WEBROOT®

an opentext™ company

Business Management Console Getting Started Guide

Copyright

Business Management Console Getting Started Guide

Table of Contents

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 Mac 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.

Business Management Console Overview

Is This For Me?

This getting started guide is for small and medium businesses who manage their own security. If you manage the security for other companies or clientele, use the MSP Management Console: Getting Started Guide at https://docs.webroot.com/us/en/business.

It is intended for people familiar with computers but who are not necessarily system administrators.

We will take you through setting up and using Webroot Business – Endpoint Protection using our management console for a company. If you manage up to 5 computers, consider using Webroot SecureAnywhere® Internet Security Complete.

What Is An Endpoint?

For this product, an endpoint is a Microsoft Windows or an Apple Mac computer, laptop, server or virtual machine. Webroot Business – Endpoint Protection will protect your endpoints from malware, viruses, and other threats. If you want to protect Google Android or Apple iOS devices, consider Webroot – Mobile Protection.

Continue to Getting Started.

Getting Started

Every company uses their computers in their own way, and has a different network. You probably have your own security requirements. This Getting Started Guide covers getting you up and running with standard security settings, and once you see the product in action, you can try out the powerful features of modifying security policies and overrides, deploying agents silently, and organizing computers into groups.

Set up in three steps

We'll take you through three major steps to get you up and running.

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. You will install an agent on each computer you want protected, and the agent will register and report through the business management console.

After these steps, you'll use the management console to see all your computers and devices under Webroot protection.

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 have purchased a Webroot business product.

> Skip to Step 2: Creating an account if you have registered for a trial or purchased a product and have to 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 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 with Step 2: Creating an account.

Step 2: Creating an Account

In this section, we'll walk through:

- Activating and creating your Webroot account
- Setting up two-factor authentication (2FA)
- The first-time setup of your business management console

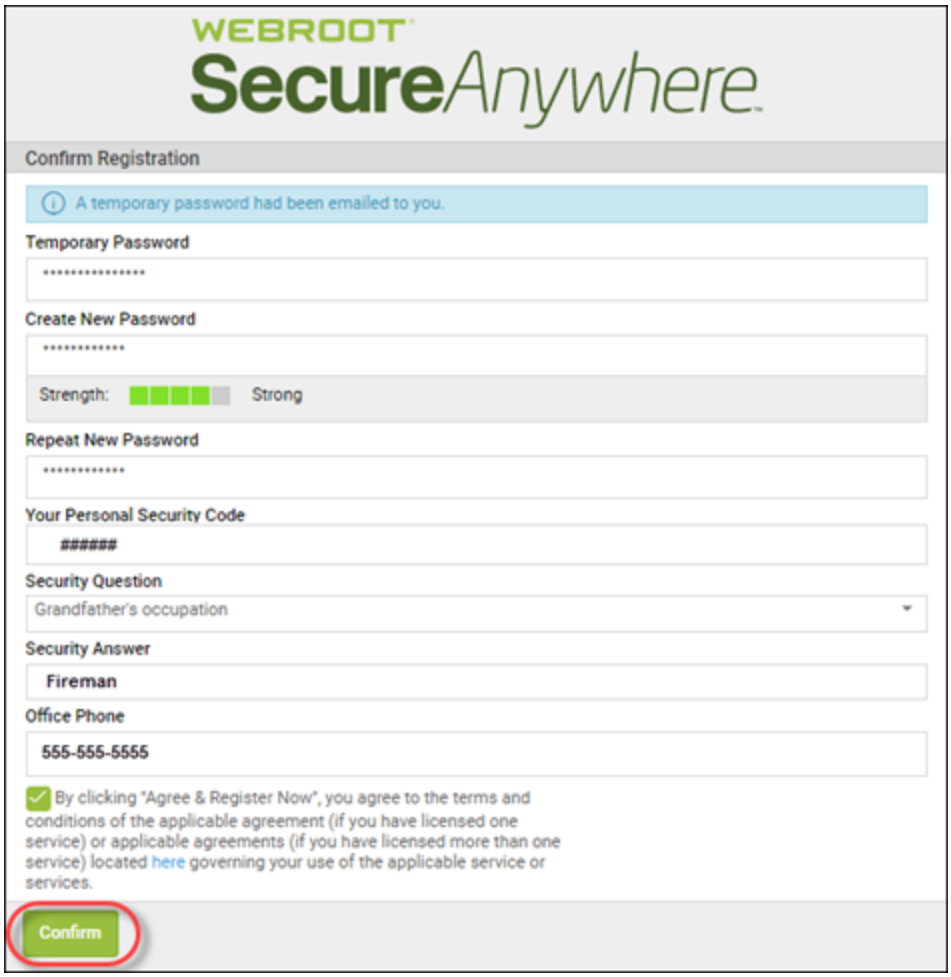
Activating and Creating Your Account

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.

To create an account:

1. Open, read, and follow the information in the Webroot Management Console (Trial) Account - Instructions email from Webroot to set up your management console. This email usually arrives 5-10 minutes after your Welcome email.
2. Click the registration link in the email.
3. Copy the temporary password from email you receive, and paste 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.
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 phone number for your office.
8. Select the **Agree & Register Now** checkbox.

9. Click the **Confirm** button.



10. You've now created and activated your account.

Continue with Setting up two-factor authentication (2FA).

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.

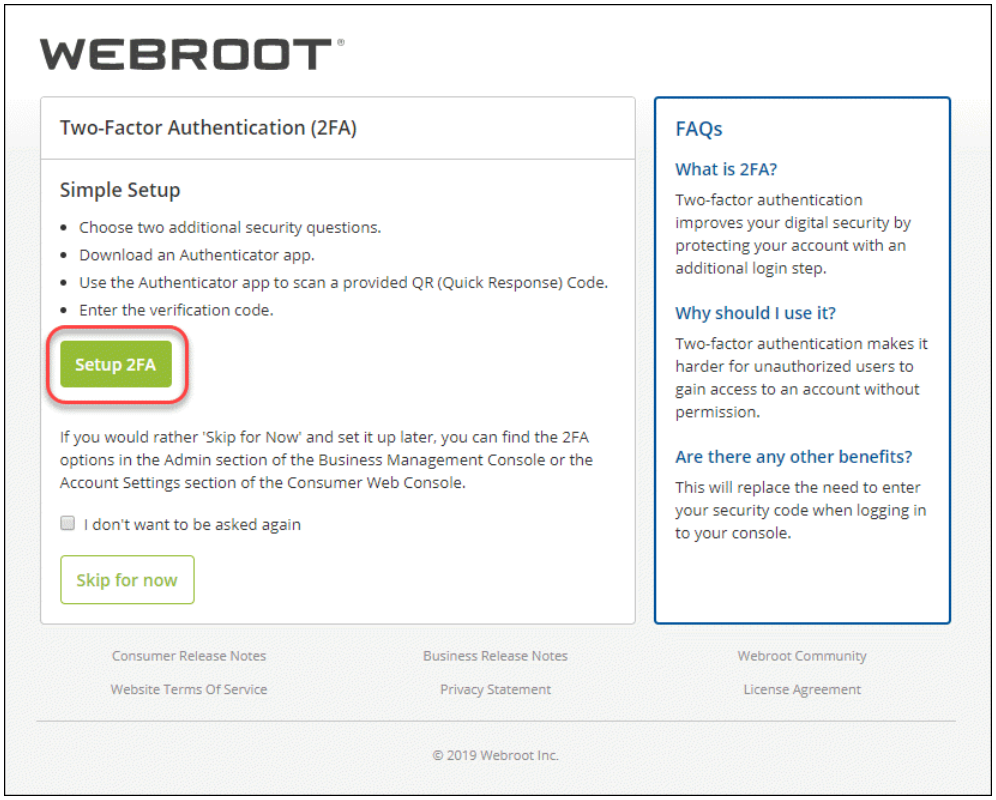
Setting up 2FA is optional. If you do not wish to use 2FA, skip ahead to Selecting your console.

System Requirements

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

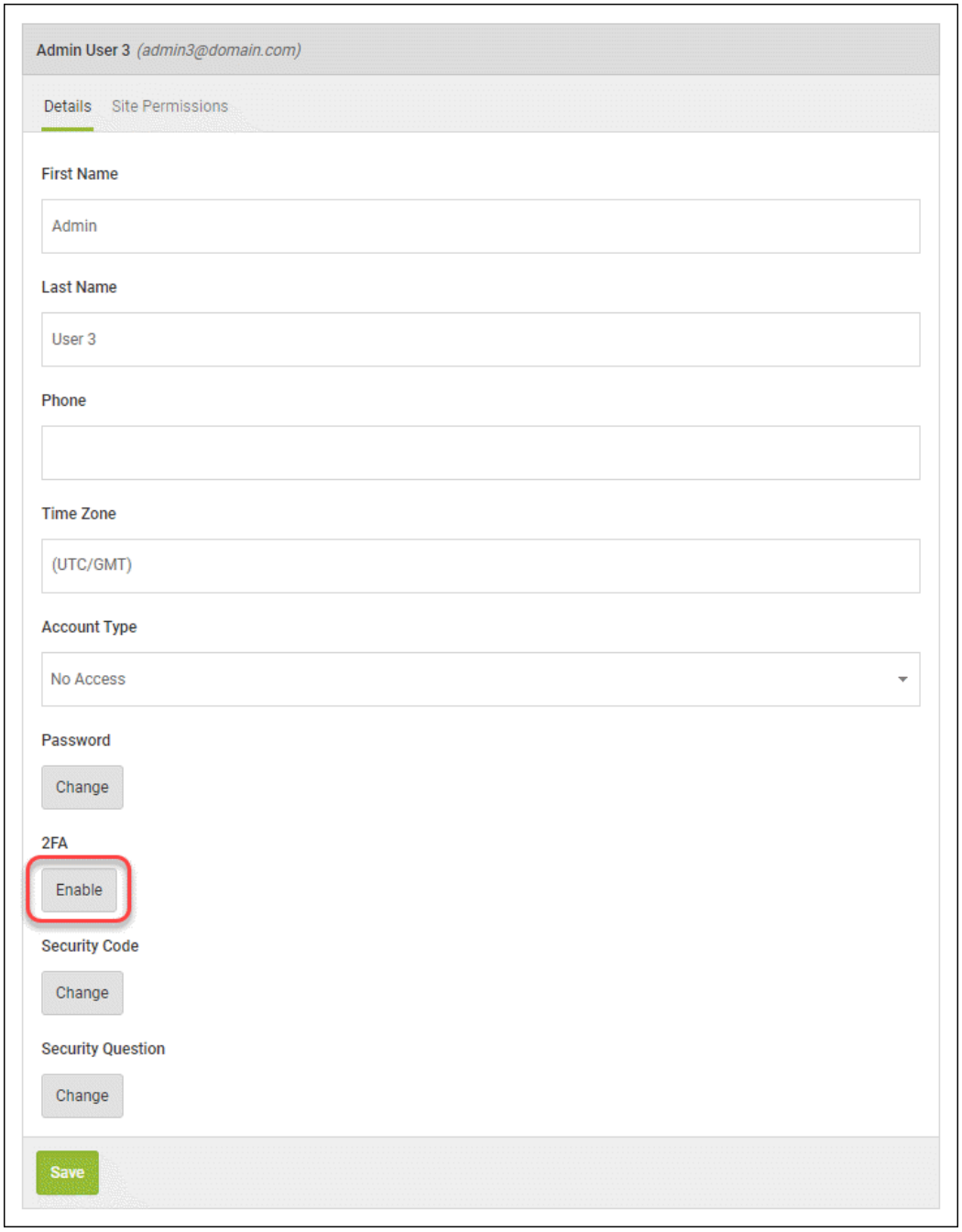
To enable 2FA

1. First, visit the Webroot Management Console, and log in using your account credentials.
2. The Setup 2FA screen will be presented. 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.

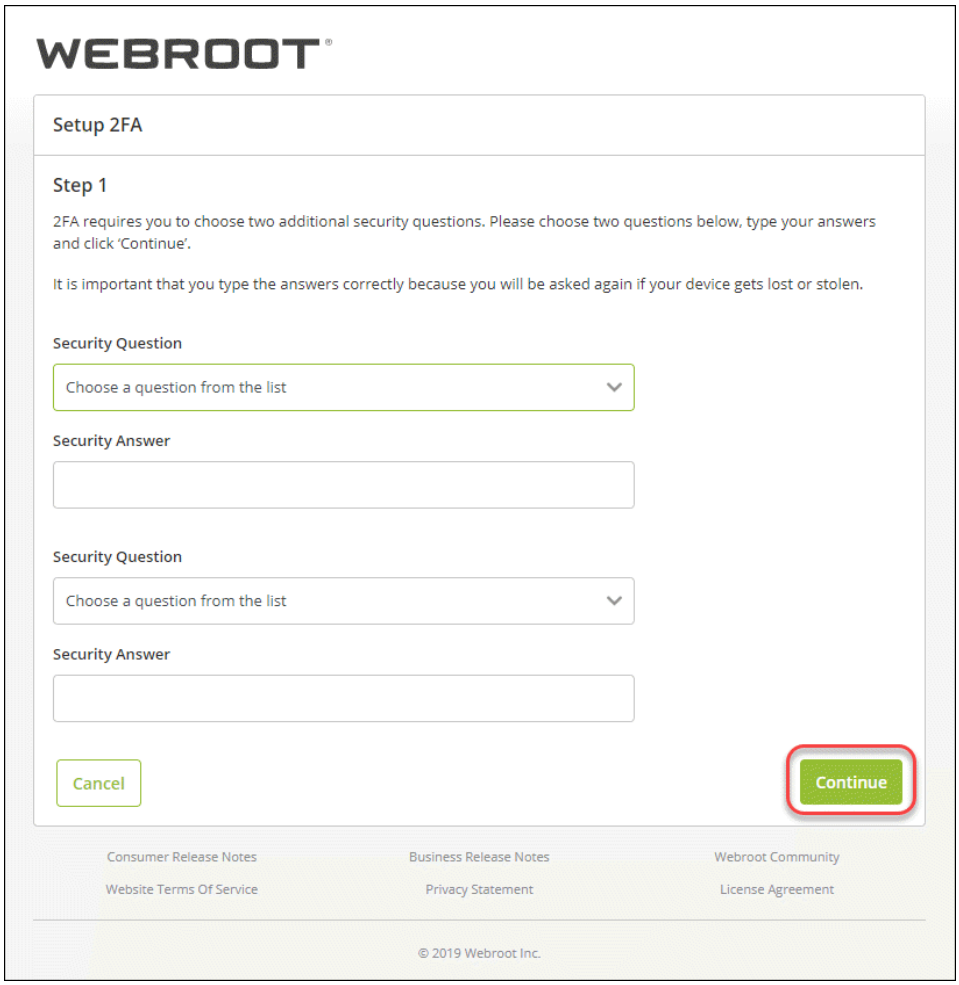


If you have already logged into the Management Console and opted to skip the 2FA setup process, click here for instructions on enabling 2FA.

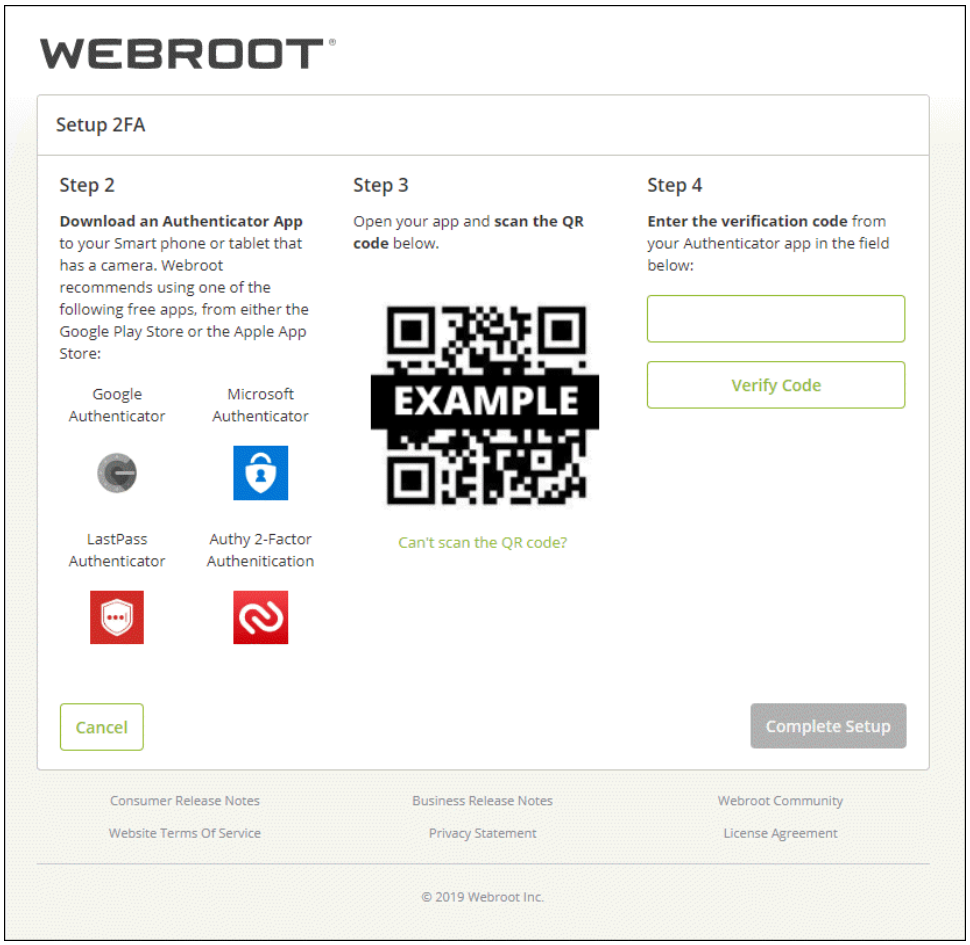
You can also start the 2FA setup process from the **Admins** tab in the Management Console by clicking your name in the Admin list which displays your details in the right panel and click **Enable**.



3. Next, the **Setup 2FA** screen displays and will prompt you to pick two security questions and provide your answers and then click **Continue**.

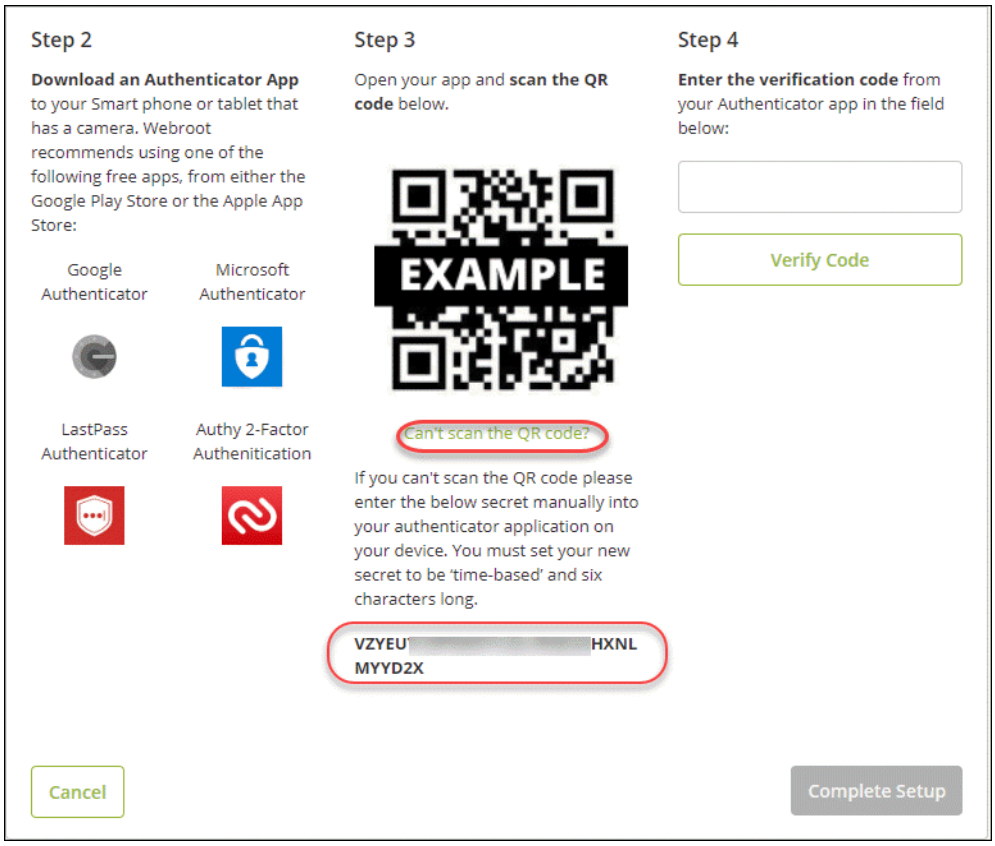


4. You will need to download and install an authenticator app from the Google Play Store or the Apple App Store to a smart phone or tablet with a working camera.

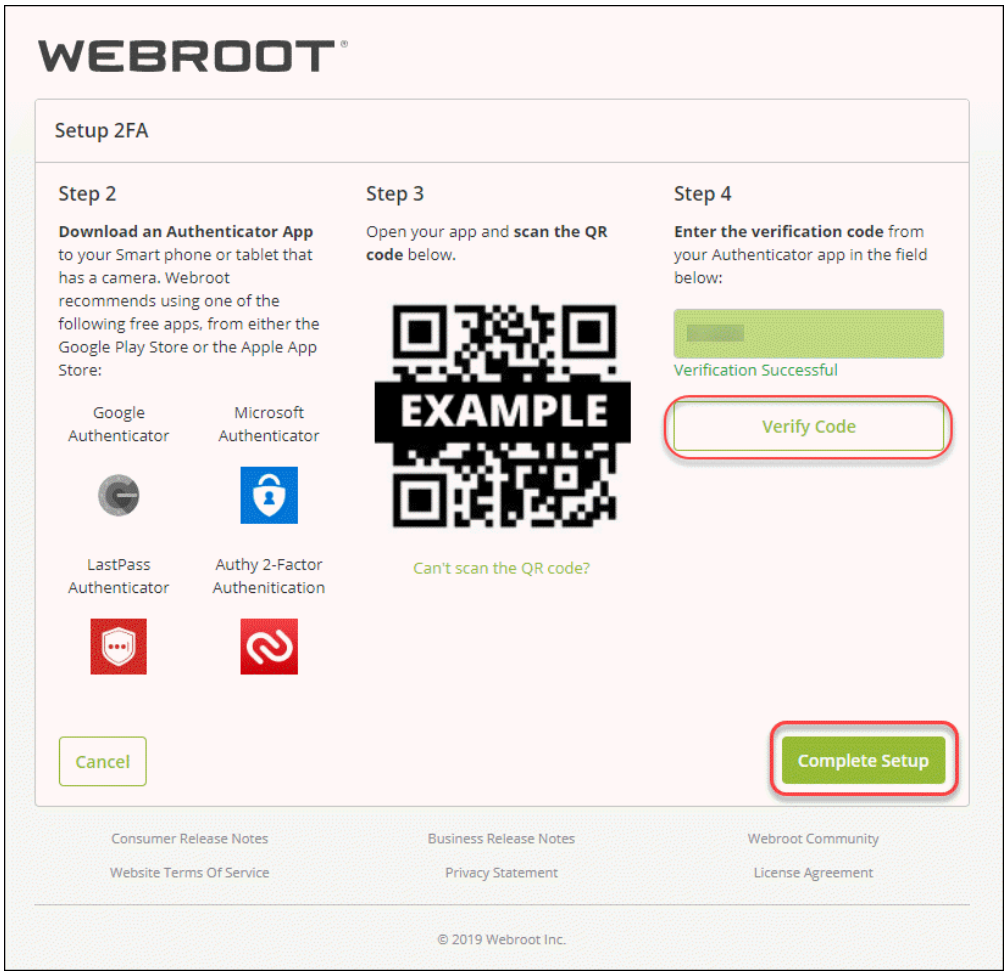


Examples of mobile authentication apps include: Google Authenticator, Microsoft Authenticator, LastPass Authenticator and Authy 2-Factor Authentication.

5. Once you have downloaded an authenticator app, open the app and follow the prompts to scan the QR code shown that is presented 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.



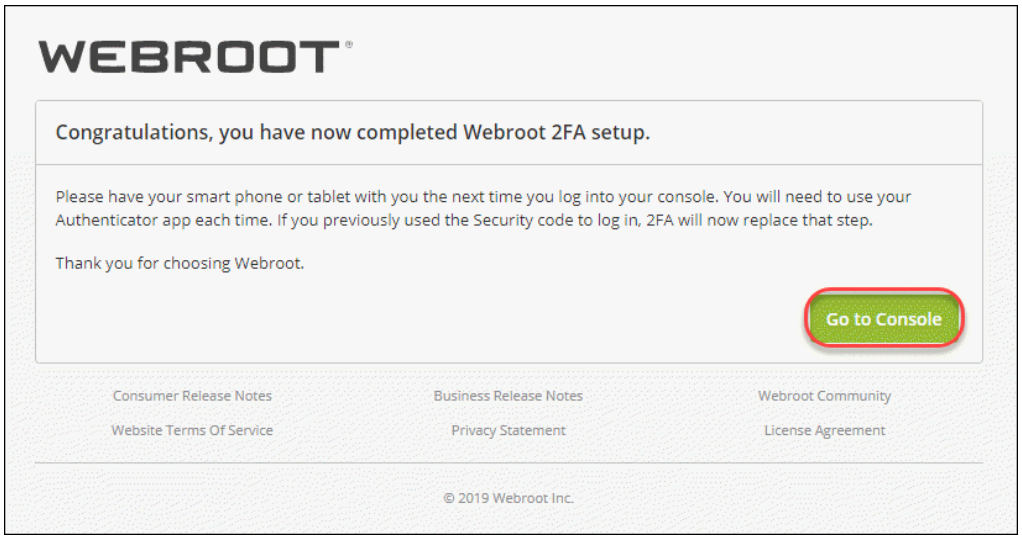
6. Enter the verification code from the authenticator app in the box under **Step 4**, and click **Verify Code**. The code will be verified, and the screen will show a Verification Successful message. Click **Complete Setup** to finish setting up 2FA.



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 2FA.

   The authenticator app will supply the authentication code you will be prompted to enter at login, which replaces the Security Code.



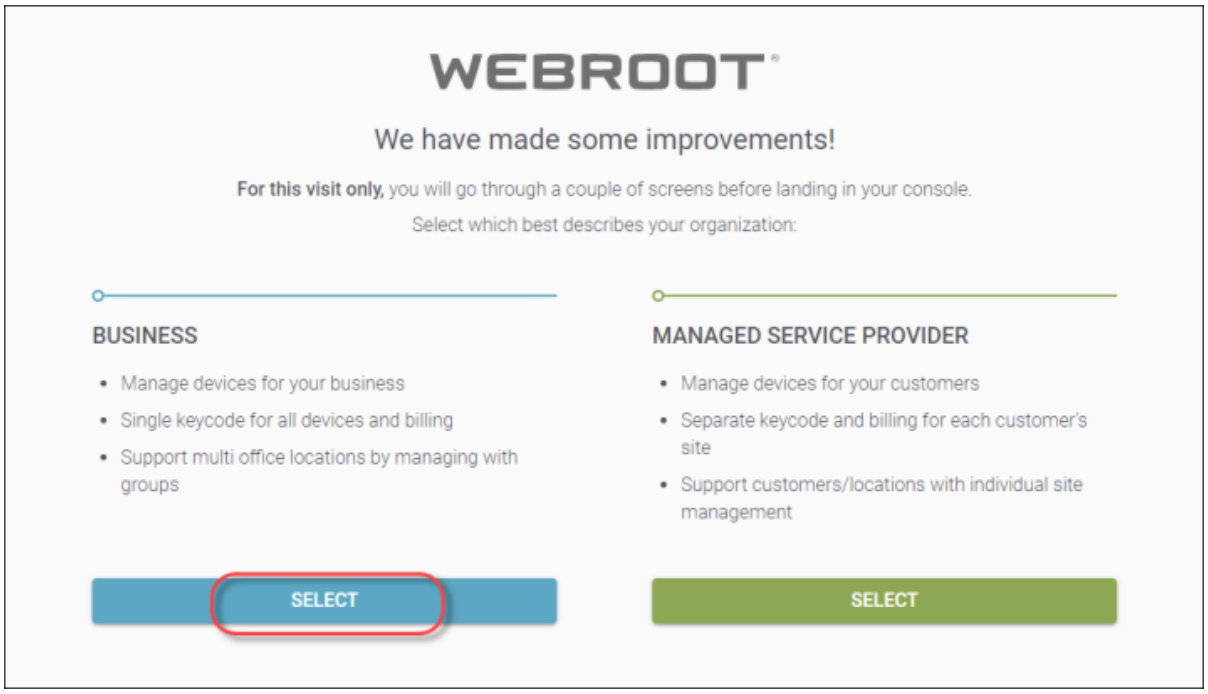
Note: The Security Code will be stored for your account and will be used if 2FA is disabled.

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

Continue to Selecting your console.

Selecting Your Console

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



Business option

The Business option will set up a management console as a single site, where you manage the security for your company. A site is used to represent a company, and under the single site business configuration, you will have a simplified view to focus only on your company's security.

If you will manage the security of other companies or clientele, you should instead refer to The first time setup of your management console in the *MSP Management Console: Getting Started Guide*.

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.

To select your console:

1. Log in to the management console, find and read the information under the business heading, and click **Select**.

   Note: If you manage devices for your customers, and have separate keycode and billing for each customer's site, select the Managed Service Provider Console. For More information, see About the Managed Service Provider Console.

Continue with Setting up your business management console.

Setting Up Your Business Management Console

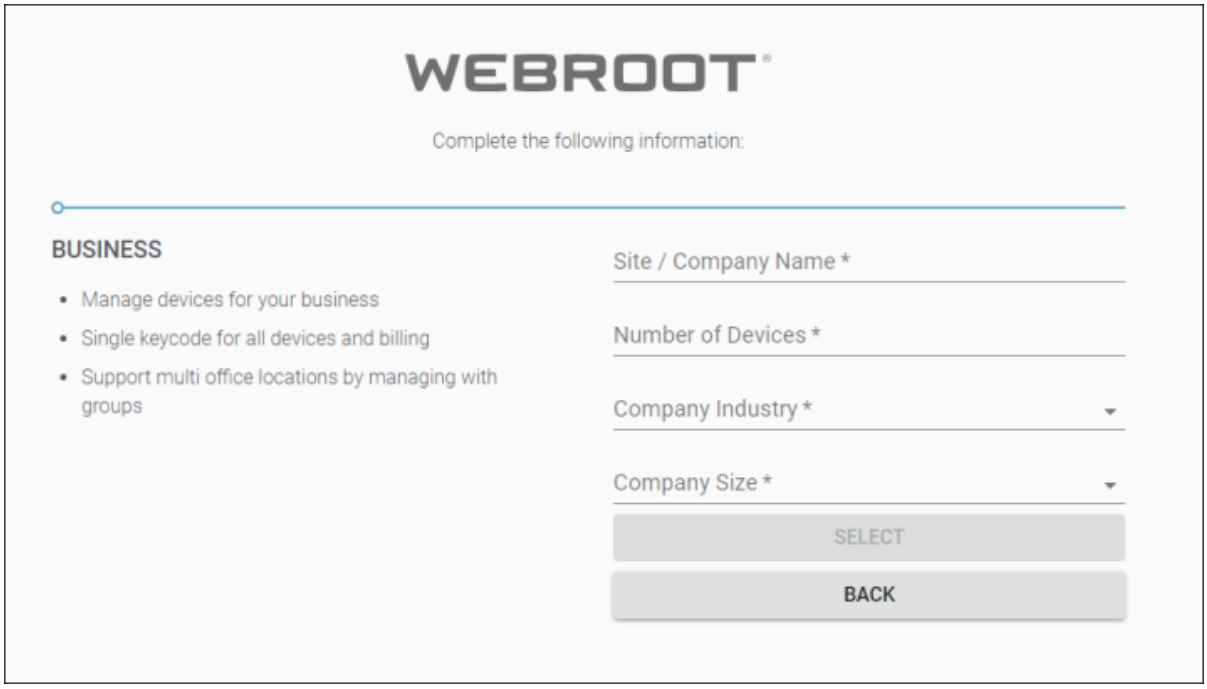
After you create an account, and select the Business Management Console, you will need to enter information about your company.

What Is The Business Management Console

The Webroot business management console is the online portal that you will use to manage the security for your Windows or Mac computers (endpoints). The console also manages the other Webroot business products if you use them.

To set up your business console:

1. After you've selected the Business Management Console, the Business information page displays.



2. In the **Site / Company Name** field, enter the site or company name.
3. In the **Number of Devices** field, enter the number of devices you manage.
4. From the **Company Industry** drop-down menu, select the type of industry that best represents your company.

5. From the **Company Size** drop-down menu, select the range that best represents the number of workers in your company.
6. When you're done, click the **Select** button.

You will be directed to the console dashboard.

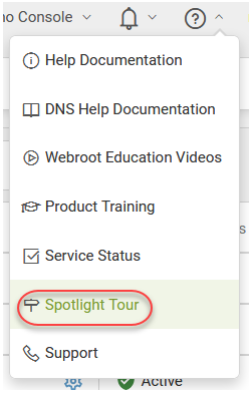
Spotlight tour

The Spotlight Tour launches when you first visit the console. The tour includes a brief description about the following:

- Dashboard
- 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. For more information see, About the Business Console Spotlight Tour.



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 deploying the Endpoint Protection agents to endpoints.

What Is An Agent?

The Webroot agent is our small piece of software that runs on your computers. The agent has a unique identity to the computer it's on, and performs security actions outside of the end user's control on behalf of the administrator using the management console.

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.

Deploying agents to endpoints

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

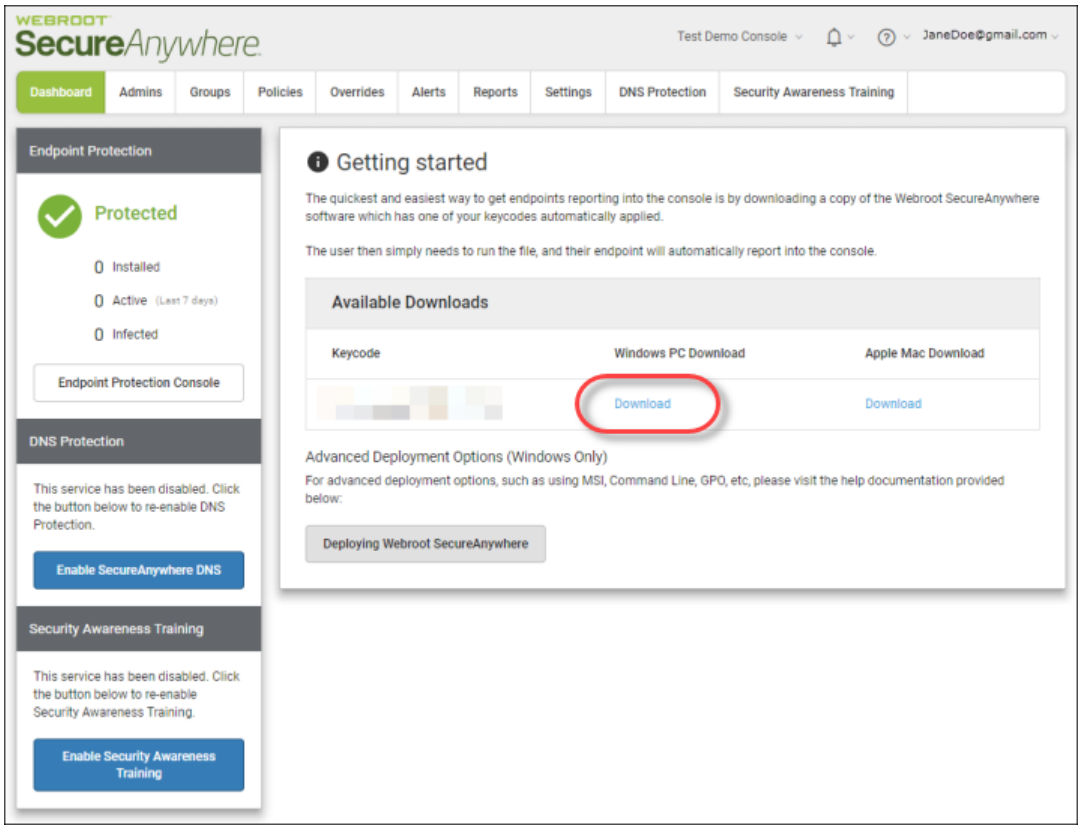
In this example, we'll manually install an agent on a Windows PC or Apple Mac.

Download a Windows or Mac agent

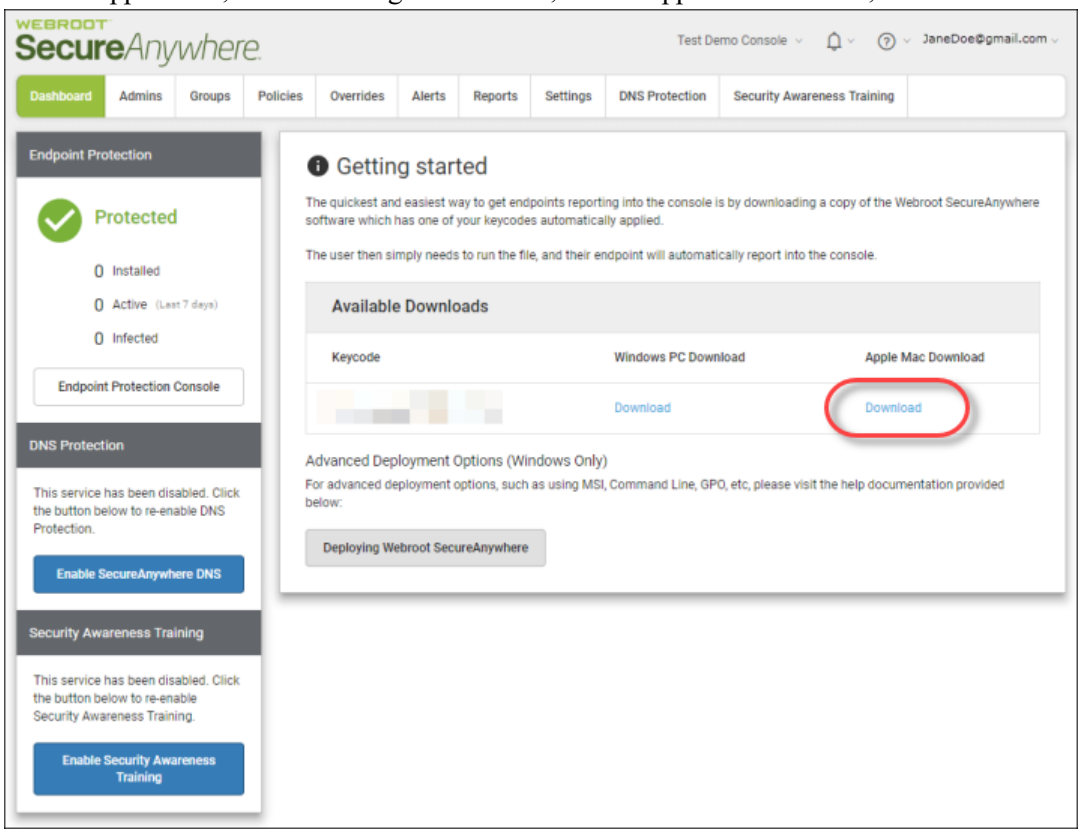
You should be logged into the console.

1. If you are not there, click the **Dashboard tab**.

2. For a Windows PC, in the Getting started area, in the Windows PC Download column, click the **Download** link.



3. For an Apple Mac, In the Getting started area, in the Apple Mac column, click the **Download** link.



The agent(s) will be in the download folder of your web browser or where you save your downloads. You will need these files to install the agent on a PC or Mac and you run the Windows file or open the Mac file to start the installation.

Manually install a Windows agent on the PC

Copy or download the Windows installation file to the PC that you want to protect. Some companies use an email with these instructions on how to install the agent. Some email is set to not allow executable files to be sent, so the file has to be compressed in a zip or other archive.

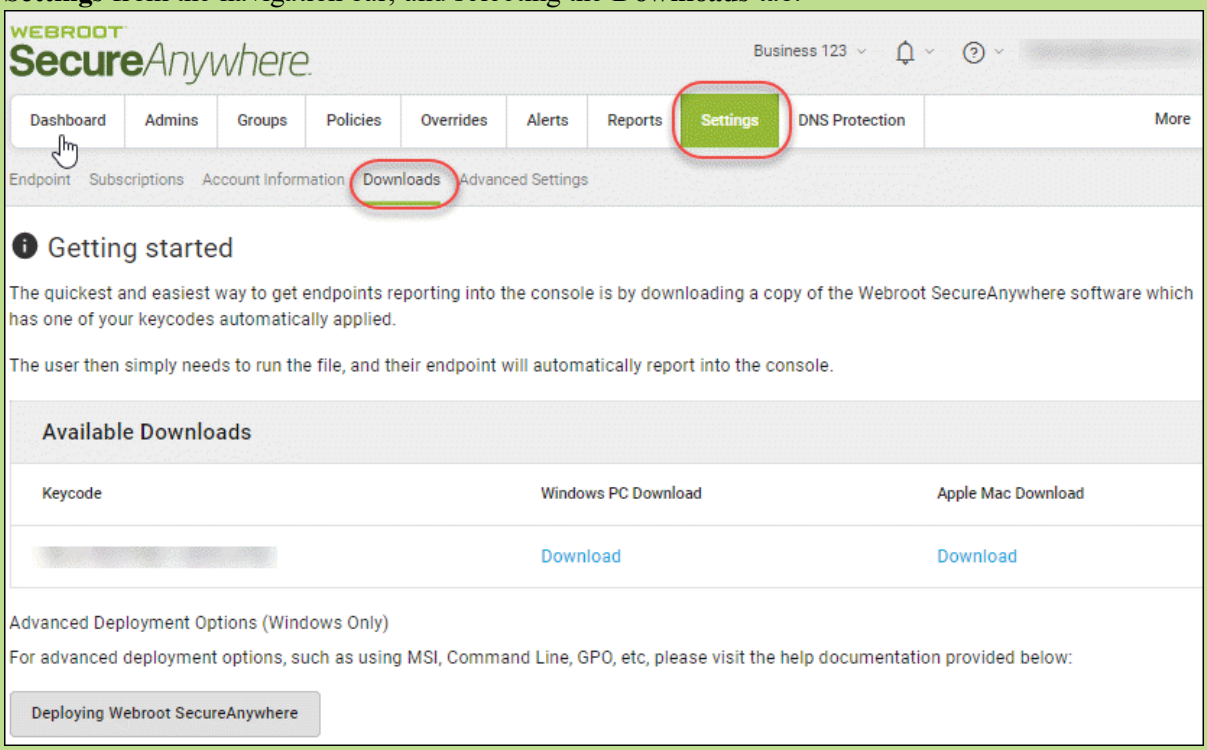
When the file is on the PC:

1. Run the .exe file to install the agent.

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

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.

Note: After your first agent installation, you can always find the deployment options by clicking **Settings** from the navigation bar, and selecting the **Downloads** tab.



Mac Agent Installation

We'll walk you through the easiest way to install the Mac agent.

Copy or download the Webroot .dmg installation file to the Mac that you want to protect. Some companies use an email with these instructions on how to install the agent. Some email is set to not allow executable files to be sent, so the file has to be compressed in a zip or other archive.

Manually install a Mac agent on the target endpoint

To install a Mac agent:

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.

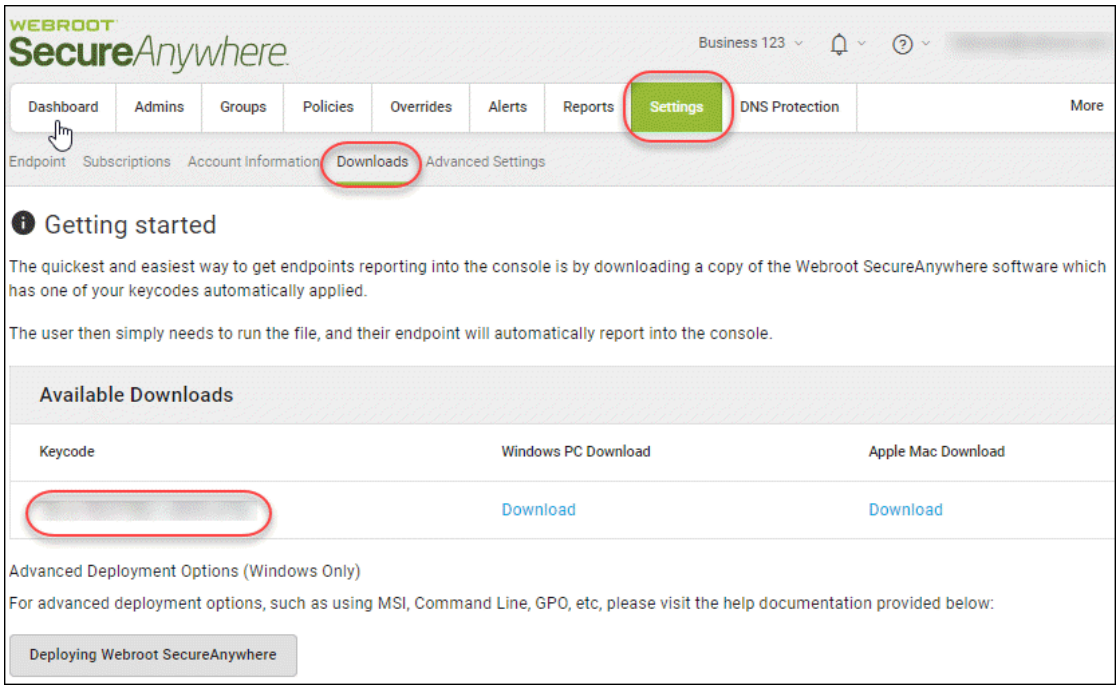
   Note: Make sure to select the correct language. You cannot change the language after you install the product.

5. In the next panel, click the **Activate** button.
6. Follow any remaining on-screen prompts to complete the installation.

   Note: After your first agent installation, you can always find the deployment options under the Resources tab in your management console view.

Finding your Keycode

If you need to find your Keycode after installing your first agent, you can always find it by clicking **Settings** from the navigation bar, and selecting the **Downloads** tab.



Continue to What's Next.

What's Next

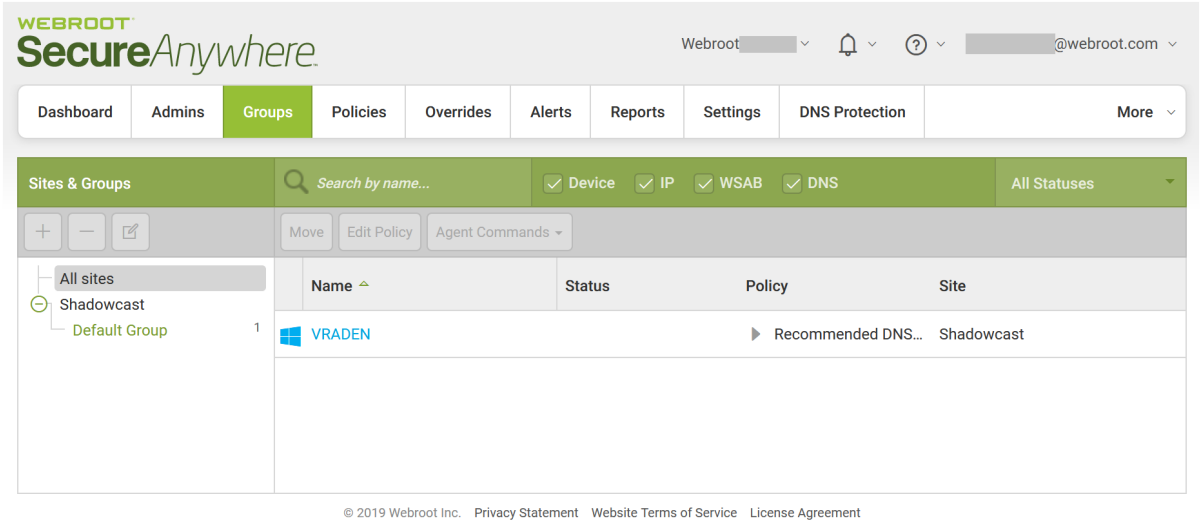
You've finished setting up your Endpoint Protection product.

- The agents should complete their first scans for threats in seconds or minutes and report back to your site.
- Webroot uses cloud-based threat detection, so you won't have to download and install any definition files. Any new threats that are identified are updated in the cloud for immediate protection for all Webroot customers.
- You can run Endpoint Protection alongside any other security products without conflicts.

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**.



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

- The Administration Guide at docs.webroot.com
- Business Endpoint Protection at The Webroot Community
- The Webroot Support Knowledge Base at answers.webroot.com