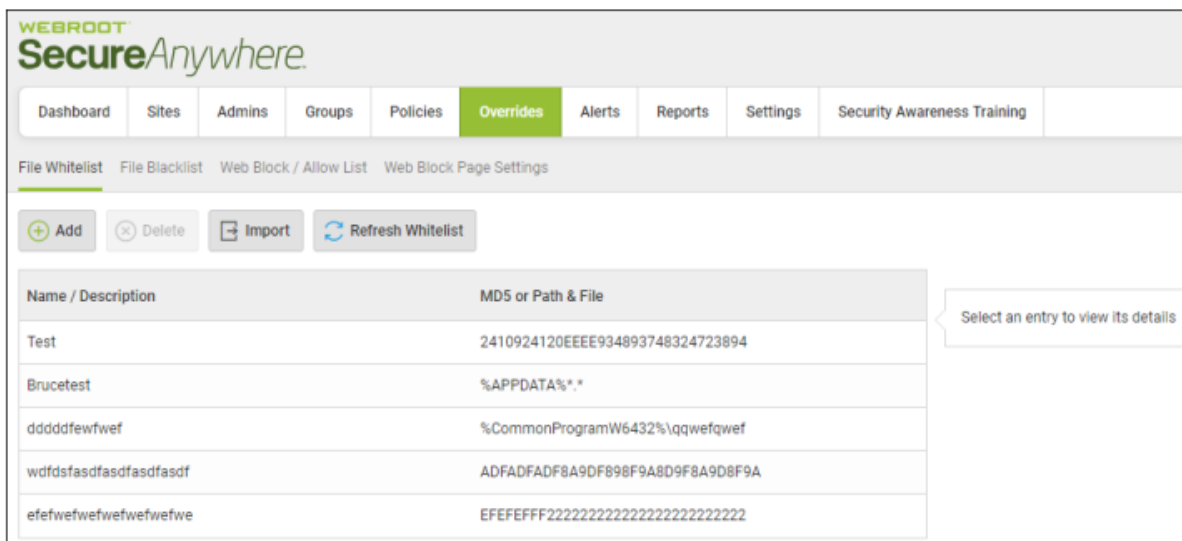
The management console displays, with the Sites tab active.



2. Click the **Overrides** tab.



The Overrides tab displays, with the File Whitelist tab active.

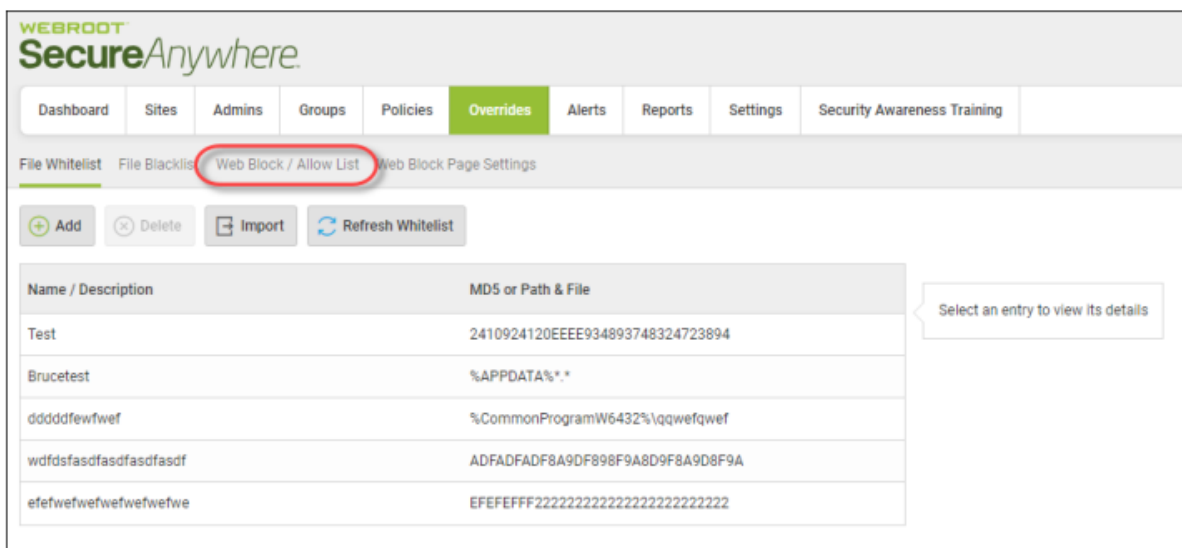


The screenshot shows the Webroot SecureAnywhere interface. The top navigation bar includes Dashboard, Sites, Admins, Groups, Policies, Overrides (highlighted), Alerts, Reports, Settings, and Security Awareness Training. Below this, the sub-navigation bar shows File Whitelist (highlighted), File Blacklist, Web Block / Allow List, and Web Block Page Settings. The main content area features buttons for Add, Delete, Import, and Refresh Whitelist. A table displays the following data:

Name / Description	MD5 or Path & File
Test	2410924120EEEE934893748324723894
Brucetest	%APPDATA%*. *
dddddfewfwe	%CommonProgramW6432%\qqwefqwe
wdfdsfasdfasdfasdf	ADFADFADF8A9DF898F9A8D9F8A9D8F9A
efefwefwefwefwefwe	EFEFEFFF222222222222222222222222

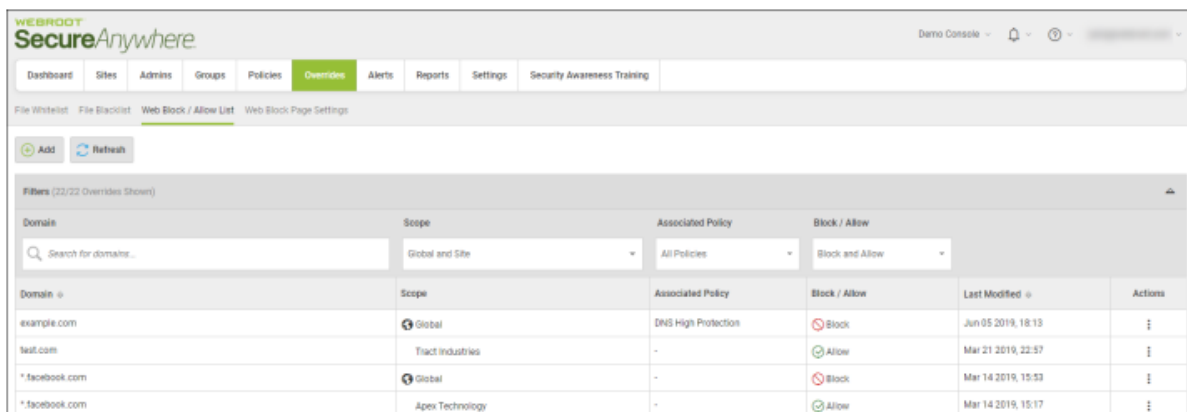
A callout box on the right says "Select an entry to view its details".

- Click the **Web Block / Allow List** tab.

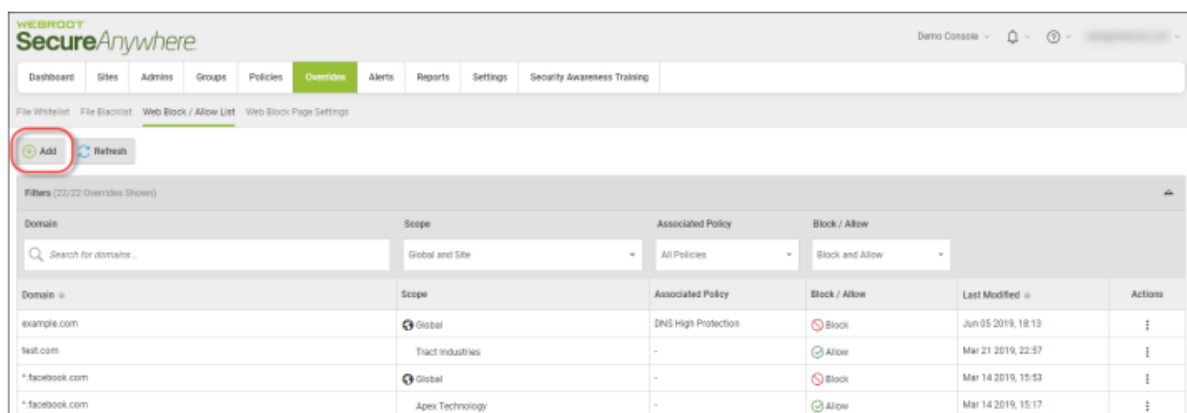


The screenshot shows the same Webroot SecureAnywhere interface, but the 'Web Block / Allow List' tab is now selected and highlighted with a red circle. The table content remains the same as in the previous screenshot.

The Web Block / Allow List tab displays.



4. Click the **Add** button.



The Create New Entry window displays.

Create New Entry

Domain(s) ?

goodwebsite.com, productivity.net...

Wild cards are supported within domain(e.g. *.subdomain.com) 0 / 50 domain(s) entered

Scope ?

☐ Global ☒ Site

Select a site...

Policy ?

☒ Associated Policy

Select policy...

Block / Allow ?

☐ Block ☐ Allow

☒ Block Malicious URLs ?

Create Cancel

5. In the Domains field, enter the URL that you want to add as a web override.

Note: When you are entering the URL, you do not have to enter any protocols such as *www*, *http*, or *https*. Also, wildcards are now supported in this field.

6. In the Scope area, select one of the following radio buttons to determine at which site you create the override:
 - **Global** — Makes this entry available for all sites that have the Include Global Overrides checkbox selected in their site settings. For more information, see [Editing Site Settings](#).

- **Site** — Applies the web override to the specific site that you have selected.
7. In the Policy area, select the **Associated Policy** checkbox to display the Policy drop-down menu, from which you can select any of the following DNS Protection policies:
 - DNS High Protection
 - DNS Medium Protection
 8. In the Block/Allow area, select one of the following radio buttons:
 - **Allow**
 - **Block**
 9. Do either of the following:
 - Select the **Block Malicious URLs** checkbox to block URLs that are detected as malicious, regardless of the allow setting.
 - Do not select the **Block Malicious URLs** checkbox.
 10. When you're done, click the **Create** button.

Create New Entry ✕

Domain(s) ?

goodwebsite.com, productivity.net...

Wild cards are supported within domain(e.g. *.subdomain.com) 0 / 50 domain(s) entered

Scope ?

☐ Global ☐ Site

Policy ?

☐ Associated Policy

Block / Allow ?

☐ Block ☐ Allow

☒ Block Malicious URLs ?

Create Cancel

Chapter 6: Working With Reports

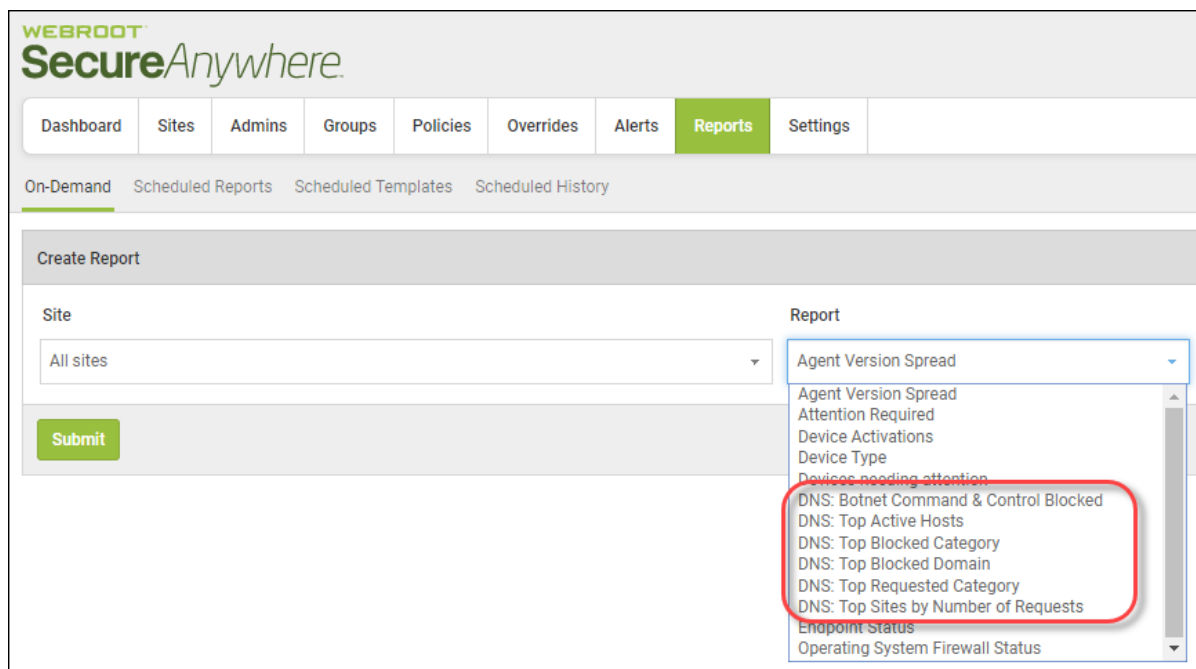
To work with reports, see the following topics:

DNS Protection Reports Overview	38
Generating DNS Protection Reports	39
Exporting CSV Files	45

DNS Protection Reports Overview

All of our reports are designed to improve visibility of internet usage. There are six on-demand and scheduled reports available under the Reports tab to help identify the different characteristics of the internet traffic for a Site. They can identify domains and categories that are blocked, as well as illustrate the protection provided.

Note: For more information about reporting, see the [Global Site Manager Reports Overview](#) in the [GSM Admin Guide](#).



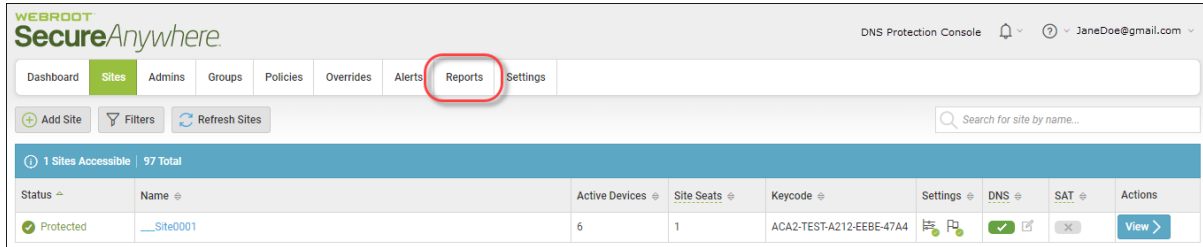
The screenshot shows the Webroot SecureAnywhere interface. At the top, there's a navigation bar with tabs: Dashboard, Sites, Admins, Groups, Policies, Overrides, Alerts, Reports (highlighted), and Settings. Below this is a sub-navigation bar with links: On-Demand, Scheduled Reports, Scheduled Templates, and Scheduled History. The main section is titled 'Create Report'. It has two columns. The left column is labeled 'Site' and contains a dropdown menu with 'All sites' selected. Below it is a green 'Submit' button. The right column is labeled 'Report' and contains a dropdown menu. The dropdown menu is open, showing a list of report types: Agent Version Spread, Agent Version Spread, Attention Required, Device Activations, Device Type, Devices needing attention, DNS: Botnet Command & Control Blocked, DNS: Top Active Hosts, DNS: Top Blocked Category, DNS: Top Blocked Domain, DNS: Top Requested Category, DNS: Top Sites by Number of Requests, Endpoint Status, and Operating System Firewall Status. A red rectangle highlights the DNS-related reports in the list.

Generating DNS Protection Reports

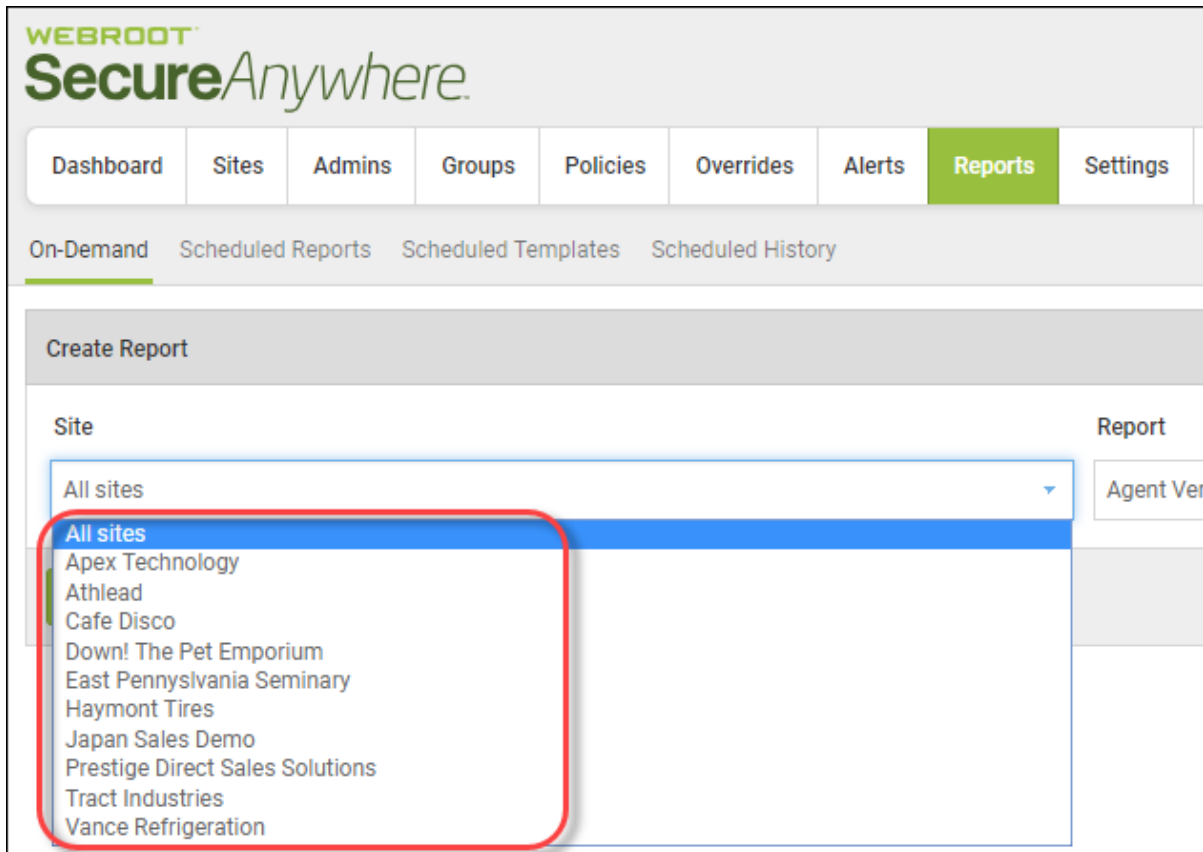
To run a report and display the information on your screen while you're in the console, follow this procedure to generate an on-demand report.

To generate a DNS Protection report:

1. [Log in](#) and click the **Reports** tab.



2. From the Sites drop-down menu, select the site for which you want to generate the report.



3. From the Report drop-down menu, select one of the following reports:
 - **DNS: Botnet Command & Control Blocked** – Shows domains that have been blocked by DNS Protection and are categorized as Command and Control. This report highlights malicious activity that has been blocked by DNS Protection. Results can be grouped by Site, with drill down capabilities.
 - **DNS: Active Hosts** – Improves visibility of internet usage and displays complete browsing history of devices within a Site, including requested and block counts by device, username, domains, category, block reason, etc.

Data can be displayed up to 90 days. It is an equivalent to raw log data, empowering partners and customers to slice and dice data from this report to build custom reporting. You can drill into more information to see which Sites were requested by each hostname and device. This report is available as an on-demand report as well as an export.

- **DNS: Top Blocked Category** – Includes an overview that shows blocked categories for all of your customers during the selected time frame. You can filter by customer, and drill into specific categories to see blocked URLs and the devices and users accessing it.

Security risks are conveniently grouped together for further analysis, with the ability to view security risk as a percentage of total traffic – giving you better visibility into and control over network usage on a Site-by-Site basis, or in aggregate.

- **DNS: Top Blocked Domain** – Similar to the Top Blocked Categories, this report improves visibility of internet usage by detailing the top 12 domains that were blocked by Site. Drilling into the report provides useful insights about Sites that have attempted to visit the domain, days and times of the requests, and device information where available. The agent must be installed for this level of insight.
- **DNS: Top Requested Category** – Provides insight into all domains begin requested, organized by category. Simply click on the category of interest to see what domains your users are requesting.

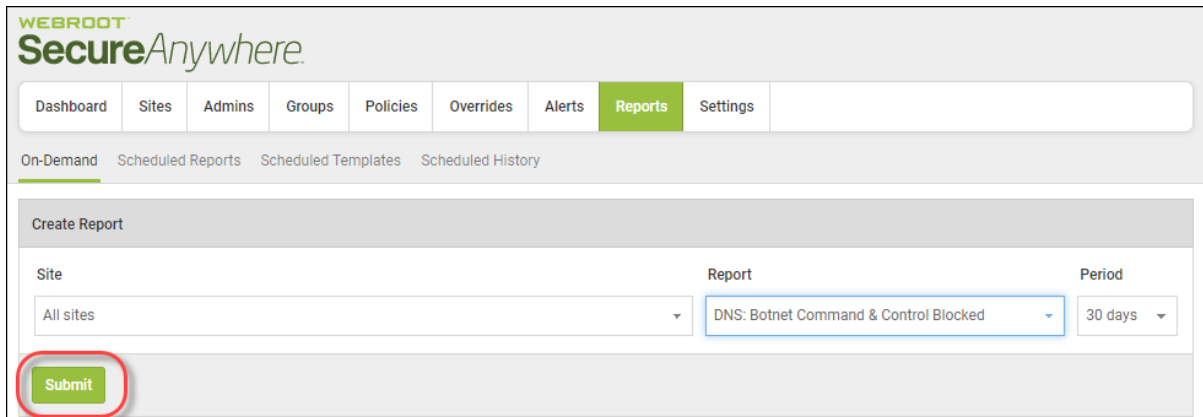
This provides an additional level of granularity to help MSPs find concerning cloud services by type. Personal storage, for example, might pose a greater interest for validating data loss Policies. You can focus your analysis by clicking the legend to the right, which will remove those categories from the analysis. You can also drill into the information by clicking the pie chart and the Sites to see which specific domains have been requested.

- **DNS: Top Sites by Number of Requests** – Designed for implementations of DNS Protection using the network setting, this report can be used to approximate traffic, billing usage approximation, etc. Admins can click into the Site they are interested in examining to see number of requests by day. You can drill into the detail by clicking a specific day to see which categories were requested how many times on that day.

4. From the Period drop-down menu, select one of the corresponding periods:

- Last 24 hours
- 2 days
- 3 days
- 14 days
- 30 days - This is the default.
- 60 days
- 90 days

5. When you're done, click the **Submit** button.



WEBROOT[™]
SecureAnywhere.

Dashboard Sites Admins Groups Policies Overrides Alerts **Reports** Settings

On-Demand Scheduled Reports Scheduled Templates Scheduled History

Create Report

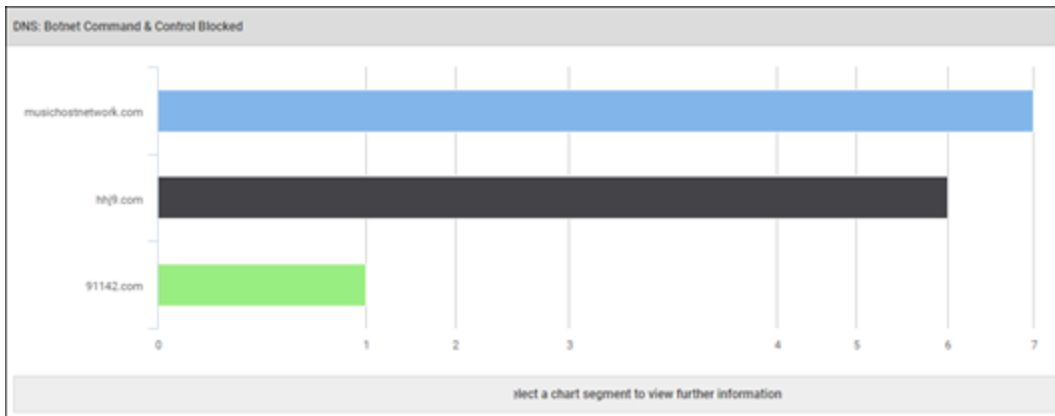
Site Report Period

All sites DNS: Botnet Command & Control Blocked 30 days

Submit

The system displays the report in the console; report formats are predetermined, and typically clicking on results of the report allows you to drill down for more information.

6. To display additional information about the report, do any of the following:
 - **DNS: Botnet Command & Control Blocked** – Select a chart segment to view further information.



- **DNS: Top Active Hosts** – Click the Requested or Blocked column to view further detail.

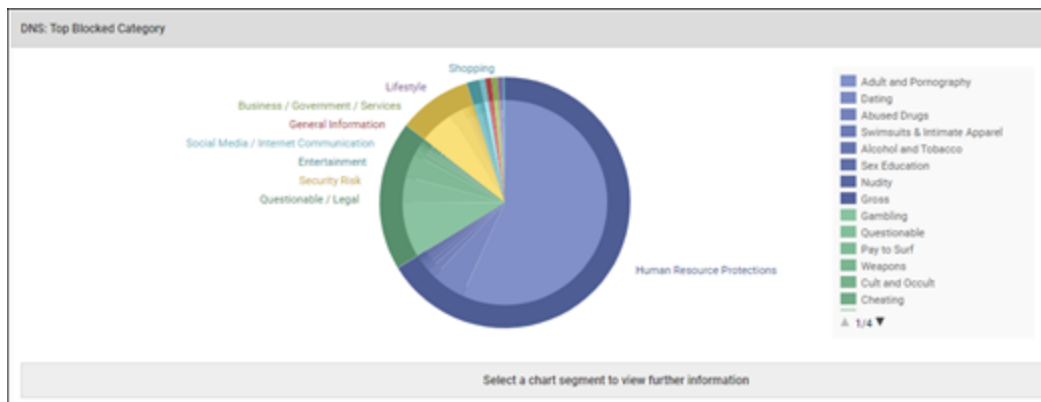
Top Active Hosts

Export to CSV

Hostname	Username	Site	Requested	Blocked
DESKTOP-4004VAQ	Webroot	DNSTestSDQATeam	View 43,938	View 2,088
QATST-5609L-SDG	Webroot	DNSTestSDQATeam	View 10,160	View 718
IP-AC100163	Webroot	___Site0001	View 3,572	View 54
IP-AC100033	Webroot	___Site0001	View 3,491	View 24
IP-0A600151	Webroot	___Site0001	View 2,023	View 3
IP-0A600155	Webroot	___Site0001	View 1,460	View 3
IP-0A6001CC	Webroot	___Site0001	View 565	View 0

Click the Requested or Blocked column to view further detail

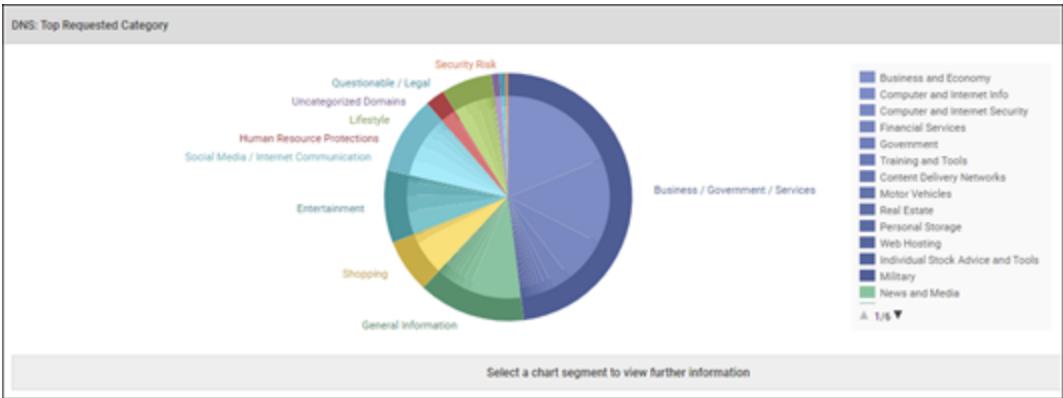
- **DNS: Top Blocked Category** – Select a chart segment to view further information.



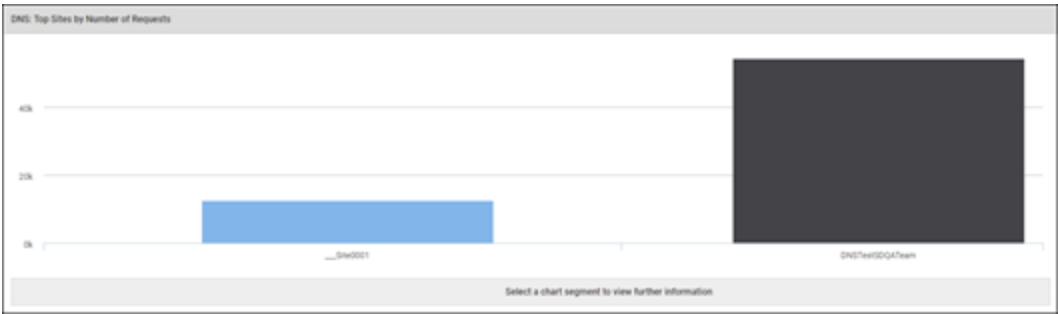
- **DNS: Top Blocked Domain** – Select a chart segment to view further information.



- **DNS: Top Requested Category** – Select a chart segment to view further information.



- **DNS: Top Sites by Number of Requests** – Select a chart segment to view further information.



Exporting CSV Files

Currently you can export CSV files of report data for the DNS Top Active Hosts report. Additionally, you can export CSV files of drilldown data for Blocked Domains within the report.

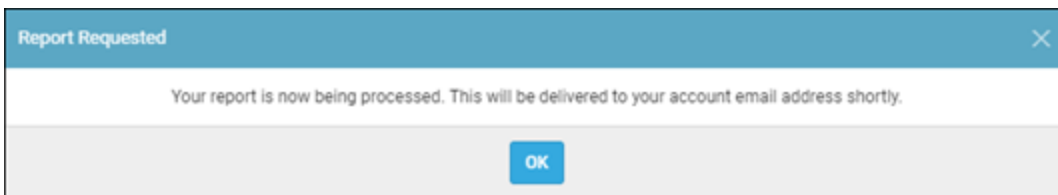
To export and email a CSV file:

1. [Log in](#) and run the DNS Top Active Hosts report for your desired site or sites.
2. Click the **Export to CSV** button.



Requested	Blocked
View 43,929	View 2,088
View 10,160	View 718
View 3,570	View 54
View 3,488	View 24
View 2,017	View 3
View 1,458	View 3
View 565	View 8

The Report Requested message displays, indicating that the file is being sent to the email address you used to log in to your console.



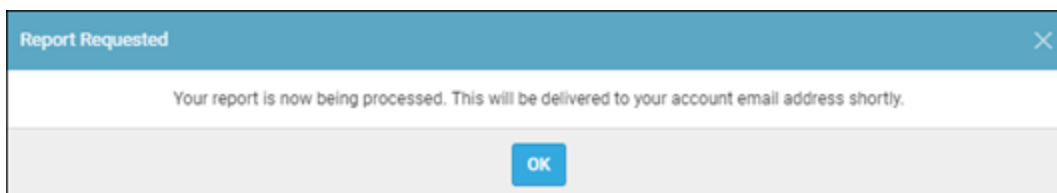
3. As needed, in the Blocked column, click the **View** link next to any hostname that you want to display a drill-down for.

Requested		Blocked	
View	43,929	View	2,088
View	10,160	View	718
View	3,570	View	54
View	3,488	View	24
View	2,017	View	3
View	1,458	View	3
View	565	View	8

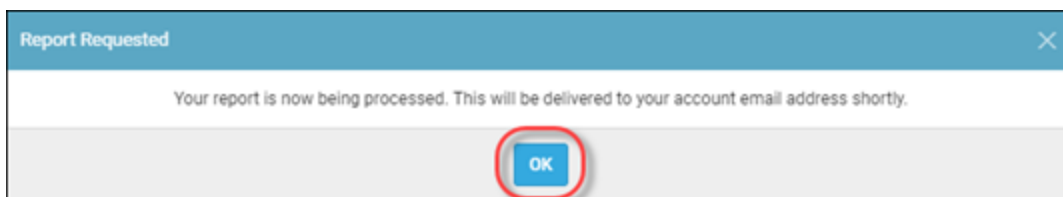
- Click the **Export to CSV** button for the drill-down information.

DESKTOP-4G04VAQ						Export to CSV
Date	Hostname	Username	URL	Category	Block Reason	
Apr 9 2018, 14:27	DESKTOP-4G04VAQ	Webroot	www.eharmony.com	Dating	By Category	
Apr 6 2018, 23:59	DESKTOP-4G04VAQ	Webroot	adam4adam.com	Adult and Pornography	By Category	
Apr 6 2018, 23:59	DESKTOP-4G04VAQ	Webroot	jra.go.jp	Gambling	By Category	
Apr 6 2018, 23:59	DESKTOP-4G04VAQ	Webroot	jra.go.jp	Gambling	By Category	
Apr 6 2018, 23:58	DESKTOP-4G04VAQ	Webroot	tukif.com	Adult and Pornography	By Category	
Apr 6 2018, 23:58	DESKTOP-4G04VAQ	Webroot	research-panel.jp	Pay to Surf	By Category	

The Report Requested message displays, indicating that the file is being sent to the email address you used to log in to your console.



5. Click the **OK** button and check your inbox.



Chapter 7: Configuring Firewalls

For information about configuring firewalls, see the following topic:

Configuring Firewalls	49
------------------------------------	-----------

Configuring Firewalls

Webroot DNS Protection requires the following IP addresses and ports to be allowed outbound on your firewall:

Network DNS Protection (port 53 – TCP and UDP):

- 45.54.55.54
- 45.54.55.55

DNS Protection Agent (Port 443 and 5222 – TCP)

- 35.244.252.192
-

Chapter 8: Accessing Usage Data

For information about accessing usage data for DNS Protection, see the following topic:

About Accessing Usage Data	51
---	-----------

About Accessing Usage Data

With the usage console that includes detailed breakdowns of your Webroot products and services, you can now access your usage data for Security Awareness Training.

For more information, see [Accessing Usage Data](#) in the [Working With Settings](#) section of the [GSM Admin Guide](#).

Chapter 9: DNS Protection Support

For information about support, see the following topic:

Accessing Technical Support	53
--	-----------

Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- [Look for the answer in our knowledgebase.](#)
 - [Look for the answer in our online documentation.](#)
 - [Enter a help ticket .](#)
 - [Connect to the Webroot Online Business Forum.](#)
-

Chapter 10: Appendix

To get started using the appendix, see the following topics:

Domain Groups and Categories Overview	55
Webroot Domain Groups	55
Security Risk Domain Group	56
Human Resources Protections Domain Group	58
Questionable and Legal Domain Group	61
Social Media and Internet Communication Domain Group	64
Shopping Domain Group	67
Entertainment Domain Group	68
Lifestyle Domain Group	70
Business / Government Services Domain Group	72
General Information Domain Group	76
Uncategorized Domain Group	79

Domain Groups and Categories Overview

Webroot® DNS Protection provides granular control over internet access through website categorization across 10 high-level, logical domain groups and 80 domain categories.

This comprehensive list details domain groups and categories, and includes brief explanations and examples of each category. Use it to finely tune internet access policies for users, user groups, IP addresses, and WiFi access points.

Webroot Domain Groups

There are nine active domain groups, with a tenth that acts as a catch-all for dead sites or sites Webroot has not yet categorized.

The domain groups are:

- [Security Risk](#)
 - [Human Resource Protections](#)
 - [Questionable/Legal](#)
 - [Social Media/Internet Communication](#)
 - [Shopping](#)
 - [Entertainment](#)
 - [Lifestyle](#)
 - [Business/Government/Services](#)
 - [General Information](#)
 - [Uncategorized](#)
-

Security Risk Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Keyloggers and Monitoring	<p>Downloads and discussion of software agents that track a user's keystrokes or monitor their web surfing habits.</p> <p>Examples: keylogger.org and spy-tools-directory.com</p>
Malware Sites	<p>Malicious content including executables, drive-by infection sites, malicious scripts, viruses, Trojans, and code. These sites are typically short-lived, so examples don't last long. Contact us for updated examples.</p> <p>Examples: loveingod.org and 666ccc.com</p>
Phishing and Other Frauds	<p>Phishing pharming and other sites that pose as a reputable site usually to harvest personal information from a user. These sites are typically short-lived so examples don't last long. Contact us for updated examples.</p> <p>Examples: chhetrisamaj.com/dem/bankofamerica/alerts/bofa.sec.html and bancofamerica.online.home.ro/onlineaccess_verification/signonSetup.html</p>

CATEGORY	DESCRIPTION
Proxy Avoidance and Anonymizers	<p>Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering.</p> <p>Examples: anonymous.org and surfen-op-school.com</p>
Spyware and Adware	<p>Spyware or adware sites that provide or promote information gathering or tracking that is unknown to or without the explicit consent of the end user or the organization also unsolicited advertising popups and programs that may be installed on a user's computer. These sites are typically short-lived so examples don't last long. Contact us for updated examples.</p> <p>Examples: allsecuritylinks.com and askyaya.com</p>
Bot Nets	<p>URLs or IP addresses which are determined to be part of a Bot network from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contact.</p>
SPAM URLs	<p>URLs contained in SPAM messages.</p>

Human Resources Protections Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Abused Drugs	<p>Discussion or remedies for illegal, illicit or abused drugs such as heroin, cocaine, or other street drugs. Includes information on “legal highs”; glue sniffing, misuse of prescription drugs; or abuse of other legal substances.</p> <p>Examples: shroomery.org and passyourdrugtest.com</p>
Adult and Pornography	<p>Sexually explicit material for the purpose of arousing a sexual or prurient interest. Adult products including sex toys, CDs/DVDs, and videos. Online groups including newsgroups, and forums that are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including videoconferencing, escort services, and strip clubs. Sexually explicit art.</p> <p>Examples: playboy.com and union.fr</p>
Dating	<p>Dating websites focused on establishing personal relationships.</p> <p>Examples: dating.com and askmen.com</p>

CATEGORY	DESCRIPTION
Sex Education	<p>Information on reproduction, sexual development, safe sex practices, sexually transmitted diseases, sexuality, birth control, sexual development, tips for better sex as well as products used for sexual enhancement and contraceptives.</p> <p>Examples: sexetc.org and sexandahealthieryou.org</p>
Swimsuits & Intimate Apparel	<p>Swimsuits, intimate apparel or other types of suggestive clothing.</p> <p>Examples: victoriassecret.com and brazilianswimwear.com</p>
Gross	<p>Vomit and other bodily functions, bloody clothing, etc.</p> <p>Examples: ratemyvomit.com, bloody-disgusting.com and bloodshows.com</p>

CATEGORY	DESCRIPTION
Nudity	<p>Nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.</p> <p>Examples: gorodtoms.ru/index-1221486260.php and pornomedia.com/extra/strange/wwbeauty</p>
Alcohol and Tobacco	<p>Sites that provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.</p> <p>Examples: thompsoncigar.com and wineinsiders.com</p>

Questionable and Legal Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Cult and Occult	<p>Methods, means of instruction, or other resources to interpret, affect or influence real events through the use of astrology, spells, curses, magic powers, or supernatural beings. Includes horoscope sites.</p> <p>Examples: horoscopes.com and astronnet.hu</p>
Gambling	<p>Gambling or lottery websites that invite the use of real or virtual money. Information or advice for placing wagers, participating in lotteries, gambling, or running numbers. Virtual casinos and offshore gambling ventures. Sports picks and betting pools. Virtual sports and fantasy leagues that offer large rewards or request significant wagers. Hotel and resort sites that do not enable gambling on the site are categorized in Travel or Local Information.</p> <p>Examples: gambling.com and zjlottery.com</p>
Marijuana	<p>Marijuana use, cultivation, history, culture, legal issues.</p> <p>Examples: howtogrowmarijuana.com and cannaweed.com</p>

CATEGORY	DESCRIPTION
Hacking	<p>Illegal or questionable access to or the use of communications equipment/ software. Development and distribution of programs that may allow compromise of networks and systems. Avoidance of licensing and fees for computer programs and other systems.</p> <p>Examples: darkwarez.pl and hackforums.net</p>
Weapons	<p>Sales reviews or descriptions of weapons such as guns knives or martial arts devices or provide information on their use accessories or other modifications.</p> <p>Examples: browning.com and e-gunparts.com</p>
Pay to Surf	<p>Sites that pay users in the form of cash or prizes for clicking on or reading specific links email or web pages.</p> <p>Examples: cashcrate.com and inboxdollars.com</p>
Questionable	<p>Tasteless humor “get rich quick” sites and sites that manipulate the browser user experience or client in some unusual unexpected or suspicious manner.</p> <p>Examples: governmentgrant.com and collegehumor.com</p>
Hate and Racism	<p>Sites that support content and languages or hate crime and racism such as Nazi, neo-Nazi, Ku Klux Klan, etc.</p> <p>Examples: nazi-lauck-nsdapao.com, americannaziparty.com and kkk.com</p>

CATEGORY	DESCRIPTION
Violence	<p>Sites that advocate violence depictions and methods including game/comic violence and suicide.</p> <p>Examples: sfdt.com, happytreefriends.com and torturegame.org</p>
Cheating	<p>Sites that support cheating and contain such materials, including free essays, exam copies, plagiarism, etc.</p> <p>Examples: wowessays.com, ffreeessays.cc and 123helpme.com</p>
Illegal	<p>Criminal activity, how not to get caught, copyright and intellectual property violations, etc. Examples: newid.com, newidcards.com and kidneykidney.com</p>
Abortion	<p>Abortion-related topics either pro-life or pro-choice.</p> <p>Examples: abortionfacts.com and prochoiceamerica.org</p>

Social Media and Internet Communication Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Social Networking	<p>These are social networking sites that have user communities where users interact, post messages, pictures, and otherwise communicate. These sites were formerly part of Personal Sites and Blogs but have been removed to this new category to provide differentiation and more granular policy.</p> <p>Examples: facebook.com and twitter.com</p>
Personal Sites and Blogs	<p>Personal websites posted by individuals or groups as well as blogs.</p> <p>Examples: blogger.com and bloghouse.net</p>
Online Greeting Cards	<p>Online greeting card sites.</p> <p>Examples: 123greetings.com and greeting-cards.com</p>
Search Engines	<p>Search interfaces using key words or phrases. Returned results may include text, websites, images, videos, and files.</p> <p>Examples: google.com and sogou.com</p>

CATEGORY	DESCRIPTION
Internet Portals	<p>Websites that aggregate a broader set of internet content and topics, and which typically serve as the starting point for an end user.</p> <p>Examples: yahoo.com and qq.com</p>
Web Advertisements	<p>Advertisements media content and banners.</p> <p>Examples: casalemedia.com and justwebads.com</p>
Web Based Email	<p>Sites offering web-based email and email clients.</p> <p>Examples: google.com/mail and foxmail.com</p>
Internet Communications	<p>Internet telephony, messaging, VoIP services, WiFi, and related businesses.</p> <p>Examples: skype.com and evaphone.com</p>
Dynamically Generated Content	<p>Domains that generate content dynamically based on arguments to their URL or other information (like geo-location) on the incoming web request.</p>

CATEGORY	DESCRIPTION
Parked Domains	<p>Parked domains are URLs which host limited content or click-through ads which may generate revenue for the hosting entities but generally do not contain content useful to the end user. Many parked sites host malware.</p> <p>Examples: 000.com and buythisdomain.com</p>
Private IP Addresses and URLs	<p>IP addresses reserved by organizations that distribute IP addresses for private networks and a URL assigned to a private domain.</p>

Shopping Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Auctions	<p>Sites that support the offering and purchasing of goods between individuals as their main purpose. Does not include classified advertisements.</p> <p>Examples: ebay.com and trademe.co.nz</p>
Shopping	<p>Department stores, retail stores, company catalogs and other sites that allow online consumer or business shopping and the purchase of goods and services.</p> <p>Examples: amazon.com andgroupon.com</p>
Shareware and Freeware	<p>Software, screensavers, icons, wallpapers, utilities, ringtones. Includes downloads that request a donation and open source projects.</p> <p>Examples: download.com and sourceforge.net</p>

Entertainment Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Entertainment and Arts	<p>Motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. Performing arts (theater, vaudeville, opera, symphonies, etc); museums, galleries, libraries, artist sites (sculpture, photography, etc.)</p> <p>Examples: eonline.com and etonline.com</p>
Streaming Media	<p>Sales, delivery, or streaming of audio or video content, including sites that provide downloads for such viewers.</p> <p>Examples: ustream.tv and warpradio.com</p>
Peer to Peer	<p>Peer-to-peer clients and access. Includes torrents, music download programs.</p> <p>Examples: mininova.org and bitcomet.com</p>

CATEGORY	DESCRIPTION
Games	<p>Game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. Also includes sites dedicated to selling board games as well as journals and magazines dedicated to game playing. Includes sites that support or host online sweepstakes and giveaways. Includes fantasy sports sites that also host games or game-playing.</p> <p>Examples: duowan.com and games.espn.com</p>
Music	<p>Music sales, distribution, streaming, information on musical groups and performances, lyrics, and the music business.</p> <p>Examples: itunes.com and bandcamp.com</p>

Lifestyle Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Travel	<p>Airlines and flight booking agencies. Travel planning, reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. Car Rentals.</p> <p>Examples: cheapflights.com and expedia.com</p>
Home and Garden	<p>Home issues and products, including maintenance, home safety, decor, cooking, gardening, home electronics, design, etc.</p> <p>Examples: homedepot.com and waysidegardens.com</p>
Religion	<p>Conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship.</p> <p>Examples: therocksandiego.org and biblesociety.ca</p>
Hunting and Fishing	<p>Sport hunting, gun clubs, and fishing.</p> <p>Examples: fishingworks.com and wildlifelicense.com</p>

CATEGORY	DESCRIPTION
Society	<p>A variety of topics, groups, and associations relevant to the general populace, broad issues that impact a variety of people, including safety, children, societies, and philanthropic groups.</p> <p>Examples: dar.org and supermama.lt</p>
Sports	<p>Team or conference websites, international, national, college, professional scores and schedules, sports-related online magazines or newsletters.</p> <p>Examples: nba.com and schoenen-dunk.de</p>
Fashion and Beauty	<p>Fashion or glamor sites, magazines, beauty, clothes, cosmetics, style.</p> <p>Examples: beauty.ivillage.com and genejuarez.com</p>
Recreation and Hobbies	<p>Information, associations, forums, and publications on recreational pastimes such as collecting kit airplanes, outdoor activities (hiking, camping, climbing etc.); specific arts, craft, or techniques; animal and pet-related information, or techniques; animal and pet-related information, training, shows, and humane societies.</p> <p>Examples: greatdogsite.com and craftster.org</p>

Business / Government Services Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Real Estate	<p>Information on renting, buying or selling real estate or properties. Tips on buying or selling a home. Real estate agents Rental or relocation services, Rental or relocation services and property improvement.</p> <p>Examples: prudentialproperties.com and realtor.com</p>
Computer and Internet Security	<p>Computer/Internet security, security discussion groups.</p> <p>Examples: siteadvisor.com and kaspersky.com</p>
Financial Services	<p>Banking services and other types of financial information, such as loans, accountancy, actuaries, banks, mortgages, and general insurance companies. Does not include sites that offer market information, brokerage or trading services.</p> <p>Examples: firstpremierbankcards.com and bankofamerica.com</p>

CATEGORY	DESCRIPTION
Business and Economy	<p>Business firms, corporate websites, business information, economics, marketing, management, and entrepreneurship. Examples: boeing.com and honda.com</p>
Computer and Internet Info	<p>General computer and Internet sites, technical information. SaaS sites and other URLs that deliver internet services.</p> <p>Examples: netcraft.com, ranking.com and system.netsuite.com</p>
Military	<p>Information on military branches, armed services, and military history. Examples: navy.mil and goarmy.com</p>
Individual Stock Advice and Tools	<p>Promotion and facilitation of securities trading and management of investment assets. Also includes information on financial investment strategies, quotes, and news.</p> <p>Examples: stockstar.com and morningstar.com</p>
Training and Tools	<p>Distance education and trade schools, online courses, vocational training, software training, skills training.</p> <p>Examples: trainingtools.com and guidetocareereducation.com</p>

CATEGORY	DESCRIPTION
Personal Storage	<p>Online storage and posting of files music pictures and other data.</p> <p>Examples: photobucket.com and qookfile.co.kr</p>
Government	<p>Information on government, government agencies and government services such as taxation, public, and emergency services. Also includes sites that discuss or explain laws of various governmental entities. Includes local, county, state, and national government sites.</p> <p>Examples: nasa.gov and premier-ministre.gouv.fr</p>
Content Delivery Networks	<p>Delivery of content and data for third parties, including ads, media, files, images, and video.</p> <p>Examples: akamaitech.net and edgestream.com</p>

CATEGORY	DESCRIPTION
Motor Vehicles	<p>Car reviews, vehicle purchasing or sales tips, parts catalogs Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs Journals and magazines on vehicle modifications.</p> <p>Examples: hotautoweb.com and getmyvolt.com</p>
Web Hosting	<p>Free or paid hosting services for web pages and information concerning their development, publication, and promotion.</p> <p>Examples: siteground.com and bluehost.com</p>

General Information Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Legal	<p>Legal websites, law firms, discussions and analysis of legal issues.</p> <p>Examples: free-law-library.com and doanlaw.com</p>
Local Information	<p>City guides and tourist information, including restaurants, area/regional information, and local points of interest.</p> <p>Examples: downtownlittlerock.com and sandiegorestaurants.com</p>
Job Search	<p>Assistance in finding employment, and tools for locating prospective employers, or employers looking for employees. Also career search and career placement from schools.</p> <p>Examples: linkedin.com/jobs and 51job.com</p>

CATEGORY	DESCRIPTION
Translation	<p>These are URL and language translation sites that allow users to see pages in other languages. These sites can also allow users to circumvent filtering as the target page's content is presented within the context of the translator's URL. These sites were formerly part of Proxy Avoidance and Anonymizers, but have been moved to this new category to provide clearer differentiation and more granular policy.</p> <p>Examples: translate.google.com and microsofttranslator.com</p>
Reference and Research	<p>Personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogues, genealogy, and scientific information.</p> <p>Examples: reference.com and wikipedia.org</p>
Philosophy and Political Advocacy	<p>Politics, philosophy, discussions, promotion of a particular viewpoint or stance in order to further a cause.</p> <p>Examples: stopthesewars.org and climatecrisis.net</p>
Educational Institutions	<p>Pre-school, elementary, secondary, high school, college, university, and vocational school, and other educational content and information, including enrollment, tuition, and syllabus.</p> <p>Examples: mit.edu and carlsbadusd.k12.ca.us</p>

CATEGORY	DESCRIPTION
Kids	<p>Sites designed specifically for children and teenagers.</p> <p>Examples: disney.go.com and kids.yahoo.com</p>
News and Media	<p>Current events or contemporary issues of the day. Also includes radio stations and magazines, newspapers online, headline news sites, newswire services, and personalized news services, and weather sites.</p> <p>Examples: abcnews.go.com and newsoftheworld.co.uk</p>
Health and Medicine	<p>General health, fitness, well-being, including traditional and non-traditional methods and topics. Medical information on ailments, various conditions, dentistry, psychiatry, optometry, and other specialties. Hospitals and doctor offices. Medical insurance. Cosmetic surgery.</p> <p>Examples: webmd.com and kindredsandiego.com</p>
Image and Video Search	<p>Photo and image searches, online photo albums/digital photo exchange, image Hosting.</p> <p>Examples: images.google.fr and gettyimages.com</p>

Uncategorized Domain Group

This domain group is made up of the following categories.

CATEGORY	DESCRIPTION
Uncategorized	Domains not yet categorized by Webroot.

Index

A

- about
 - servers 5
 - VPN 18
 - VPNs 18
 - workstations 5
- accessing technical support 53
- adding groups 11
- advanced group management 14
- agent
 - deploying 10
 - installing 10
 - unsinstalling 19

C

- certificates, installing 26
- Cisco AnyConnect 18
- configuring
 - firewalls 49
 - local DNS servers 24
 - ports 49
 - sites 6
 - TCP 49
 - UDP 49
 - web overrides 29
- creating
 - DNS Protection overrides 31
- CSV files, exporting 45

D

- deploying the agent 10
- DNS protection
 - creating overrides 31
 - overview 2
 - purchasing 3
 - reports overview 38
 - setting up 5
 - trialing 3

E

exporting CSV files 45

F

firewalls, configuring 49
Fortinet VPN 18

G

generating reports 39
group management, advanced 14
groups
 adding 11
 managing through DNS 11

I

installing certificates 26
installing the agent 10

L

local DNS servers, configuring 24

M

managing DNS through groups 11
moving systems between groups 15

N

network DNS resolution, testing 23
network settings, updating 22

O

overview
 DNS protection 2
 reports 38

P

ports, configuring 49
PulseSecure VPN 18

purchasing DNS protection 3
Pure VPN 18

R

reports
 generating 39
 overview 38

S

Safer VPN 18
servers, about 5
setting up
 DNS Protection 5
sites, configuring 6
SonicWall Mobile Connect 18
SonicWall NetExtender VPN 18
systems, moving between groups 15

T

TCP, configuring 49
technical support, accessing 53
testing network DNS resolution 23
trailing DNS protection 3

U

UDP, configuring 49
uninstalling, agent 19
updating network settings 22

V

VPN
 Cisco AnyConnect 18
 Fortinet 18
 PulseSecure 18
 Pure VPN 18
 Safer VPN 18
 SonicWall Mobile Connect 18
 SonicWall NetExtender 18
 WatchGuard 18
VPNs, about 18

W

WatchGuard VPN 18

web overrides, configuring 29

workstations, about 5