

WEBROOT®

an **opentext™** company

Webroot Business Getting Started Guide for MSPs

Copyright

Copyright 2019 Webroot. All rights reserved.

MSP Management Console 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

| | |
|--|-----------|
| System Requirements | 1 |
| Webroot business getting started guide for MSPs | 2 |
| Is this for me? | 2 |
| Step 1: Registering for a trial or purchase the product | 3 |
| Register for a trial: | 3 |
| Purchase a business product: | 3 |
| Step 2: Create your Webroot Account | 4 |
| Activating and Creating your Account | 5 |
| Setting up two-factor authentication (2FA) | 6 |
| System Requirements | 6 |
| The first time setup of your management console | 11 |
| Setting your console configuration | 11 |
| Spotlight Tour | 12 |
| Step 3: Install Webroot Endpoint Protection | 15 |
| Create your first site | 16 |
| Step 1: Details | 16 |
| Step 2: Permissions | 17 |
| Step 3: Endpoint Protection | 18 |
| Step 4: DNS Protection | 19 |
| Step 5: (optional): Security Awareness Training | 20 |
| Deploy agents to endpoints | 21 |
| Starting to use Endpoint Protection | 23 |
| Index | 25 |

System Requirements

Most modern web browsers are supported for setting up your account and management console, and the Webroot Business Endpoint Protection product protects most modern Windows and Apple computers. Windows servers and a mix of VMs are also protected. Review the detailed list if you have questions.

The system requirements are listed at the bottom of the Endpoint Protection product page:

<https://www.webroot.com/us/en/business/smb/endpoint-protection#heading-requirements>

Note: These links are to the United States English language site. Country and language options can be changed at the far top right of the website by clicking on a flag and selecting a country of your choice.

Continue to [Webroot Business Getting Started Guide for MSPs](#).

Webroot business getting started guide for MSPs

Is this for me?

This getting started guide is primarily for Managed Service Providers (MSPs) who manage the security of their clientele. Large enterprises with offices spread across various locations may want to use this guide as well.

In this guide, you will be using multiple “sites” to represent your clients. We will take you through setting up and using Webroot Business Endpoint Protection using our management console for multiple sites.

What Is A Site?

For this product, “Sites” allows service providers to manage products for a company under their protection. Besides a company account, sites can also represent department, corporate region, or office location. Sites allows the management of a large amount of endpoints to be summarized by clientele.

Set up in three steps

1. The first step was registering a trial or purchasing your Webroot business product. You should have completed this step before receiving this guide.
2. The second step is to create and activate your Webroot account, setting up two factor authentication, and a first-time set up of the Webroot business management console.
3. The third step is to install Webroot Endpoint Protection by deploying agents to endpoints or delivering security training to target users.

Continue to [Step 1: Registering for a trial or purchase the product](#).

Step 1: Registering for a trial or purchase the product

You should have already registered for a trial or purchased a Webroot business product.

Skip to [Step 2: Create your Webroot account](#) if you have registered a trial or purchased a product and must install the product.

Otherwise:

Register for a trial:

Visit the Webroot website for business at: <https://www.webroot.com/us/en/business>. Click the main navigation menu item **FOR BUSINESS** and click on **FREE TRIALS**. If you are unsure where to start, choose Endpoint Protection.

The trial page also has the telephone number for our sales experts if you need assistance.

Purchase a business product:

Visit the Webroot website for business at: <https://www.webroot.com/us/en/business>. Research and learn about our products and add products to the online cart. The cart will give you clear instructions on how to complete an online purchase or purchase through a sales channel for larger subscriptions.

Note: These links are to the United States English language site. Country and language options can be changed at the far top right of the website by clicking on a flag and selecting a country of your choice.

Continue to [Step 2: Create your Webroot Account](#).

Step 2: Create your Webroot Account

In this step, we'll walk through:

- [Activating and creating your Webroot account](#)
 - [Setting up two-factor authentication \(2FA\)](#)
 - [The first-time set up of your business management console](#)
-

Activating and Creating your Account

We'll begin by creating your Webroot account. Your Webroot account is used for Webroot's business or consumer products. It's your personal and business identity to manage Webroot's products. In this case, we are setting up your account to start using the business management console.

What Is The Business Management Console?

The Webroot business management console is the online portal that you will use to manage any or all of the Webroot business products, starting with Webroot Business Endpoint Protection.

To create an account

1. Open, read and follow the instructions in the email from Webroot to set up your management console. This email usually arrives 5-10 minutes after the Welcome email.
2. Click the registration link in the email.
3. Copy the temporary password from the email you receive, and paste it in the **Temporary Password** field on the Confirm Registration pane.
4. In the **Create New Password** field, enter a new password, and re-enter your new password again to confirm.
5. In the **Personal Security Code** field, enter a security code that you will use to log in. You will be asked to enter two of those digits randomly selected by position, so choose a code that is easy for you to memorize.
6. From the **Security Question** drop-down menu, select one of the security questions and provide your answer in the applicable box.
7. In the **Office Phone** field, enter the best business phone number to contact you.
8. Select **Agree & Register Now** checkbox.
9. Click the **Confirm** button.

Continue with [Setting up two-factor authentication](#).

Setting up two-factor authentication (2FA)

Now that your account is active, you can set up two-factor authentication. Two-factor authentication, or 2FA, adds an additional layer of protection for cyber resiliency to help prevent unauthorized users from gaining access to your account without permission.

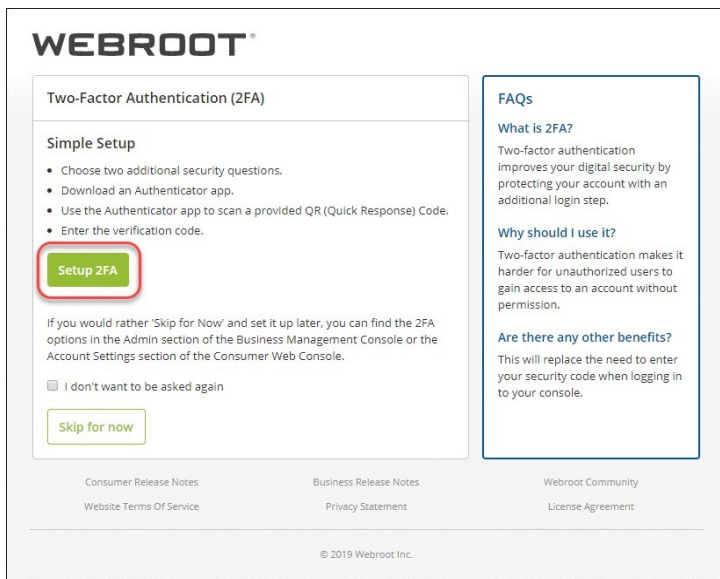
Setting up two-factor authentication is optional. If you do not wish to use 2FA, skip ahead to [the first time setup of your management console](#).

System Requirements

You will need to use an Authenticator app on an Android or iOS mobile device or tablet.

To set up two-factor authentication (2FA)

1. First, visit the [Webroot Management Console](#), and log in using your account credentials.
2. You will see the Set up Two-Factor Authentication page. If this is the first time you have logged into the Management Console, you can either click **Setup 2FA** to start the process, or click **Skip for now** to continue to the Console.



If you have already logged into the Management Console and opted to skip the 2FA setup process, click here for instructions on enabling 2FA.

You can also start the 2FA setup process from the Admins tab in the Management Console by clicking your

name in the Admin list which displays your details in the right panel. Scroll down, and click **Enable**.

The screenshot shows the profile page for 'Admin User 3 (admin3@domain.com)'. The page has two tabs: 'Details' and 'Site Permissions'. Under the 'Details' tab, there are several form fields: 'First Name' (Admin), 'Last Name' (User 3), 'Phone' (empty), 'Time Zone' (UTC/GMT), and 'Account Type' (No Access). Below these fields are sections for 'Password', '2FA', 'Security Code', and 'Security Question', each with a 'Change' button. The '2FA' section has an 'Enable' button, which is highlighted with a red rectangular box. At the bottom of the form is a green 'Save' button.

3. Next, the **Setup 2FA** screen displays and will prompt you to pick two security questions and answers and then click **Continue**.
4. You will need to download and install an authenticator app from the Google Play Store or the Apple App Store to a smart phone or tablet with a working camera.

Examples of Mobile authentication apps include Google Authenticator, Microsoft Authenticator, LastPass Authenticator, and Authy 2-Factor Authentication.

5. After you have downloaded and installed an authenticator app, open the app, and follow the prompts to scan the QR code shown in the Management Console. If you are unable to scan the QR code, click **Can't scan the QR code?**, and enter the entire code shown into the authenticator app on your device. The code is case sensitive, so enter upper and lowercase characters exactly as shown.

The screenshot displays a three-step setup process for two-factor authentication:

- Step 2:** "Download an Authenticator App to your Smart phone or tablet that has a camera. Webroot recommends using one of the following free apps, from either the Google Play Store or the Apple App Store:"
 - Google Authenticator
 - Microsoft Authenticator
 - LastPass Authenticator
 - Authy 2-Factor Authentication
- Step 3:** "Open your app and scan the QR code below."
 - A QR code is shown with the word "EXAMPLE" overlaid in the center.
 - A red callout box says "Can't scan the QR code?".
 - Text below: "If you can't scan the QR code please enter the below secret manually into your authenticator application on your device. You must set your new secret to be 'time-based' and six characters long."
 - A red callout box shows a secret key: "VZYEU1 HXNL" on the top line and "MYYD2X" on the bottom line.
- Step 4:** "Enter the verification code from your Authenticator app in the field below:"
 - An empty text input field is shown.
 - A green "Verify Code" button is below the field.

Navigation buttons: "Cancel" (green) and "Complete Setup" (grey).

6. Enter the verification code from the authenticator app in the box under **Step 4**, and click **Verify Code**. The code will be verified, and the screen will show a **Verification Successful** message. Click **Complete Setup** to finish setting up two-factor authentication.

WEBROOT®

Setup 2FA


Step 2
Download an Authenticator App to your Smart phone or tablet that has a camera. Webroot recommends using one of the following free apps, from either the Google Play Store or the Apple App Store:

| | |
|------------------------|-------------------------------|
| Google Authenticator | Microsoft Authenticator |
| LastPass Authenticator | Authy 2-Factor Authentication |

Need more help? [Click here for a guide](#)

Cancel

Step 3
Open your app and scan the QR code below.



Can't scan the QR code?

Step 4
Enter the verification code from your Authenticator app in the field below:

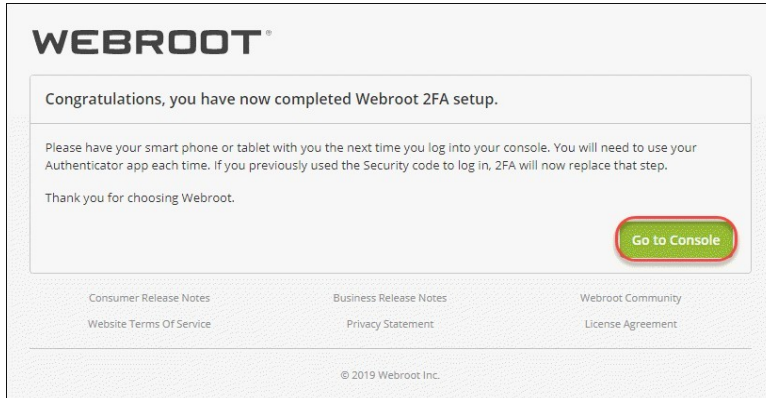
Verification Successful

Verify Code

Complete Setup

Note: If you receive a **Verification Unsuccessful** message when entering the code, you will need to enter a new code from the authenticator app as codes are only valid for 30 seconds, and click **Verify Code**.

7. 2FA is now enabled, and the Congratulations screen will display. Click **Go to Console** to log into the Management Console using the authenticator app that will supply the authentication code you will enter at login which replaces the Security Code.



Note: The Security Code will be stored for your account and will be used if 2FA is disabled.

8. An email from Webroot will be sent to you informing you that 2FA has been enabled for your account.

Continue to [The first time setup of your management console](#).

The first time setup of your management console

When you sign into the console for the first time, you will need to make an important console configuration decision.

Setting your console configuration

Managed Service Provider option

The Managed Service Provider (MSP) configuration will set up a management console where you can manage sites for the companies that pay you to provide their cyber security. A site is used to represent separate entities under your management to help with reporting and billing your customers.

If you will manage the security of clientele, choose **Managed Service Provider**.

What Is A Site?

For this product, “Sites” allows service providers to manage products for a company under their protection. Besides a company account, sites can also represent a department, corporate region, or office location. Sites allows the management of a large amount of endpoints to be summarized by clientele.

Note: Selecting Managed Service Provided with a multi-site configuration is not reversible.

If you only manage the security of your own business, select the business option. This action will set up your management console to a single site configuration which can be upgraded to a multi-site configuration in the future. If you want to select the business option, start using the [Business Management Console Guide](#) at this step instead of this guide.

To set your console to a multi-site MSP configuration:

1. Log in to the management console.
2. Under Managed Service Providers on the right, click Select.

3. Your console is configured for using multiple sites.

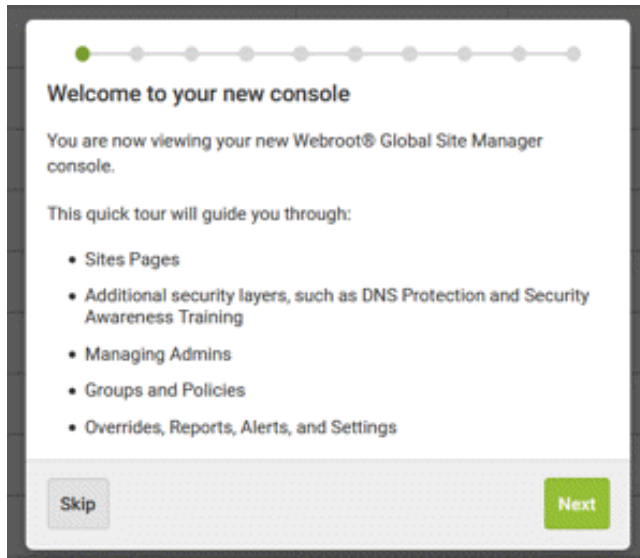


Spotlight Tour

The Spotlight Tour displays when you first set up your account. The tour includes a brief description about the following:

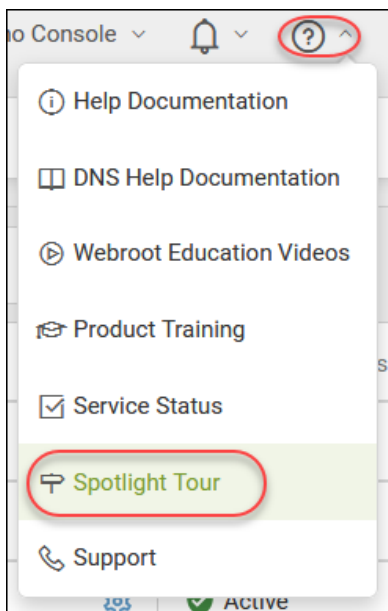
- Sites Pages
- Additional security layers, such as DNS Protection and Security Awareness Training
- Managing Admins
- Groups and Policies

- Overrides, Reports, Alerts, and Settings



To view the Spotlight Tour again in the future:

Click on the help menu icon  in the upper right-hand global navigation bar, and select **Spotlight Tour** from the drop-down menu.



Continue to [Step 3: Install Webroot Endpoint Protection](#).

Step 3: Install Webroot Endpoint Protection

Webroot Business Endpoint Protection is the base product for Webroot's suite of products for layered security. To get you up and running with your first Endpoint Protection deployment, we'll be:

- Creating your first site
- Deploying the Endpoint Protection agents to endpoints


What Is An Endpoint?

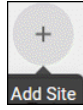
An endpoint is any device connected to a network. For this product, an endpoint is a device using Windows or Mac OS X operating systems.

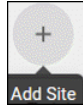
Continue to [Create your first site](#).

Create your first site

For your first site we will create an internal site where you will deploy agents to your business's endpoints. This is a good introduction to the product before you use it on any of your customers that you manage.

If you haven't done so, log into your management console, and click the **Sites** tab icon .



Add a site by clicking on the plus sign icon  to the right of the search bar. The search bar and other tools are located on the right directly above the sites table.

The **Add Site** step wizard will load.

Step 1: Details

In the following example, the site will represent your own company.

Add site details

1. In the **Site/Company Name** field, use your company name.
2. In the **Site Type** field, select **Internal Site**. When you create a site that is an external customer purchasing services from you, you would use the **External Company** option, and complete the additional fields as applicable to your customer.

Dashboard Sites Admins Groups Policies Overrides Alerts Reports Settings

< Back Add Site

1 Details 2 Permissions 3 Endpoint Protection 4 DNS Protection

Site / Company Name ?

Site Type ?

External Company Internal Site

Comments ?

Tags ?

Add Tag... Add

Next

3. You do not need to add comments or tags at this time.
4. Click **Next**.

Step 2: Permissions

You will see a list of the global administrators.

Set site permissions

1. Click the **Admin** button on the header to give administrator privileges to yourself. As you add more global administrators to your console, you can selectively add permissions on an as needed basis.

< Back Add Site

1 Details 2 Permissions 3 Endpoint Protection 4 DNS Protection

Admin Admin View Only No Access

2. Click the **Next** button to move to the next step.

Step 3: Endpoint Protection

In this step, we will configure the overall site settings for the Endpoint Protection product. The Endpoint Protection product is the base Webroot business product.

Configure site settings for Endpoint Protection

1. For Keycode Type, click either the **Full** or **30 day trial** option depending on if you have purchased or are trialing the product.
2. In the **Site Seats** field, enter the total number of endpoints for the new site that you plan to protect.
3. Keep the “Recommended Defaults” selection in the **Default Endpoint Policy** drop down list. Endpoint protection has several pre-configured policies and as you use the product, you will be able to create, manage and deploy your own security policies.
4. Click to enable the **Include Global Policies?** Checkbox. This allows you to experiment with using global policies and having changes inherited and rolled out to your site.

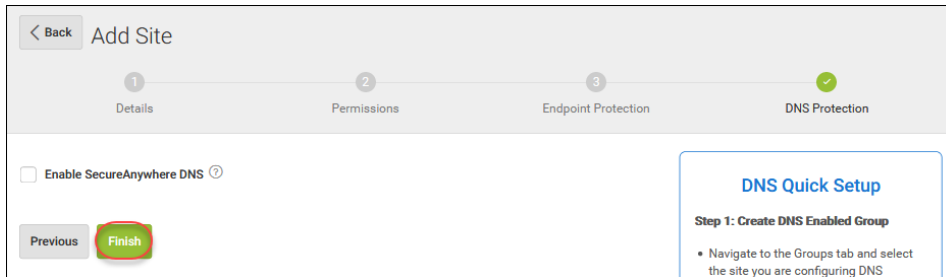
5. Click to enable the **Include Global Overrides?** checkbox. This allows you to experiment with using overrides to the default policy and having them deploy to your site.
6. In the **Data Filter** drop-down menu, keep the **Inherit the GSM data filter** selection. GSM is “Global Site Manager” and means settings made at the global level in the console will distribute outwards to this site. This choice allows you to try changing the data filter at some point and seeing the results in this site.
7. You're done. Click the **Next** button.

Step 4: DNS Protection

After you have set up and used Endpoint Protection, you might want to try using Webroot Business DNS Protection. For now, do not enable DNS Protection unless you wish to start using both DNS Protection and

Endpoint Protection. You can always easily enable DNS Protection for a site afterwards under the **Settings** tab.

Click **Finish** or **Next**. If you have a trial or purchased Webroot Security Awareness Training, you will have an additional step. Otherwise the site will be created and you will see it in your Sites tab list.



Step 5: (optional): Security Awareness Training

If you have a trial or purchased Webroot Security Awareness Training you will have a step to enable the product. After you have set up and used Endpoint Protection, you will want to try using the product. For now, do not enable the product unless you wish to start using it. You can always easily enable the product for a site afterwards under the **Settings** tab.

Click **Finish**.

Continue to [Deploy Agents to Endpoints](#).

Deploy agents to endpoints

Webroot Business Endpoint Protection protects PCs and Macs by installing an agent on the machine.


In this example, we'll manually install an agent on a Windows PC and an Apple Mac.

You can deploy the Webroot agent using a silent background installation, using MSI, or using Group Policy Object (GPO). At this point we want you to see a scan in progress and the results in the console.

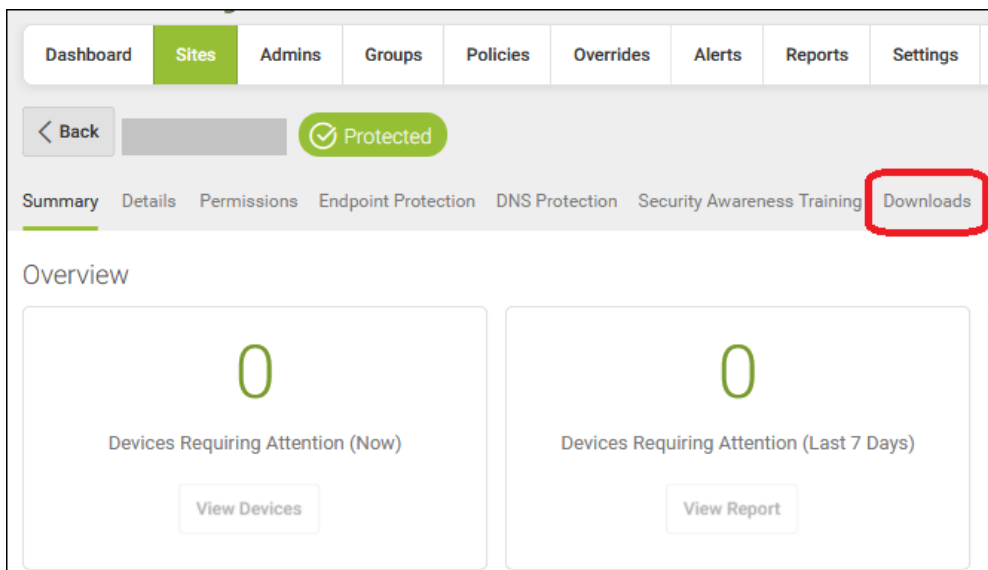
Download a Windows or Mac agent

You should be logged into the console and then do the following:

1. Click on the **Sites** tab.

2. In the list, click on the **Manage** button  in the Site column located to the right of your Site name.

3. The site view has its own set of tabs underneath the site name and site status. Click on the **Downloads** tab.



4. In the downloads tab you will see Download links to download a Windows PC or Mac agent to your local computer. These downloads include a keycode for the site pre-completed. Click the Download link for Windows PC or Mac.

5. The agent .exe or .dmg will download from your web browser to your computer.
6. You then run the Windows file or open the Mac file to start the installation.

Install a Windows agent on the target endpoint

- Run the .exe file to install the agent.


That's it! When the agent has installed, it will report to the console for centralized management.

Manually install a Mac agent on the target endpoint

1. Download or copy the Webroot agent .dmg file to your Mac.
2. Locate and double-click the wsamac.dmg file to open the installer.
3. Open the Applications folder and double-click the Webroot icon to launch the installer.
4. In the first activation window, the Language Selection drop-down menu, select the main language for the end user. You cannot change this setting later. Click the **Next** button.
5. In the next panel, click **Activate**.
6. Follow any remaining on-screen prompts to complete the installation.

Finding the site's keycode

If you ever need to use a site's Keycode while installing an agent do the following:

- Click the **Sites** tab and click on the key icon  next to the site name.
- The keycode is also displayed on the downloads tab under the site view.

Continue with [Starting to use Endpoint Protection](#).

Starting to use Endpoint Protection

As the endpoint agents check into the console, you will see the number of devices increase in the **Devices** column. If any threats are detected, the **Status** will change to **Needs Attention** as shown in the below example:

The screenshot shows the Webroot SecureAnywhere console interface. The top navigation bar includes 'Dashboard', 'Sites', 'Admins', 'Groups', 'Policies', 'Overrides', 'Alerts', 'Reports', 'Settings', and 'Security Awareness Training'. The 'Sites' section is active, showing 11 sites accessible and 12 total. A search bar and action icons are present. The main table displays the following data:

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|-----------------|------------|---------|------------|----------------|-----------------------------|
| Needs Attention | [Redacted] | 13 | 45 | Active | Active |
| Needs Attention | [Redacted] | 12 | 30 | Active | Active |
| Needs Attention | [Redacted] | 7 | 4 | Active | Active |
| Expired | [Redacted] | 0 | 5 | Inactive | Inactive |
| Suspended | [Redacted] | 0 | 18 | Inactive | Inactive |
| Protected | [Redacted] | 8 | 11 | Active | Active |
| Protected | [Redacted] | 5 | 4 | Active | Active |
| Protected | [Redacted] | 7 | 9 | Active | Active |
| Protected | [Redacted] | 17 | 25 | Active | Active |
| Protected | [Redacted] | 0 | 12 | Active | Active |
| Deactivated | [Redacted] | 0 | 30 | | |

Summary statistics at the bottom of the table:

- 69 Active Devices, 158 Site Seats
- 0 Trial Active Devices, 5 Trial Site Seats

You'll want to get used to the product, and can learn more about Endpoint Protection in these places:

- The [Administration Guide](https://docs.webroot.com) on docs.webroot.com
- [Business Endpoint Protection](#) on [The Webroot Community](#)
- The Webroot [Support Knowledge Base](https://answers.webroot.com) on answers.webroot.com

Index

C

configurations, service 3

S

service configurations 3

