Contents

Overview .................................................................................................................................................. 3
Trialing or Purchasing DNS Protection ................................................................................................. 3
Setting Up DNS Protection ..................................................................................................................... 4
Configuring the Web Console .................................................................................................................. 4
  Defining Policies .................................................................................................................................. 4
  Web Overrides ...................................................................................................................................... 5
Web Block / Allow List ............................................................................................................................... 5
Web Block Page Settings .......................................................................................................................... 6
Configuring Sites ..................................................................................................................................... 6
Default DNS Policy ................................................................................................................................ 7
Network Settings ..................................................................................................................................... 7
Agent Bypass List (Intranet) .................................................................................................................... 8
Deploying the Agent ................................................................................................................................. 8
  Managing DNS through Groups ........................................................................................................... 9
Viewing and Filtering DNS Statuses ........................................................................................................ 11
  Displaying Device and IP Information ................................................................................................ 12
Configuring the Network .......................................................................................................................... 13
  Network Settings ................................................................................................................................. 13
  Installing Certificates .......................................................................................................................... 13
Testing Network DNS Resolution (Network Only) .................................................................................. 14
  Configuring Local DNS Servers ........................................................................................................ 15
Reporting .................................................................................................................................................. 16
  Generating DNS Protection Reports .................................................................................................. 16
  Exporting CSV Files ............................................................................................................................ 21
Overview
This document is designed as an admin guide for deploying and using Webroot SecureAnywhere 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 SecureAnywhere DNS Protection Getting Started Guide.

Trialing or Purchasing DNS Protection
If you have not already signed up to trial or purchase 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.
   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.

2. In the DNS Protection row, click the appropriate button:
   ● If you have not yet started your trial, click the Start Free Trial button.
   ● If you have run a trial and would like to upgrade to a full license, click the Upgrade/Renew button.

3. Do either of the following:
   ● If you clicked the Start Free Trial button, the system displays a confirmation message. Click the Confirm button. A Success message displays. If you have any questions regarding your trial, please reach out to your sales representative.
   ● If you clicked the Upgrade/Renew button, you are taken to Webroot’s Easy One-Page Checkout page, where you can purchase licenses, as needed.
Setting Up DNS Protection

DNS Protection has two components: An agent-based solution that allows granular control of DNS independent of the network and a network-based 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.

The configuration process includes three steps:

- Configuring the Web Console
- Deploying the Agent
- Configuring the Network

Configuring the Web Console

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

- **DNS Policies** – The Category configuration for the DNS filters.
- **Web Overrides** – The exception list to enhance the filters and the Block Page customization.
- **Site DNS Settings** – Enabling DNS Protection for the Site.

Defining Policies

Policies for DNS Protection provide the ability to customize which filtering categories are available or blocked. Once configured, these Policies can be linked to Sites, Groups, or systems to implement filtering. Policies for DNS Protection are managed under the DNS subtab under the Policies section of the console.

- To create custom Policies, click the **Add** or **Copy** button. Once a new Policy is created, it can be customized by selecting from the 80 available categories.
Web Overrides

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

- Web Block / Allow List
- Web Block Page Settings

Web Block / Allow List

Under the Web Block/ Allow List tab, custom entries can be added to augment the DNS Protection Policies. This is done by adding the specific domain or subdomain, assigning an action, and then associating it with a single Site or to all Sites by using the GSM Global Overrides selection.

Note that this entry is specific to the domain or subdomain entered. For example, allowing webroot.com does not cover news.webroot.com. In order to control access to news.webroot.com, a separate entry is required. Wild cards are not supported - *.webroot.com will be disregarded as an invalid entry.
Web Block Page Settings

The Block Page can be customized for each console; allowing 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.
- The Content field can be used for custom text such as telephone numbers, websites, and links. For example, you could enter information such as *Please contact your network administrator if you have any questions*, and then include the contact method of your choice.

![Web Block Page Settings](image)

Configuring Sites

DNS must be enabled for DNS Protection Agent to install or in order to protect a network. The DNS Status can be determined from the Sites tab of the Web Console. The blue number in the DNS column indicates the number of days remaining in the trial. This will turn green once upgraded from Trial to Full.

![Configuring Sites](image)
To enable DNS Protection for a Site,

1. Click the Manage button next to the Site to which you want to add DNS Protection functionality.
2. Click the DNS tab, and select the Enable SecureAnywhere DNS checkbox.
3. Select whether the Site is licensed or a trial.

![SecureAnywhere DNS Protection Admin Guide](image)

**Default DNS Policy**

This is the default DNS Policy assigned to any Endpoint or IP if one is not explicitly defined in Groups.

**Network Settings**

This section is used to register the network for network based DNS filtering.

- On the network, identify the public IPv4 address used for internet access (WAN IP). An internet search of My IP generally reveals the appropriate IP address.
- These addresses will need to be entered in order for DNS Protection to answer DNS requests, and for logging and filtering to be provided.
- IPv6 is not yet supported.
Agent Bypass List (Intranet)

The Agent Bypass List (Intranet) is designed to accommodate Active Directory. If you will be running the DNS Protection Agent in an Active Directory environment, make sure to add your AD Domain to the Agent Bypass list (both specific and wildcard).

Deploying the Agent

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 deploy the agent:
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.

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.

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.

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.

![Edit Policy Button](image)

5. You can then specify what Policies apply.

![Edit Policy Window](image)

### Viewing and Filtering DNS Statuses

To find the devices on which you have DNS installed, select the Site or Group you wish to review and configure the filter. You can select to show based on device type and Policy type.

![Filter DNS Statuses](image)
Displaying Device and IP Information

More information is available regarding the selected device by clicking the name. Here you will see an overview of the system as well as the DNS information.

On the Blocked URLs tab, each domain blocked by DNS protection is displayed.
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.

Network Settings

Under the DNS tab, you must register the network for network based DNS filtering.

- On the network, identify the public IPv4 address used for internet access (WAN IP). An internet search of My IP generally reveals the appropriate IP address.
- These addresses will need to be entered in order for DNS Protection to answer DNS requests, and for logging and filtering to be provided.
- IPv6 is not yet supported.

![Network Settings (Optional)](image)

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, and then press Enter.
3. From the File menu, select Add/Remove Snap-in.
4. Under Available snap-ins, click Certificates, and then click Add.
5. Under This snap-in will always manage certificates for, click Computer account, and then click Next.
6. Click Local computer, then click Finish then 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.
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. 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. Note that this IP is specific Network DNS Protection and does not apply to the Agent.
4. Check several Sites to confirm valid responses.

A successful test looks like the following:

```
Default Server: testwifi here
Address: 192.168.86.1
> 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.wsadns.net
Address: 66.35.53.194
Aliases: www.webroot.com
```

Configuring Local DNS Servers

Configure the DNS on the network to use the Webroot SecureAnywhere DNS Protections servers. This setting should be managed on the router or, in the case of a Windows server, under the DNS forwarders. Note that some routers use Round Robin DNS and in this instance a failover DNS server cannot be used.

- DNS1: 45.54.55.54
- DNS2: 45.54.55.55
- DNS3: Failover DNS Server (Provided by ISP)
Reporting

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 [Global Site Manager Reports Overview](#) in the [GSM Admin Guide](#).

![Image of SecureAnywhere interface](#)

### 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.

![Image of SecureAnywhere interface](#)
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: Top 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.

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.

  ![Chart showing DNS Botnet Command & Control Blocked]

  - Click the Requested or Blocked column to view further detail.

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

  ![Table showing DNS Top Active Hosts]

- **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 Blocked Domain](image1)

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

![DNS: Top Requested Category](image2)

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

![DNS: Top Sites by Number of Requests](image3)
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 URLs within the report.

To export and email a CSV file:

1. **Log in** and run the DNS Top Active Hosts report.
2. Click the [Export to CSV] button.

![Export to CSV button]

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

![Report Requested message]

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

![Report Requested message]

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

![Table showing blocked hostnames with view links](image)

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

![Export to CSV button and table](image)

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

![Report Requested message](image)

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

![Report Requested message with OK button](image)