WEBROOT®

an opentext™ company

DNS Protection
Getting Started Guide

Copyright

DNS Protection Getting Started Guide

Table of Contents

Chapter 1: DNS Protection Getting Started Guide

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

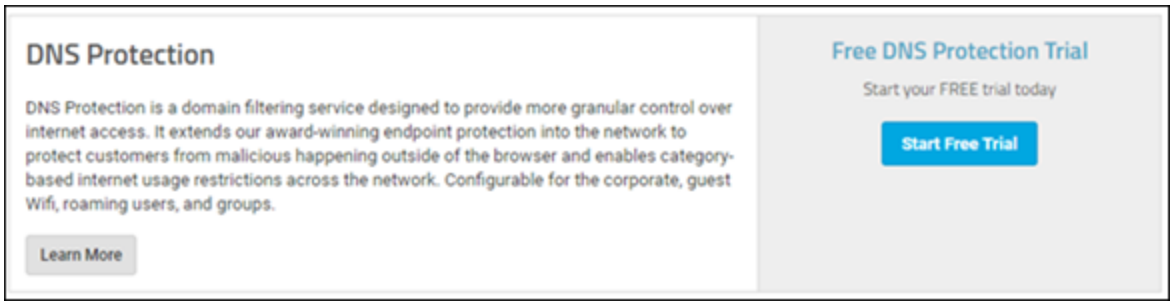
DNS Protection Getting Started Guide Overview

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

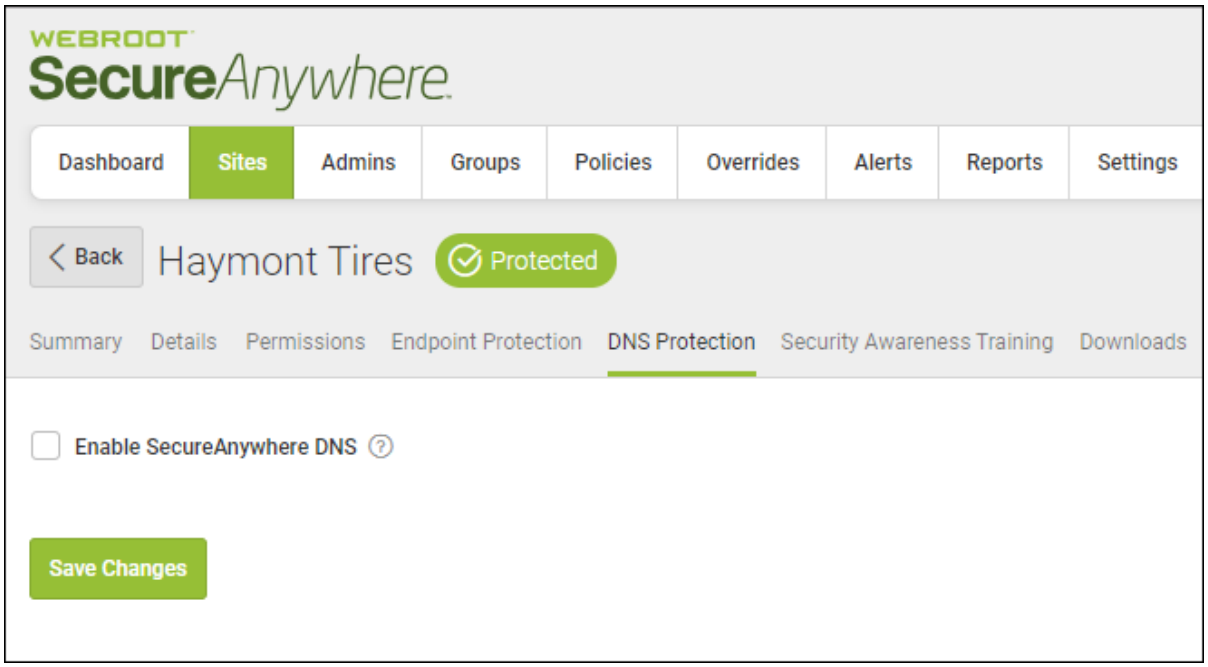
The first step is to activate DNS Protection for your console. This is done from the Settings tab. Here you can initiate a trial by clicking the Start Free Trial button. Once the trial is active or once you have purchased, you can use the Settings tab to reference the remaining days on your trial or your subscription status.



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.



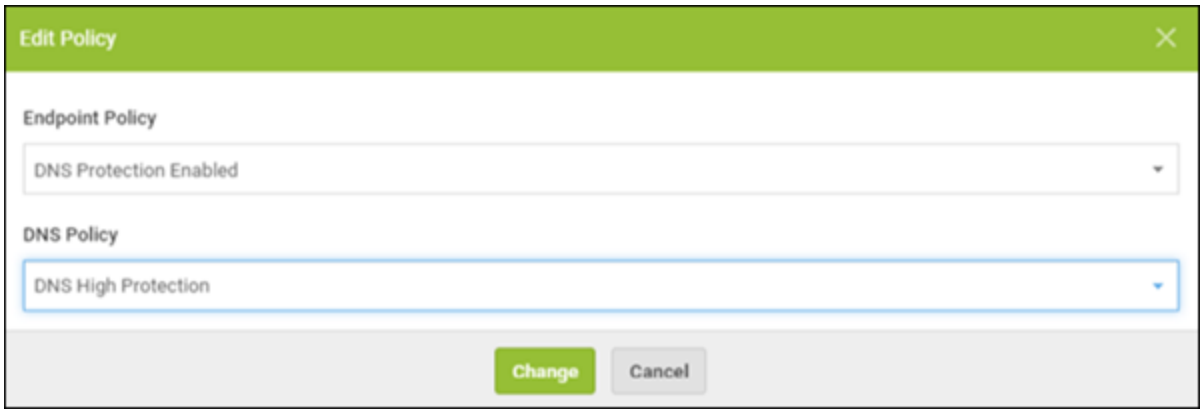
The Domain Bypass List (Intranet) is designed to accommodate Active Directory. If you will be running the DNS Protection Agent in an Active Directory environment, make sure to add your AD Domain to the Domain Bypass list.

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

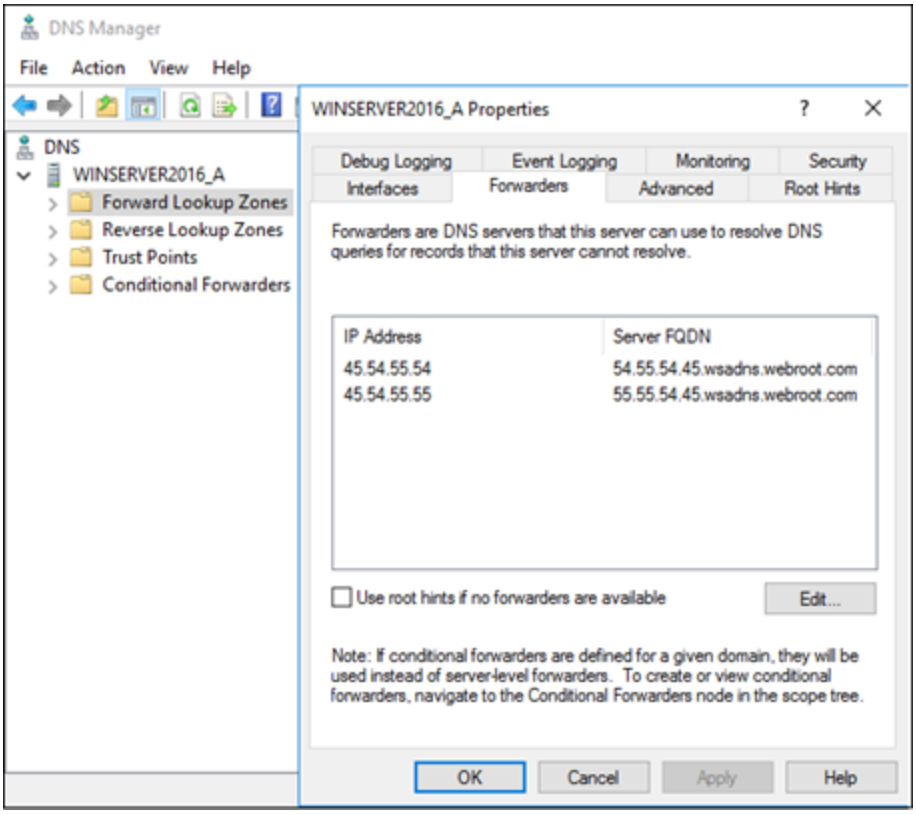
Register Your WAN IP

- 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.

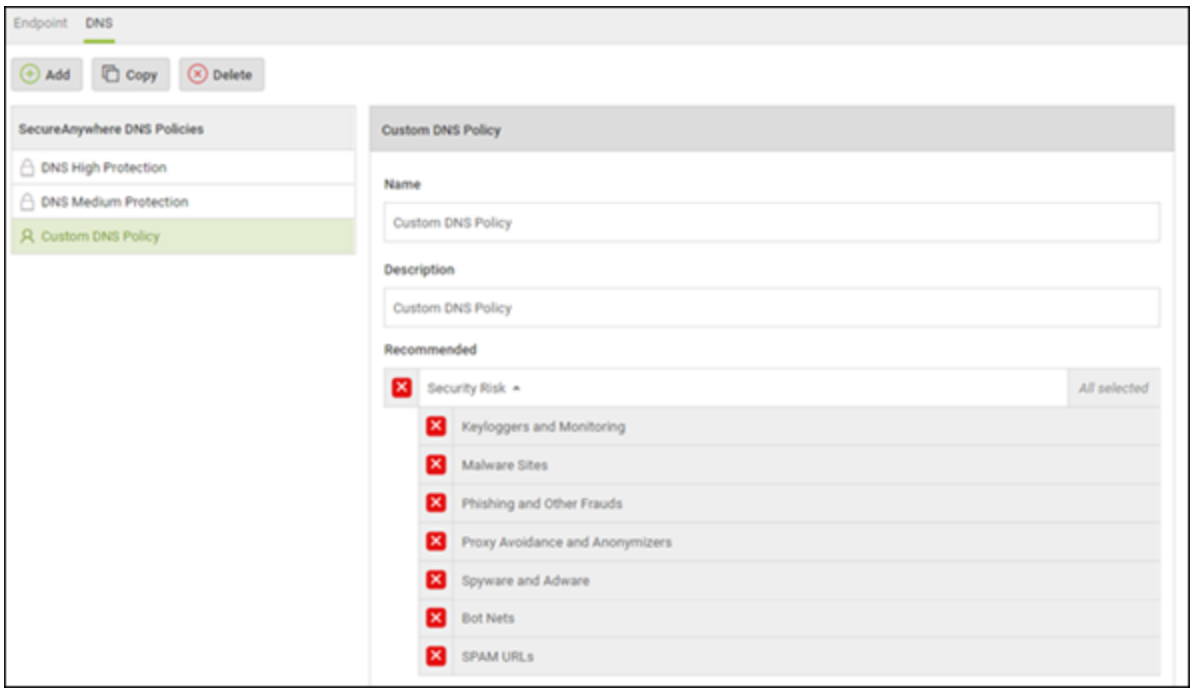


Continue with *Step 5: Customize Your Settings on page 9*.

Step 5: Customize Your Settings

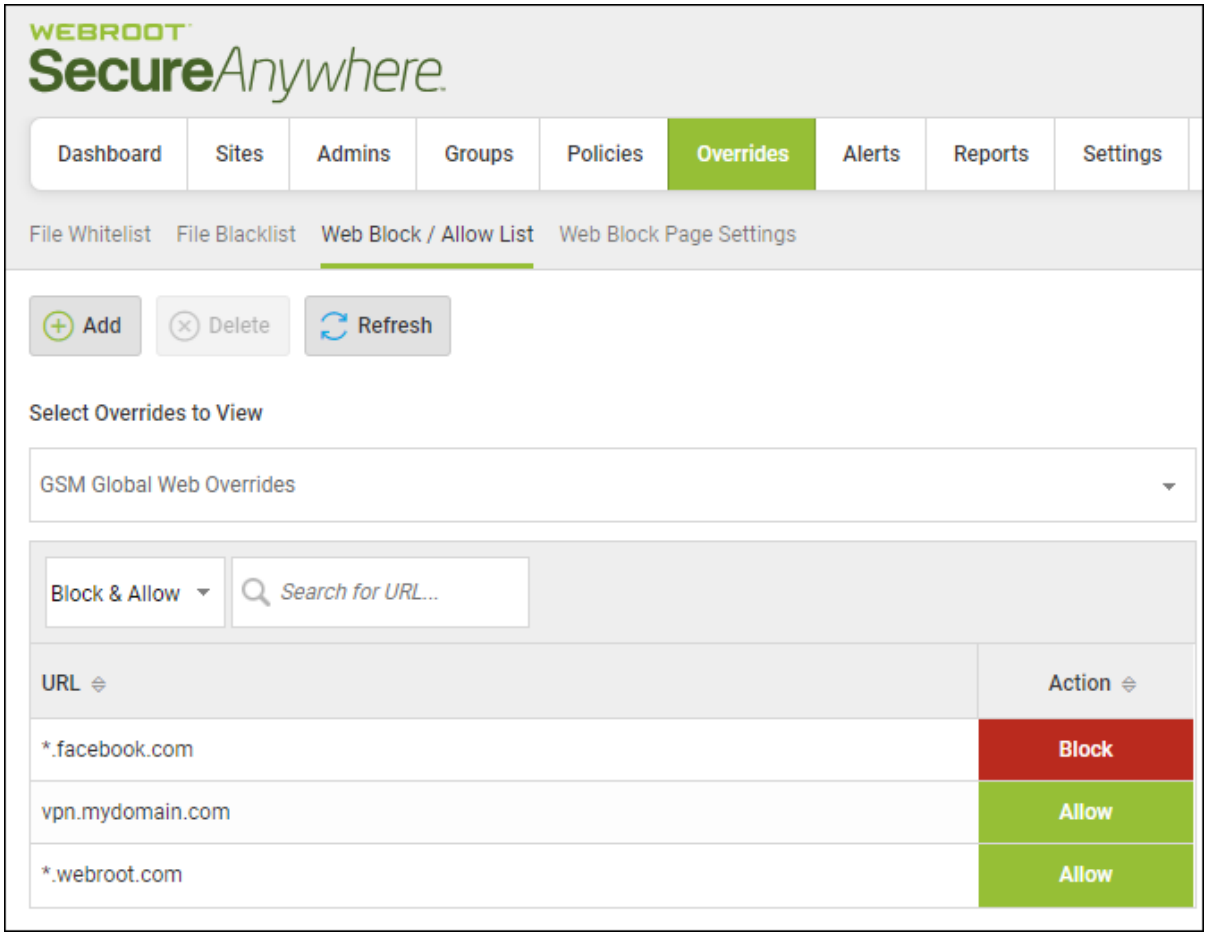
Build Policies

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



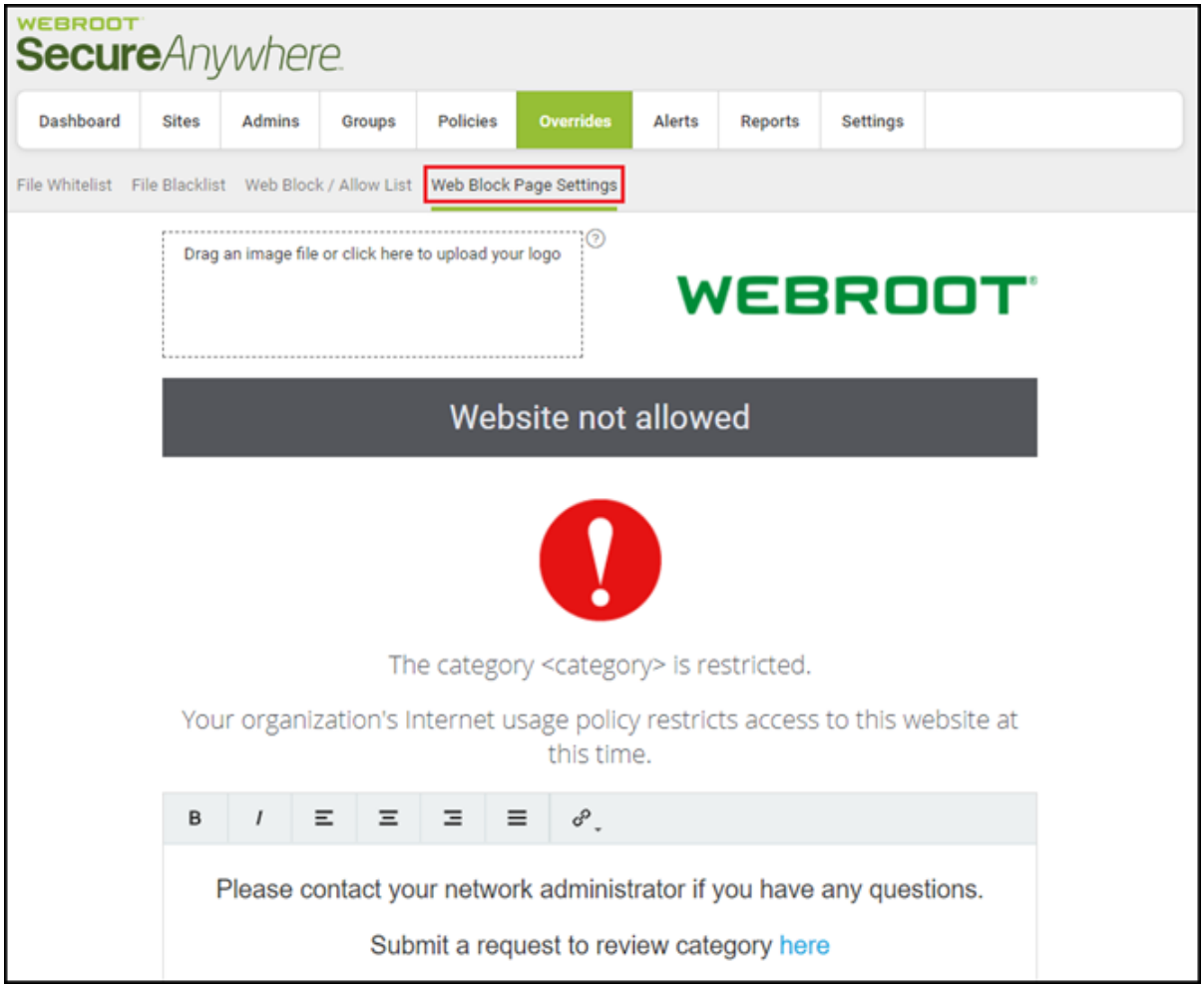
Filtering Exceptions

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.



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.



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

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
