

WEBROOT®

an **opentext™** company

DNS Protection Getting Started Guide

Copyright

Copyright 2020 Webroot. All rights reserved.

DNS Protection Getting Started 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 Getting Started Guide	1
DNS Protection Getting Started Guide Overview	2
Step 1: Start Your DNS Protection Trial	3
Step 2: Enable DNS Protection	4
Step 3: Deploy The Agent	6
Step 4: Protect the Network	7
Register Your WAN IP	7
Configure DNS Forwarders	7
Step 5: Customize Your Settings	9
Build Policies	9
Filtering Exceptions	9
Block Page	10
Conclusion	12
Chapter 2: DNS Protection Support	13
Accessing Technical Support	14
Index	i

Chapter 1: DNS Protection Getting Started Guide

To get started using the DNS Protection Getting Started guide, see the following topics:

DNS Protection Getting Started Guide Overview	2
Step 1: Start Your DNS Protection Trial	3
Step 2: Enable DNS Protection	4
Step 3: Deploy The Agent	6
Step 4: Protect the Network	7
Register Your WAN IP	7
Configure DNS Forwarders	7
Step 5: Customize Your Settings	9
Build Policies	9
Filtering Exceptions	9
Block Page	10
Conclusion	12

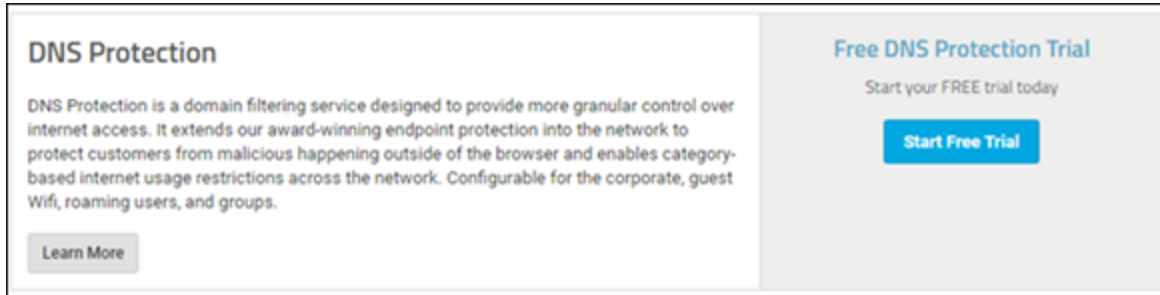
DNS Protection Getting Started Guide Overview

This document is designed as a getting started 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 DNS Protection. For more detailed information, see the Webroot SecureAnywhere DNS Protection Admin Guide.

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.

Step 1: Start Your DNS Protection Trial

The first step is to activate DNS Protection for your console. This is done from the Settings 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 Settings tab to reference the remaining days on your trial or your subscription status.

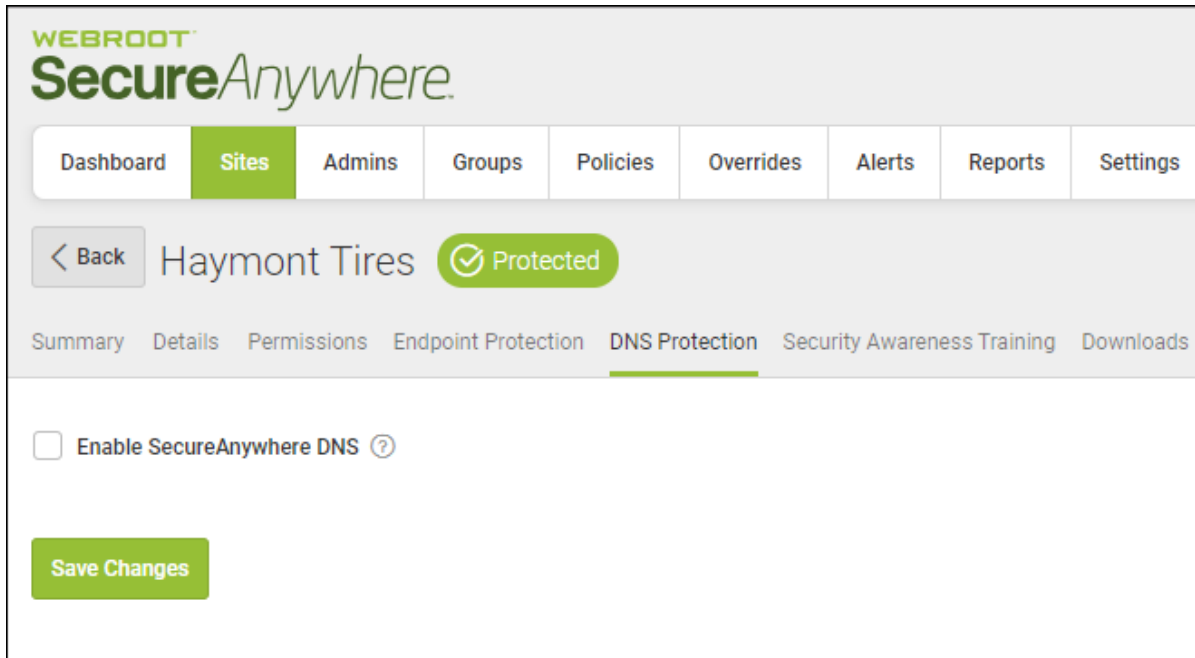


The screenshot shows a user interface for DNS Protection. On the left, under the heading "DNS Protection", there is a paragraph of text: "DNS Protection is a domain filtering service designed to provide more granular control over internet access. It extends our award-winning endpoint protection into the network to protect customers from malicious happening outside of the browser and enables category-based internet usage restrictions across the network. Configurable for the corporate, guest Wifi, roaming users, and groups." Below this text is a "Learn More" button. On the right, there is a promotional box titled "Free DNS Protection Trial" with the subtext "Start your FREE trial today" and a prominent blue "Start Free Trial" button.


Continue with [Step 2: Enable DNS Protection on page 4](#).

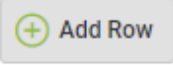
Step 2: Enable DNS Protection

DNS Protection is enabled by Site. In order to turn it on, click the **Manage** button next to the corresponding site and select the **DNS Protection** tab.





The Domain 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 Domain Bypass list.

Domain Bypass List (Optional) 

 + Add Row

Domain

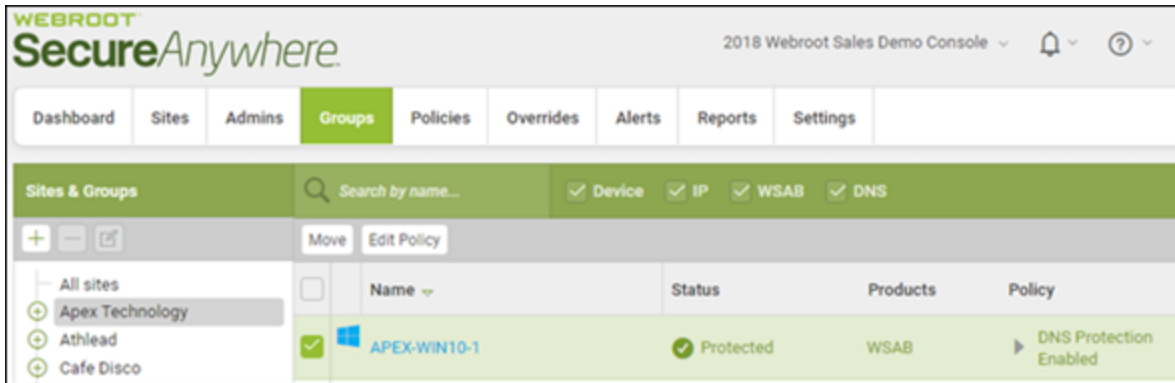


 Save Changes

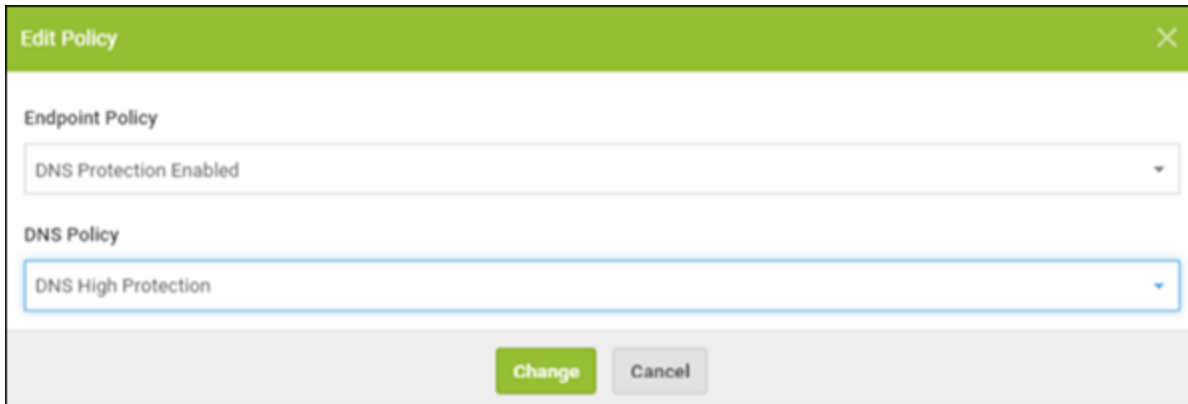
Continue with [Step 3: Deploy The Agent on page 6](#).

Step 3: Deploy The Agent

For the DNS Protection agent to be deployed, it must be configured to do so by specifying an Endpoint Policy with Install DNS Protection turned on. Recommended DNS Enabled is a usable example policy that is provided. To assign it to a system, select the **Groups** tab, select the site you just enabled, and then select the systems you want to install.



Next, click the **Edit Policy** button and specify the Endpoint policy with DNS enabled as well as your DNS Policy. Once you click the **Change** button, the next time this system checks in with the Console, the DNS Agent will install and begin filtering DNS requests.



Continue with [Step 4: Protect the Network on page 7](#).

Step 4: Protect the Network

Enabling DNS Protection for the network will allow DNS requests to be filtered for every device on the network even if they are not running the DNS Agent; allowing you to protect guest laptops, printers and even IOT devices.

There are two steps:

- [Register your WAN IP](#)
- [Configure DNS Forwarders](#)

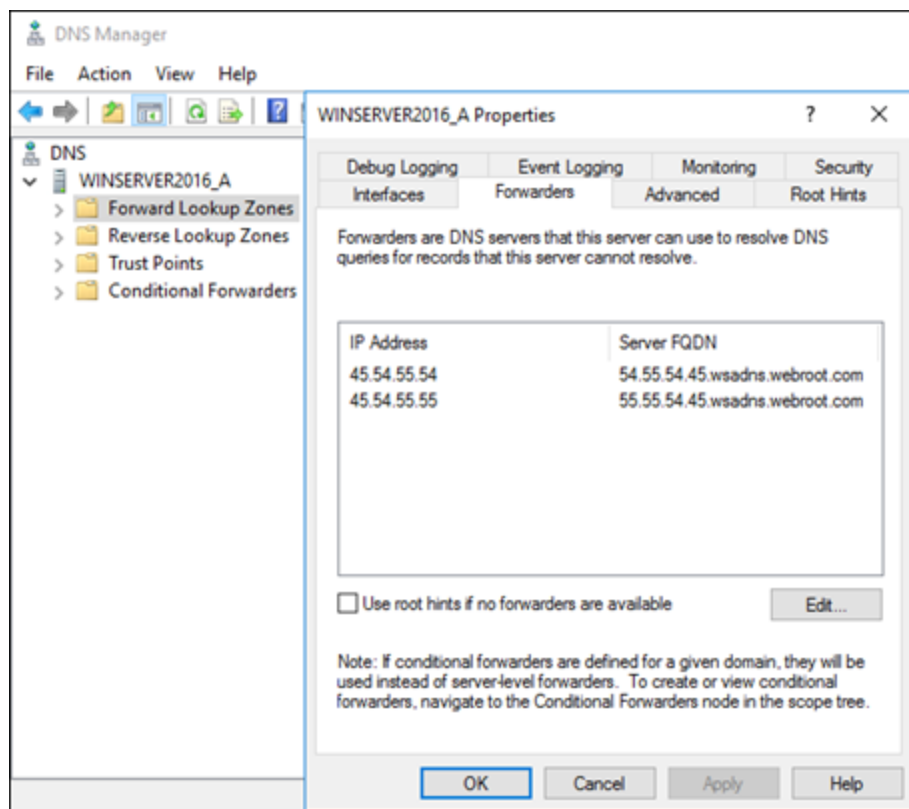
Register Your WAN IP

- Under Network Settings on the DNS tab, select **Add Row**.
- Enter your WAN IP address and select a DNS Policy.

Configure DNS Forwarders

This setting should be managed on the router or, in the case of a Windows server, under the DNS forwarders.

- DNS1: 45.54.55.54.
- DNS2: 45.54.55.55.



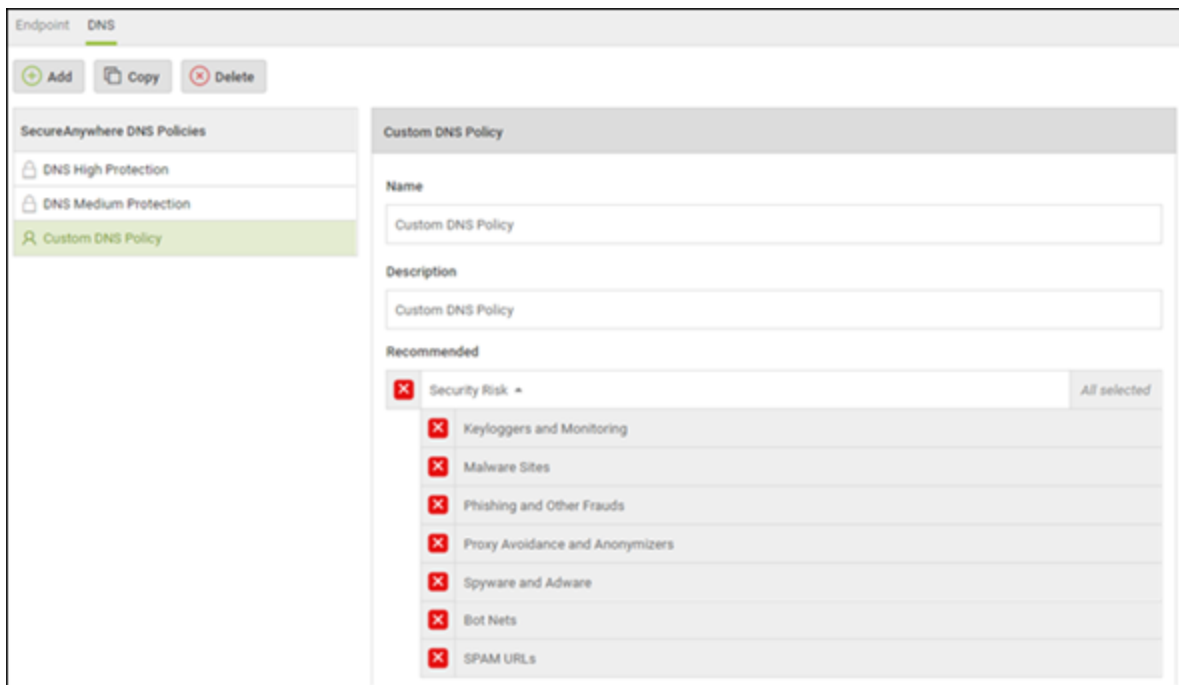
Continue with [Step 5: Customize Your Settings on page 9](#).

Step 5: Customize Your Settings

- [Build Policies](#)
- [Filtering Exceptions](#)
- [Block Page](#)

Build Policies

Custom Policies can be defined under the Policies tab by selecting DNS. To build a new policy, click the **Add** button.



Filtering Exceptions

To add exceptions to the Policies, select Overrides, Web Block / Allow List. Here domains and subdomains can be added to allow specific exceptions. These can be applied to all Sites or individual Sites.

The screenshot shows the Webroot SecureAnywhere interface. At the top, the logo 'WEBROOT SecureAnywhere' is visible. Below it is a navigation menu with tabs: Dashboard, Sites, Admins, Groups, Policies, Overrides (highlighted), Alerts, Reports, and Settings. Under the 'Overrides' tab, there are sub-tabs: File Whitelist, File Blacklist, Web Block / Allow List (highlighted), and Web Block Page Settings. Below the sub-tabs are three buttons: '+ Add', 'x Delete', and 'Refresh'. A section titled 'Select Overrides to View' contains a dropdown menu currently set to 'GSM Global Web Overrides'. Below this is a 'Block & Allow' dropdown and a search box labeled 'Search for URL...'. The main content is a table with two columns: 'URL' and 'Action'.

URL	Action
*.facebook.com	Block
vpn.mydomain.com	Allow
*.webroot.com	Allow

Block Page

The messaging provided to the user when a requested site is blocked can be defined under the Overrides tab, Web Block Page Settings.

The screenshot displays the Webroot SecureAnywhere management console. The top navigation bar includes 'Dashboard', 'Sites', 'Admins', 'Groups', 'Policies', 'Overrides' (highlighted in green), 'Alerts', 'Reports', and 'Settings'. Below this, a secondary menu shows 'File Whitelist', 'File Blacklist', 'Web Block / Allow List', and 'Web Block Page Settings' (highlighted with a red box). The main content area features a logo upload box on the left and the 'WEBROOT' logo on the right. A dark grey banner reads 'Website not allowed'. Below this is a large red circle with a white exclamation mark. The text states: 'The category <category> is restricted. Your organization's Internet usage policy restricts access to this website at this time.' At the bottom, there is a browser-style toolbar with icons for bold, italic, list, and link. A text box contains the message: 'Please contact your network administrator if you have any questions. Submit a request to review category [here](#)'.

Continue with the [Conclusion on page 12](#).

Conclusion

The steps provided allow for the initial configuration of DNS Protection. All DNS requests for the network should be protected by the DNS Protection Servers and all systems running the Agent should be protected regardless of the network to which they are attached.

For more information including additional deployment strategies, reporting, testing and troubleshooting, Active Directory considerations, and Firewall management, please see the [DNS Protection Admin Guide](#).

For more information on the Web Console and Policy Management, please see the [Business Endpoint Protection Admin Guide](#).

Chapter 2: DNS Protection Support

For information about support, see the following topic:

Accessing Technical Support	14
--	-----------

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.](#)
-

Index

A

- activate DNS Protection 3
- agent, deploying 6
- assigning to system 6

B

- block page, customizing 9
- build policies 9

C

- conclusion 12
- configuring DNS Forwarders 7
- customizing
 - block page 9
 - settings 9

D

- deploying agent 6
- DNS Forwarders, configuring 7
- DNS Protection
 - activate 3
 - enabling 4
 - free trial 3

E

- enabling DNS Protection 4
- exceptions, filtering 9

F

- filtering exceptions 9
- free trial, starting 3

N

- network, protecting 7

P

policies, building 9
protecting network 7

R

registering WAN IP 7

S

settings, customizing 9
starting free trial 3
system, assigning 6

W

WAN IP, registering 7