WEBROOT®

an opentext™ company

# Management Console Admin Guide

# Copyright

*GSM Admin Guide*

# Table of Contents

# Chapter 1: Global Site Manager Admin Guide

To use the Global Site Manager Admin Guide, see the following topics:

# Creating Accounts

Before you can log in to Endpoint Protection, you will need to create an account using your license keycode. Your keycode will be included in the activation and setup instruction email.

**To create an account:**

1. Log into the SecureAnywhere Management Console. On the login page, click the **Create Account** button.

2. Populate the fields using the information in the following table as a reference.

| FIELD | DESCRIPTION |
|---|---|
| **Webroot Product Keycode** | Enter the license keycode you received when you purchased Endpoint Protection. |
| **Email Address** | Enter the email address for the administrator who will manage Endpoint Protection.<br>The account activation confirmation is sent to this email address, which is also the username for logging in to the Management Portal. |
| **Password** | Enter a minimum of nine characters. Your password must contain at least six alphabetic characters and three numeric characters. Your password can be longer than the required nine characters. It can include special characters, except for the angle brackets: < >. Your password is case sensitive.<br>As you type, the Strength meter displays how secure your password is. For optimum security, it's a good idea to make your password as strong as possible. |
| **Your Personal Security Code** | Enter a word or number, which will be used for an extra security step after you enter the password during login. Pick a code that is easy to remember, using a minimum of six characters.<br>Every time you log in, the Management Portal prompts you to enter two random characters of this code. For example, if your code is *123456* and the system prompts you for the fourth and sixth character, you would enter 4 and 6. Your Personal Security Code is case sensitive. |

| FIELD | DESCRIPTION |
|---|---|
| **Security Question** | Select a question from the drop-down list.<br>If you forget details of your login later, you will need to provide the answer to this question to retrieve the information. |
| **Security Answer** | Type an answer to your security question. The Security Answer is case-sensitive. |

3. After you enter your account details, click the **Register Now** button.

   SecureAnywhere displays a confirmation message and sends an email to the email address you specified.

4. Open your email application, and click the link in the confirmation email message.

   When the SecureAnywhere Registration Confirmation page opens, enter the two randomly selected characters of the security code you specified when you created the account.

5. Click **Confirm Registration Now**.

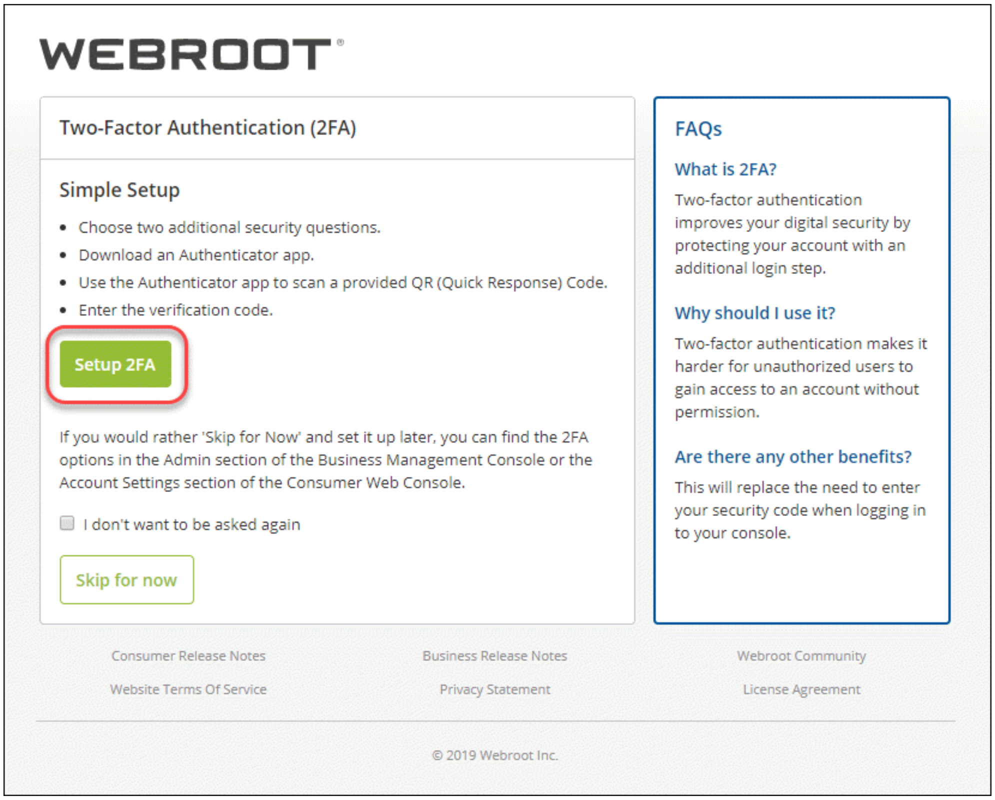
   After entering your security code, you will be presented with options about setting up two-factor authentication (2FA), for more information see *Enabling two-factor authentication (2FA) on page 5*.

# Enabling two-factor authentication (2FA)

Webroot SecureAnywhere allows users to enable 2-factor authentication (2FA) to help prevent unauthorized users from gaining access to your account without permission.

**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.



Two-Factor Authentication (2FA)

Simple Setup

- Choose two additional security questions.
- Download an Authenticator app.
- Use the Authenticator app to scan a provided QR (Quick Response) Code.
- Enter the verification code.

If you would rather 'Skip for Now' and set it up later, you can find the 2FA options in the Admin section of the Business Management Console or the Account Settings section of the Consumer Web Console.

□ I don't want to be asked again

FAQs

What is 2FA?

Two-factor authentication improves your digital security by protecting your account with an additional login step.

Why should I use it?

Two-factor authentication makes it harder for unauthorized users to gain access to an account without permission.

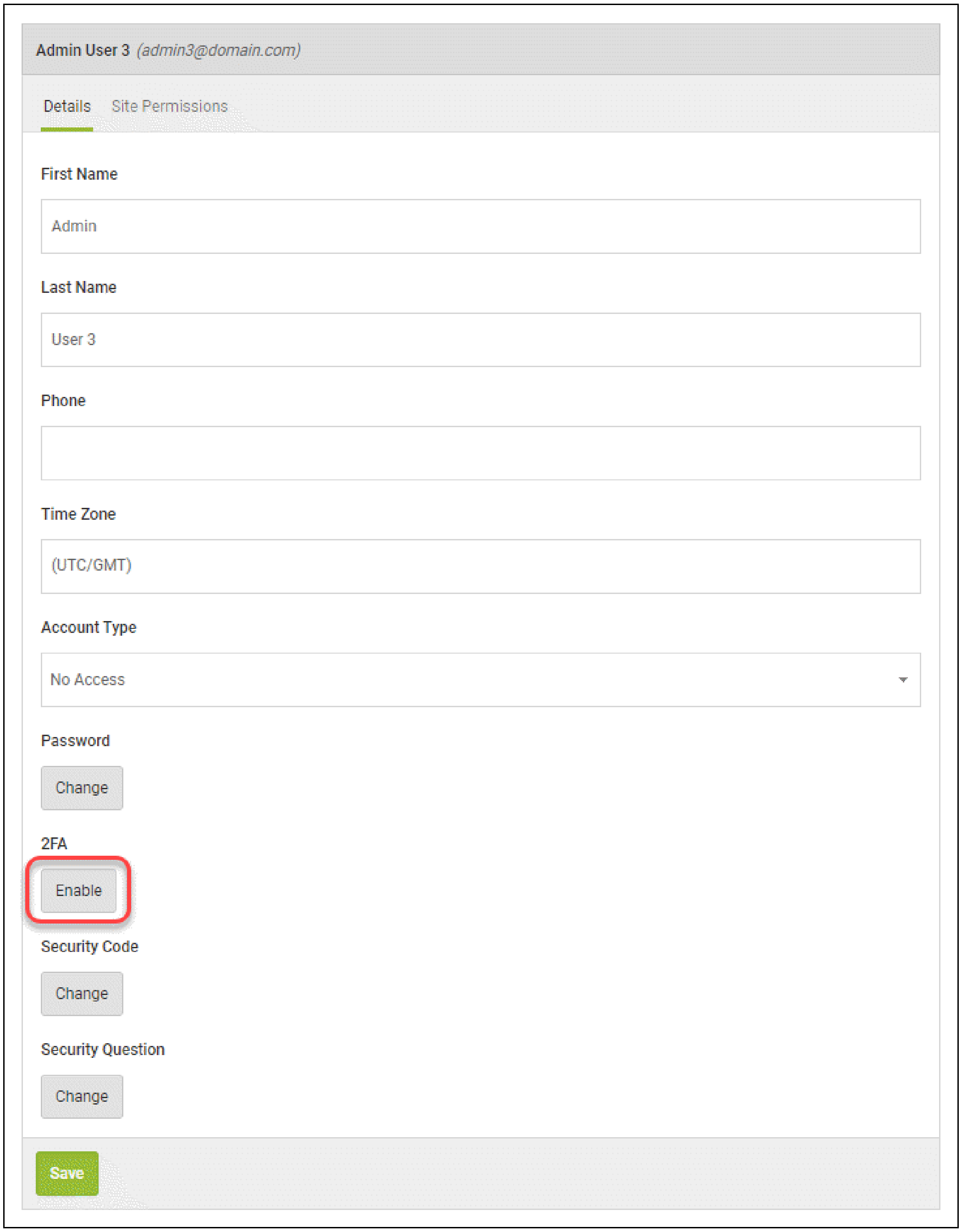
Are there any other benefits?

This will replace the need to enter your security code when logging in to your console.

© 2019 Webroot Inc.

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

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**.



Admin User 3 *(admin3@domain.com)*

First Name: Admin

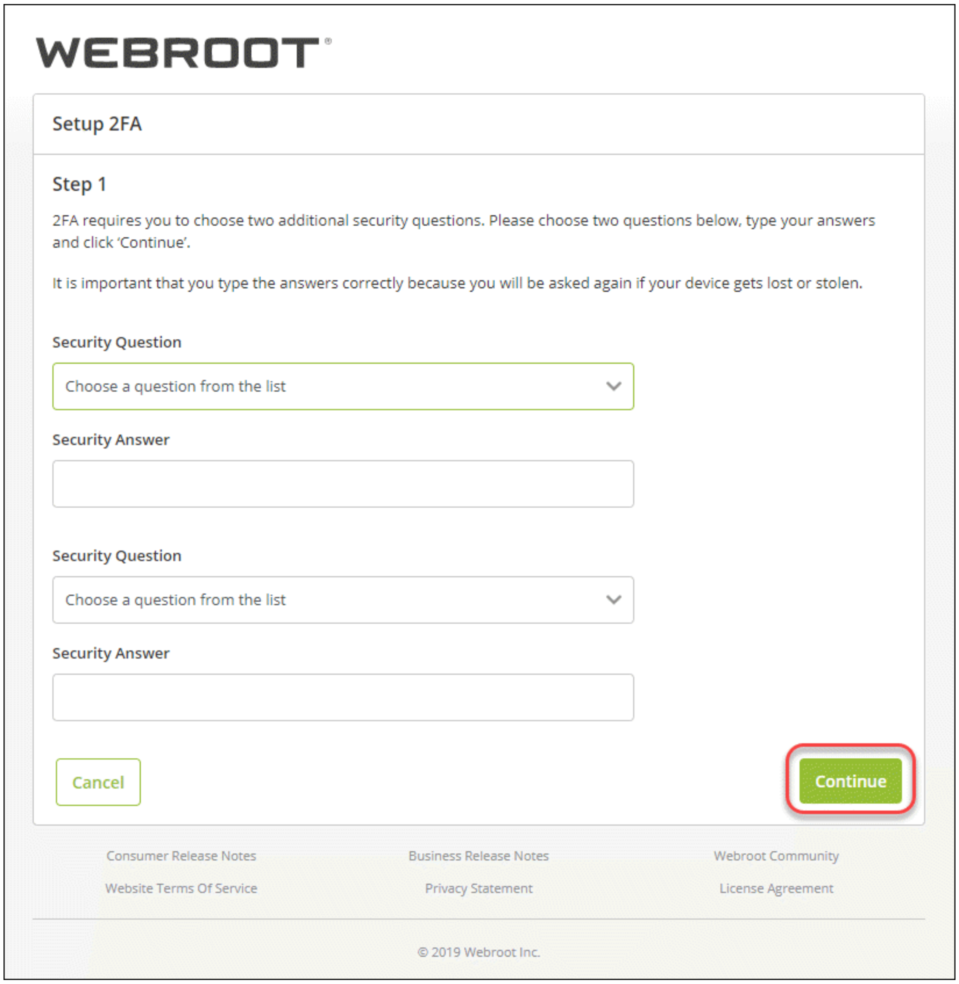
Last Name: User 3

Phone:

Time Zone: (UTC/GMT)

Account Type: No Access

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



Setup 2FA

Step 1

2FA requires you to choose two additional security questions. Please choose two questions below, type your answers and click 'Continue'.

It is important that you type the answers correctly because you will be asked again if your device gets lost or stolen.

Security Question

Choose a question from the list

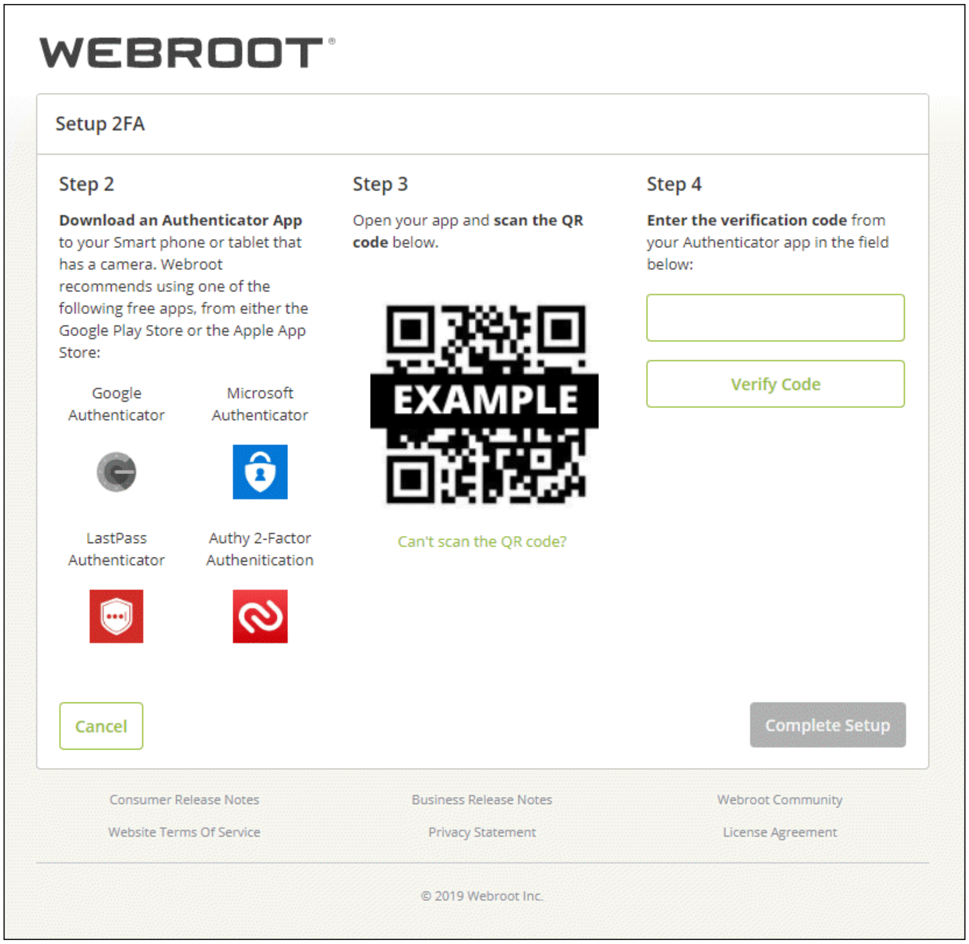
Security Answer

Security Question

Choose a question from the list

Security Answer

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.



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:

Step 3

Open your app and **scan the QR code** below.

Step 4

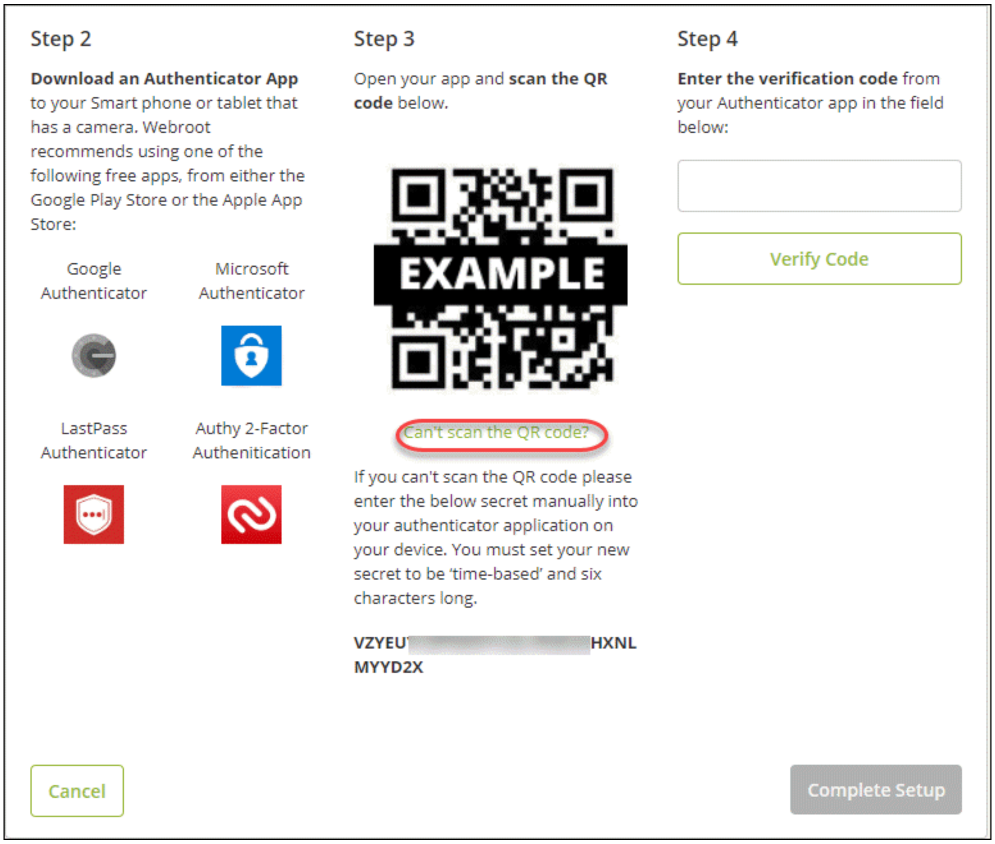
**Enter the verification code** from your Authenticator app in the field below:

Examples of mobile authentication apps include:

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

5. Once you have downloaded an authenticator app, open the app, and follow the prompts to enable the app to access the camera on your smartphone, so you can scan the QR code shown that is presented in the Management Console. If you are unable to scan the QR code, try turning up the brightness on your display, or 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.



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:

Step 3

Open your app and **scan the QR code** below.

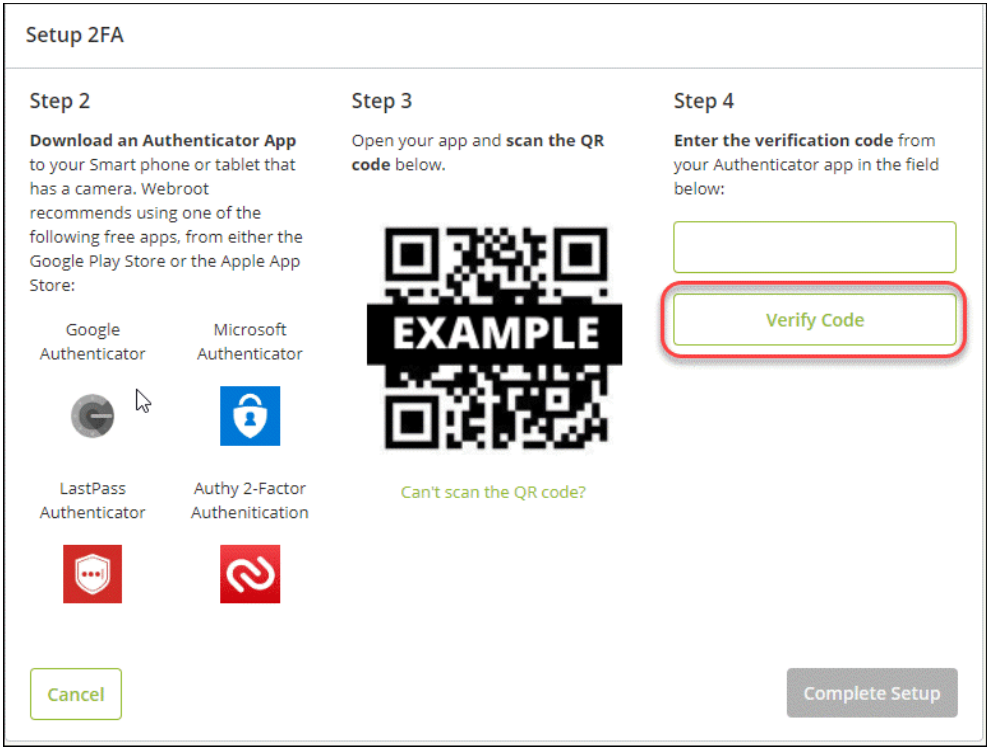
If you can't scan the QR code please enter the below secret manually into your authenticator application on your device. You must set your new secret to be 'time-based' and six characters long.

**VZYEU[redacted]HXNL MYYD2X**

Step 4

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

6. Enter the verification code from the authenticator app in the box under **Step 4**, and click **Verify Code**.



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:

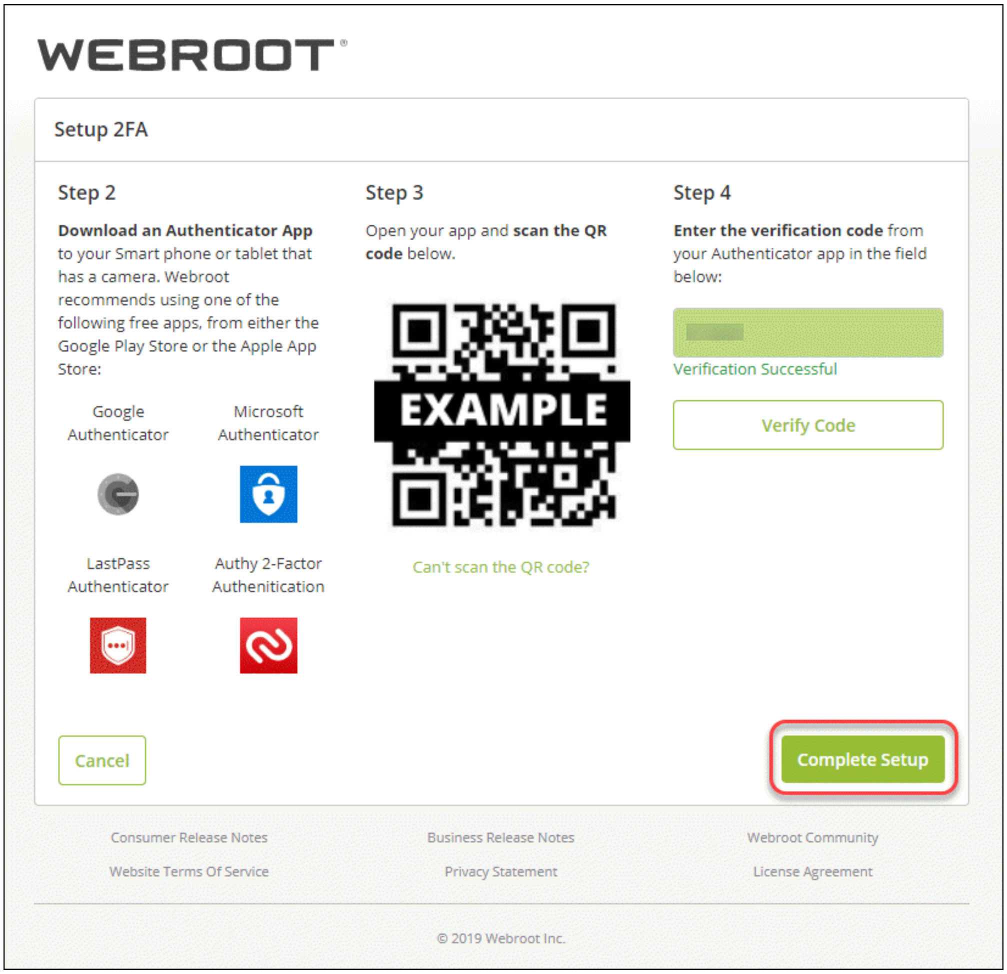
Step 3

Open your app and **scan the QR code** below.

Step 4

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

7. The code will be verified, and the screen will show a Verification Successful message. Click **Complete Setup** to finish setting up 2FA.



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:

Step 3

Open your app and **scan the QR code** below.

Step 4

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

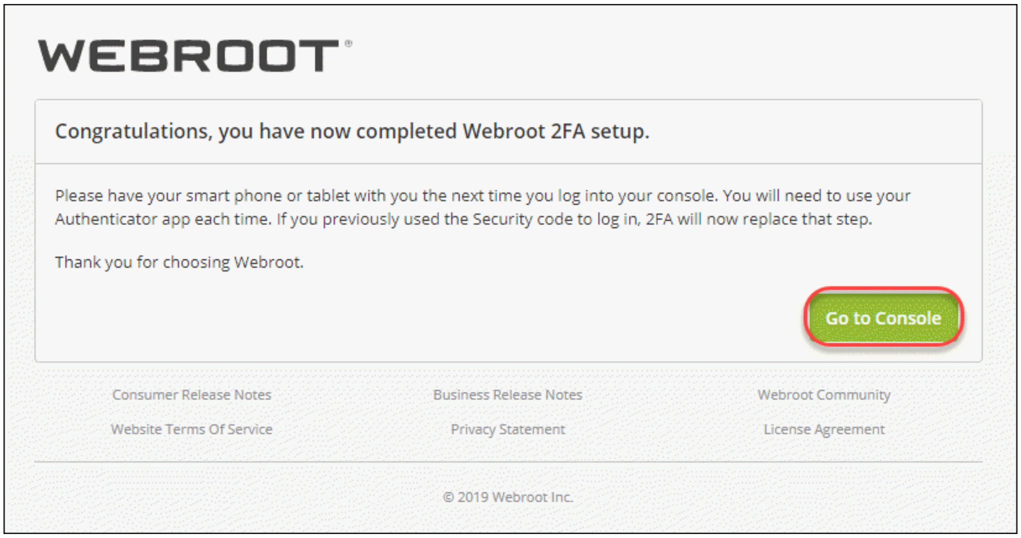
[redacted]

Verification Successful

> **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**.

8. 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.



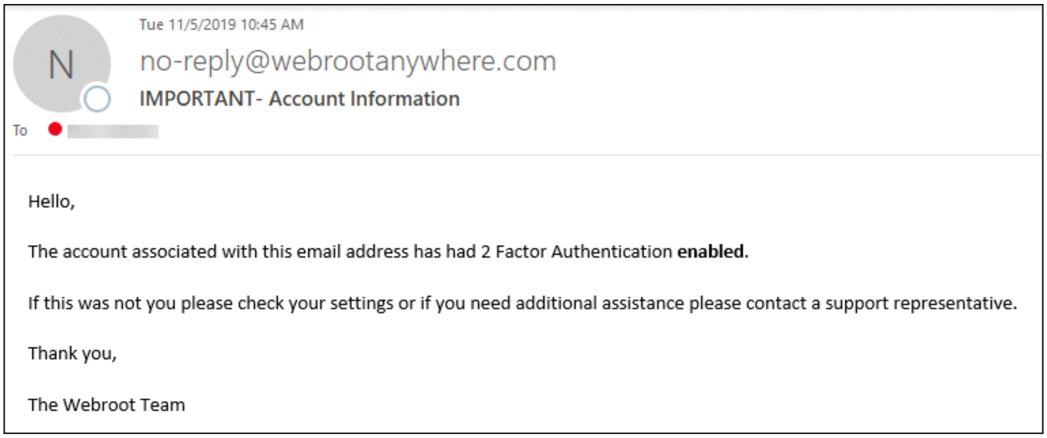
Congratulations, you have now completed Webroot 2FA setup.

Please have your smart phone or tablet with you the next time you log into your console. You will need to use your Authenticator app each time. If you previously used the Security code to log in, 2FA will now replace that step.

Thank you for choosing Webroot.

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

9. An email from no-reply@webrootanywhere.com will be sent to you informing you that 2FA has been enabled for your account.



Tue 11/5/2019 10:45 AM

no-reply@webrootanywhere.com

IMPORTANT- Account Information

To ● [redacted]

Hello,

The account associated with this email address has had 2 Factor Authentication **enabled.**

If this was not you please check your settings or if you need additional assistance please contact a support representative.

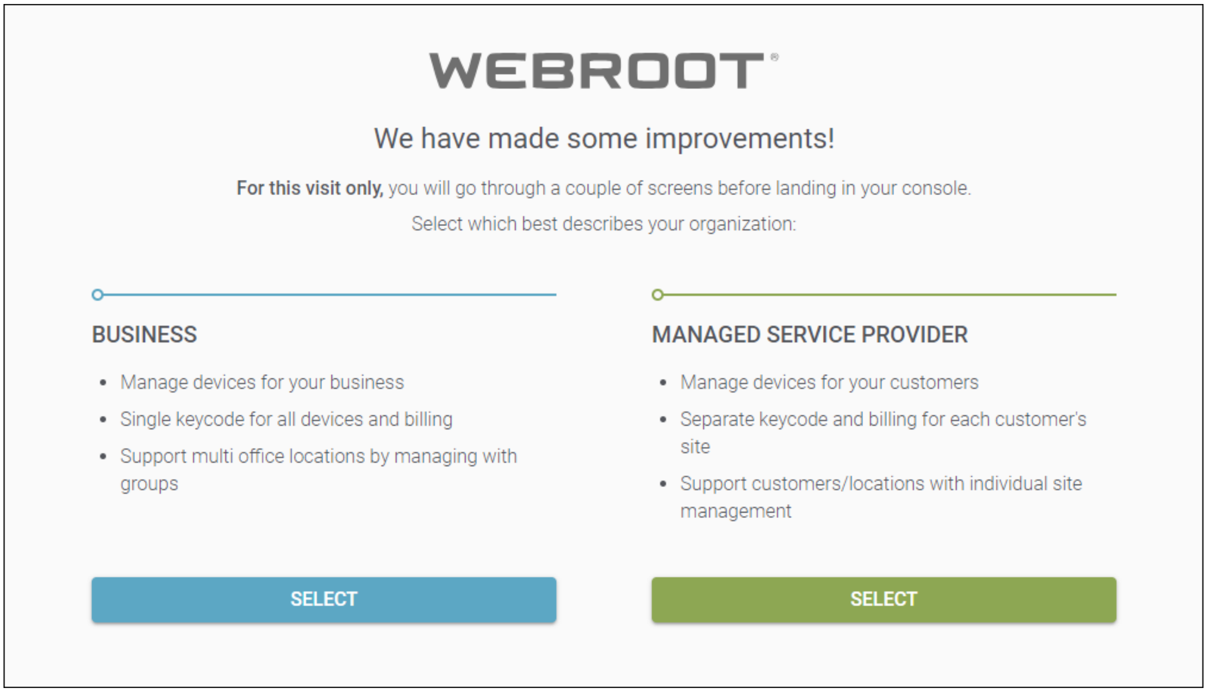
Thank you,

The Webroot Team

Continue with *Selecting Your Console on page 13*.

# Selecting Your Console

When you sign into the console for the first time, you will need to select one of the following site configurations.



WEBROOT

We have made some improvements!

**For this visit only,** you will go through a couple of screens before landing in your console.

Select which best describes your organization:

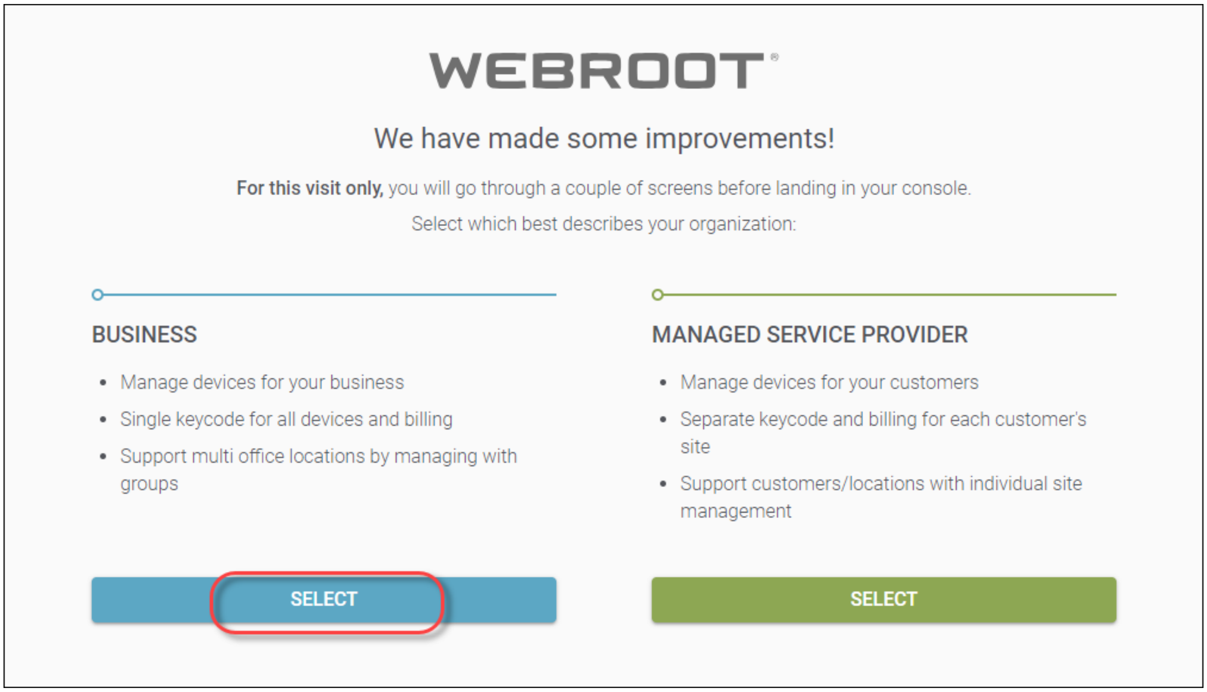
BUSINESS

- Manage devices for your business
- Single keycode for all devices and billing
- Support multi office locations by managing with groups

MANAGED SERVICE PROVIDER

- Manage devices for your customers
- Separate keycode and billing for each customer's site
- Support customers/locations with individual site management

- If you manage devices for your business, and have a single keycode for all devices and billing, select the Business Console. For more information, see *About The Business Console on page 19*.



We have made some improvements!

**For this visit only,** you will go through a couple of screens before landing in your console.

Select which best describes your organization:

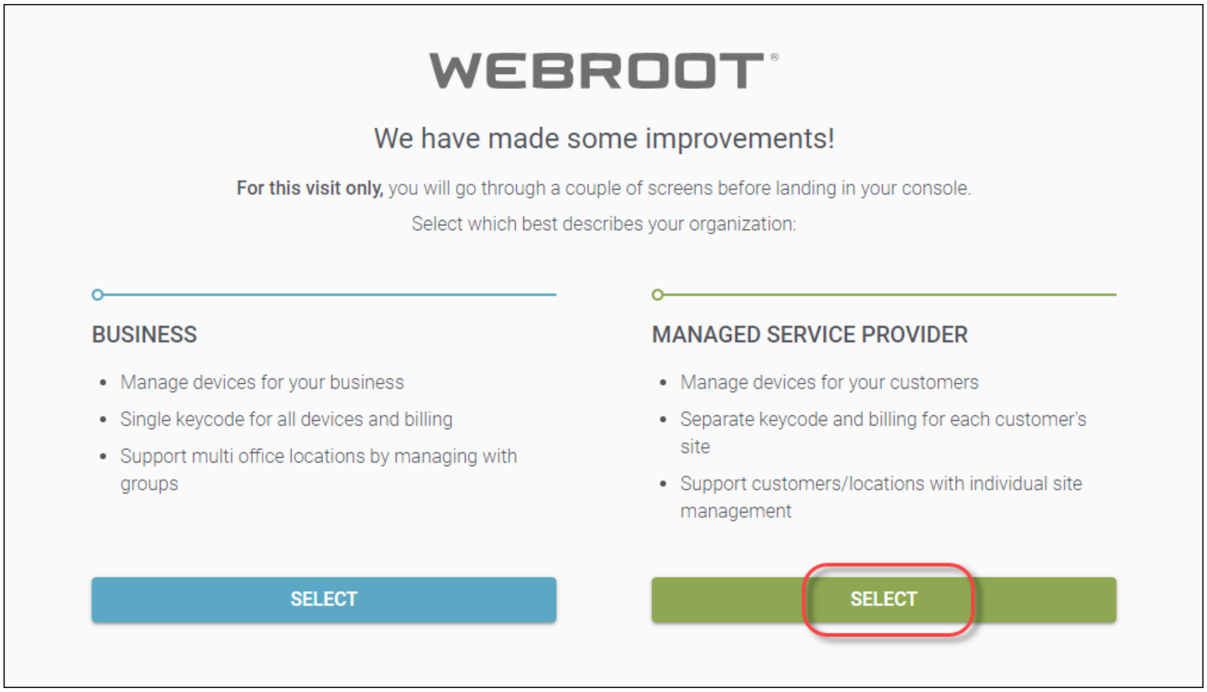
BUSINESS

- Manage devices for your business
- Single keycode for all devices and billing
- Support multi office locations by managing with groups

MANAGED SERVICE PROVIDER

- Manage devices for your customers
- Separate keycode and billing for each customer's site
- Support customers/locations with individual site management

- 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 on page 16*.



WEBROOT

We have made some improvements!

**For this visit only,** you will go through a couple of screens before landing in your console.

Select which best describes your organization:

BUSINESS

- Manage devices for your business
- Single keycode for all devices and billing
- Support multi office locations by managing with groups

MANAGED SERVICE PROVIDER

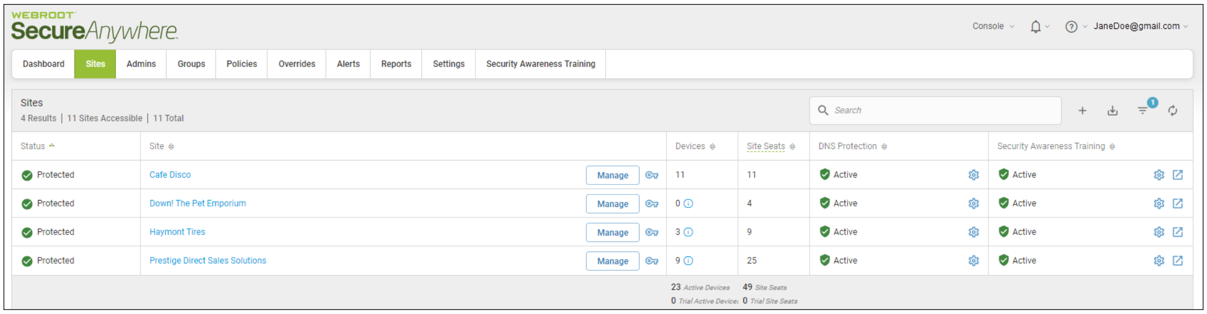
- Manage devices for your customers
- Separate keycode and billing for each customer's site
- Support customers/locations with individual site management

# About the Managed Service Provider Console

The Managed Service Provider (MSP) console is very similar to the previous version of the console. You will still experience the same look and feel, and be able to perform the same tasks. Those tasks are described in this Admin Guide.

The following tabs can be accessed from the main console:

- **Dashboard** — Displays various charts that give you a visual interpretation of your endpoints. From here you can create and drill down into charts, as well as delete charts.
- **Sites** — Displays a list of your sites with information about number of seats, settings, etc. You can click the More info drop-down menu to display more information about your sites. For more information, see the *Management Console Sites Tab Overview on page 69*.
- **Admins** — Displays a list of admins, and you can drill down to access information about their permission levels for various sites. For more information, see the Working With Admins section.
- **Groups** — Allows you to add, edit, delete and work with groups.
- **Policies** — Allows you to create, copy, edit, and rename policies.
- **Overrides** — Allows you to create, customize, and import overrides.
- **Alerts** — Allows you to create alerts at the global level.
- **Reports** — Allows you to run reports on the health and performance of sites.
- **Settings** — Allows you to view account information, create API client credentials, and set data filters.

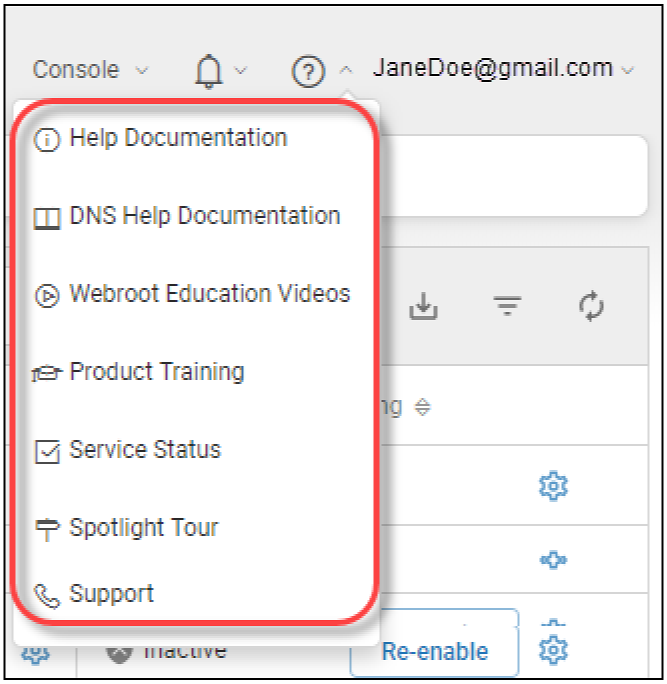


Sites
4 Results | 11 Sites Accessible | 11 Total

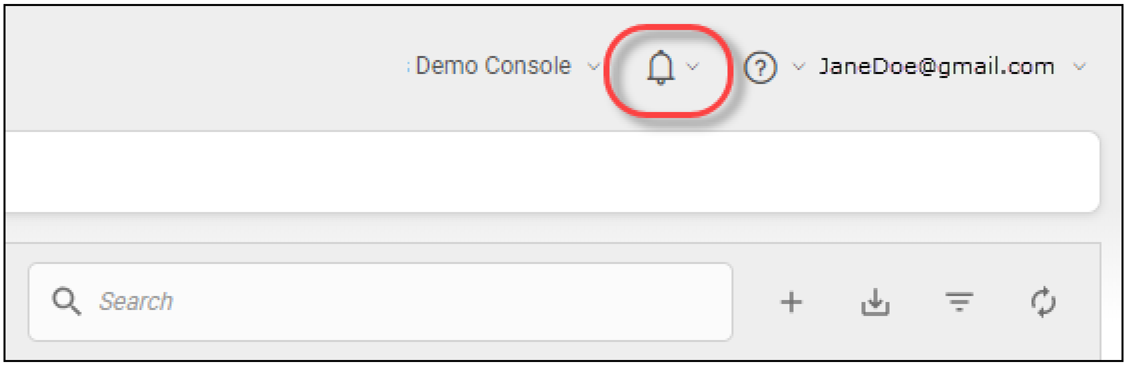
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

- For additional information, from the **Question Mark (?)** icon in the upper right corner, click the **Down Arrow** to access any of the following:
  - Help Documentation — In most cases, the help that displays relates to the panel or window you are working in.
  - DNS Help Documentation — Displays the business documentation portal where you can access DNS Protection guides.

- Webroot Education Videos — Displays a playlist of Webroot videos.
- Service Status — Displays the status page for your console, where you can view the status of your products and systems.
- Spotlight Tour — Allows you to view the Spotlight Tour, which is a quick tour through the console. For more information, see *About the Spotlight Tour on page 22*.
- Support — Click the link to enter a help ticket. For more information see Accessing Technical Support.



- To review any alerts or notifications, from the Alert Bell icon in the upper right corner, click the **Down Arrow**.



# About The Business Console

The Business console is designed for customers with the following characteristics:

- You manage devices for your business.
- You have a single keycode for all devices and billing.
- You support multi-office locations by managing with groups.

If you have selected the Business console:

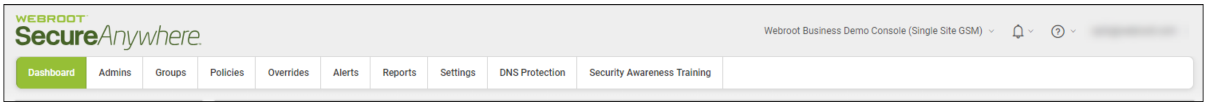
- You will need to enter information about your business. For more information, see *Setting Up Your Business Console on page 579*
- You will be presented with the opportunity to take the Spotlight Tour, which you can opt out of and take another time. For more information, se e *About the Spotlight Tour on page 22*.

The Business Console has different tabs and functionality than the standard console, and is geared to single-site businesses, and allows you to easily manage your devices.

The following tabs and functionality can be accessed from the Business Console:

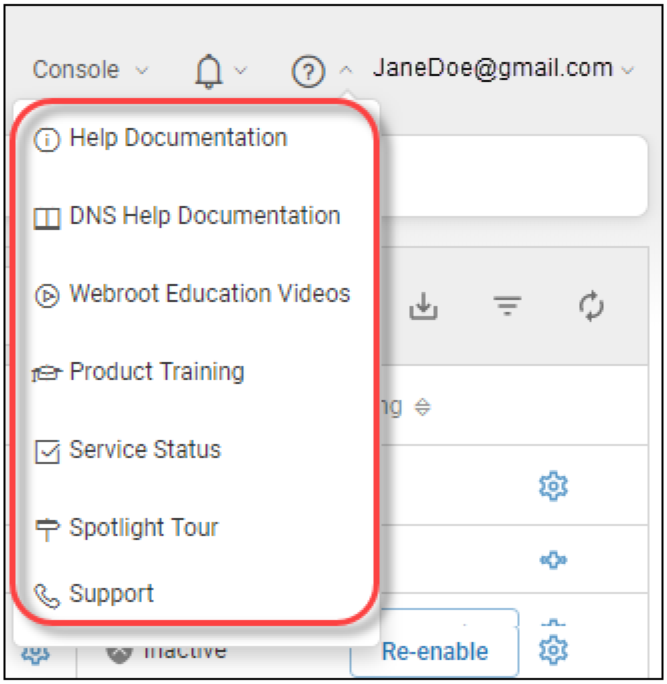
- **Dashboard** — Displays various charts that give you a visual interpretation of your endpoints. From here you can review charts that contain information about the status of your endpoints. For more information, see About the Business Dashboard Tab. Additionally, you can sign up for a free trial of either DNS Protection or Security awareness Training.
- **Admins** — Displays a list of admins, and you can drill down to access information about their permission levels for various sites. For more information, see the Working With Admins section.
- **Groups** — Allows you to add, edit, delete and work with groups. For more information see the Working With Groups section.
- **Policies** — Allows you to create, copy, edit, and rename policies. For more information, see the Working With Policies section.
- **Overrides** — Allows you to create, customize, and import overrides. For more information, see the Working With Overrides section.
- **Alerts** — Allows you to create alerts at the global level. For more information, see the Working With Alerts section.
- **Reports** — Allows you to run reports on the health and performance of products. For more information, see the Working With Reports section.

- **Settings** — Allows you to view and edit account information and advanced settings. For more information see *Viewing and Editing Company Information on page 588* and *Viewing and Editing Advanced Settings on page 590*.
- **DNS Protection** — Displays information about Security Awareness Training and allows you to sign up for a free trial. For more information, see *DNS Protection Trial on page 598*.
- **Security Awareness** — Displays information about Security Awareness Training and allows you to sign up for a free trial. For more information, see *Security Awareness Training Trial on page 603*.

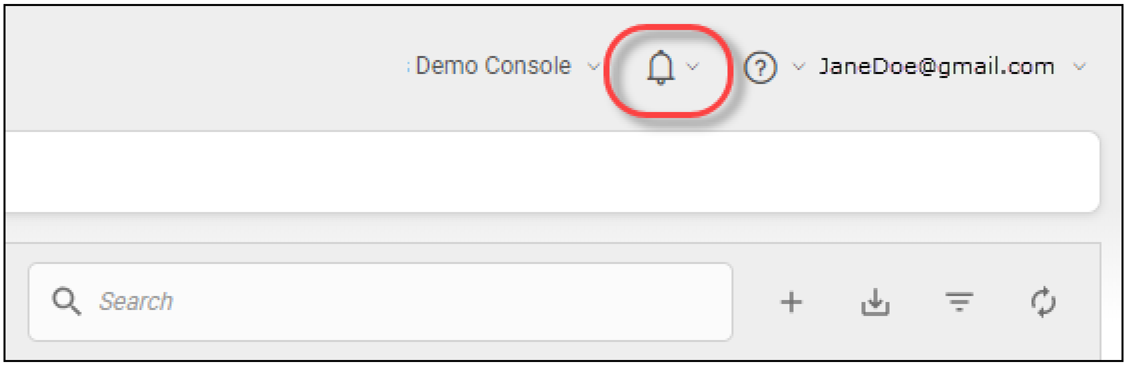


- For additional information, from the Help (?) icon in the upper right corner, click the **Down Arrow** to access any of the following:
  - Help Documentation — In most cases, the help that displays relates to the panel or window you are working in.
  - DNS Help Documentation — Displays the business documentation portal where you can access DNS Protection guides.
  - Webroot Education Videos — Displays a playlist of Webroot videos.
  - Service Status — Displays the status page for your console, where you can view the status of your products and systems.
  - Spotlight Tour — Allows you to view the Spotlight Tour, which is a quick tour through the console. For more information, see *About the Spotlight Tour on page 22*.

- Support — Click the link to enter a help ticket. For more information see Accessing Technical Support.



- To review any alerts or notifications, from the Alert Bell icon in the upper right corner, click the **Down Arrow**.



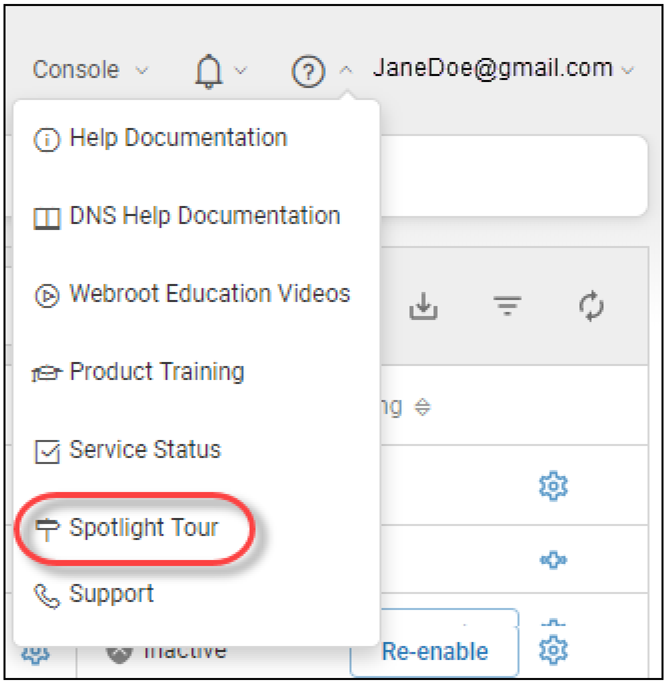
# About the Spotlight Tour

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

- The tabs in the Main menu
- Additional security layers, such as DNS Protection and Security Awareness Training
- Later, as needed, you can view the tour again.

**To view the Spotlight Tour:**

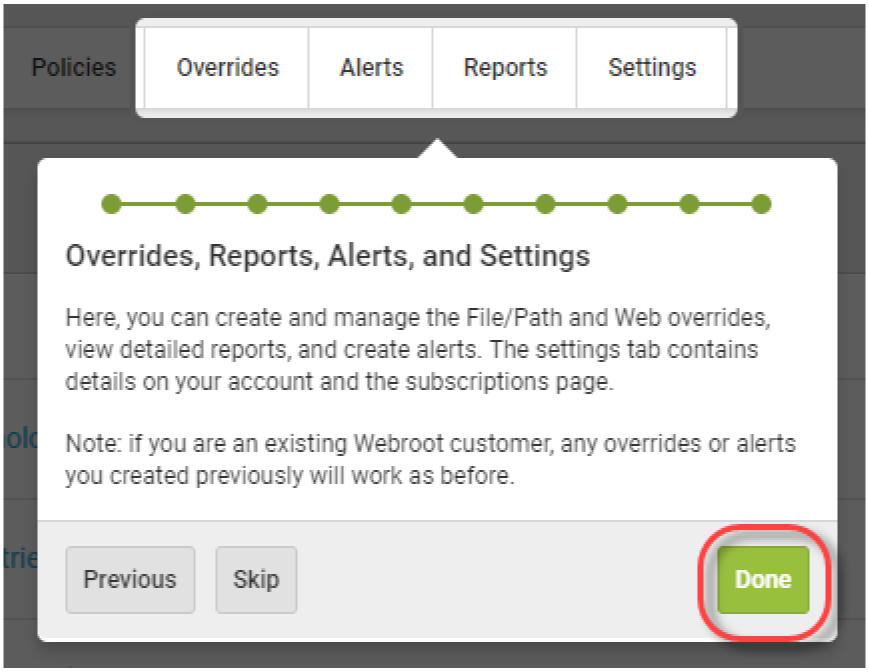
1. From the **Help (?)** drop-down menu, select **Spotlight Tour**.



The first window in the tour displays.

2. Click the **Skip** or **Next** button, as needed, until you're done viewing the tour.

3. When you're done viewing the tour, click the **Done** button.



Overrides, Reports, Alerts, and Settings

Here, you can create and manage the File/Path and Web overrides, view detailed reports, and create alerts. The settings tab contains details on your account and the subscriptions page.

Note: if you are an existing Webroot customer, any overrides or alerts you created previously will work as before.

As needed, to view the tour again, you can always select Spotlight Tour from the Help (?) drop-down menu.

# Communicating Through Firewalls

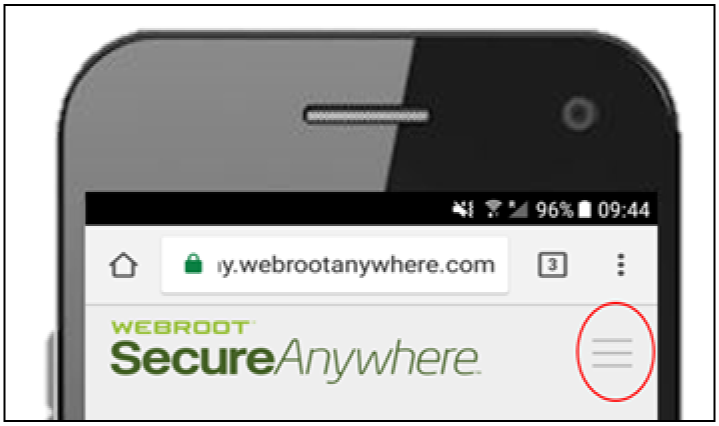
If a firewall is in place, please allow Webroot's path masks through the firewall, as described in the following table.

| PATH | PORT | INFORMATION |
|---|---|---|
| ***.webrootcloudav.com** | Port 443 (https) | Agent communication and updates.<br>**Note:** Some firewalls do not support double dotted subdomain names with a single wildcard mask, for example, g1.p4.webrootcloudav.com being represented by *.webrootcloudav.com, so some environments might require either *.p4.webrootcloudav.com or *.*.webrootcloudav.com. |
| ***.webroot.com** | Port 443 (https) | Agent messaging. |

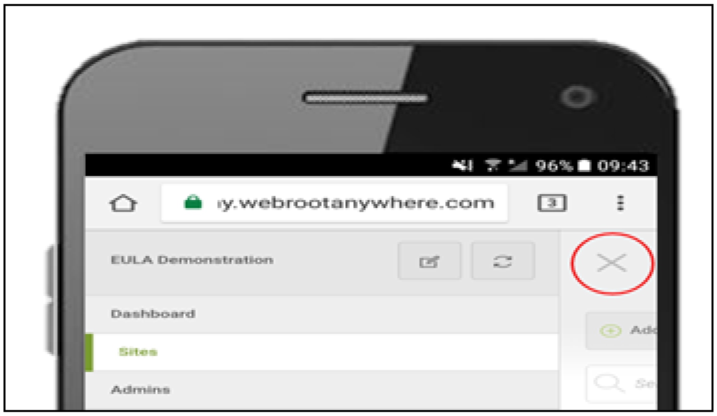
| PATH | PORT | INFORMATION |
|---|---|---|
| **https://wrskynet.s3.amazonaws.com/*** | Port 443 (https) | Agent file downloading and uploading. |
| **https://wrskynet-eu.s3-eu-west-1.amazonaws.com/*** | Port 443 (https) | Agent file downloading and uploading. |
| **https://wrskynet-oregon.s3-us-west-2.amazonaws.com/*** | Port 443 (https) | Agent file downloading and uploading. |
| **WSAWebFilteringPortal.elasticbeanstalk.com** | Port 80 (http) & 443 (https) | Required for agent Web Filtering, elasticbeanstalk is an amazon AWS domain. |
| ***.webrootanywhere.com** | Port 80 (http) & 443 (https) | Management portal and support ticket logs upload. |

# Enhanced Mobile Device Display

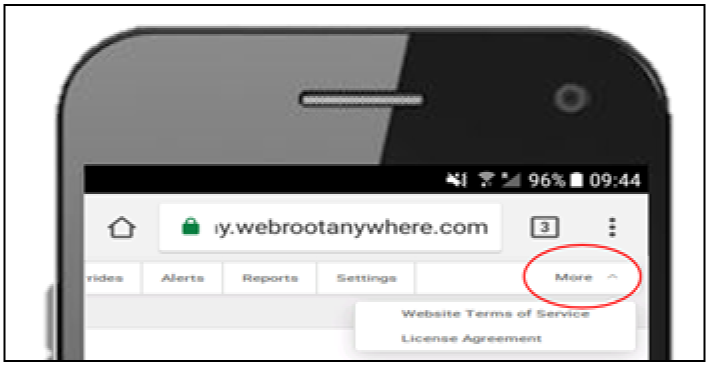
This management console has enhanced display capability for mobile devices. For mobile / small screen resolutions, the navigation bar disappears, and a Hamburger menu appears in the top right corner of the screen.



Clicking on this icon slides in the navigation from the left; click X icon to close it again.



The navigation has been improved for all screens. Any any navigation items exceeding the nav bar width are lifted from the bar and dropped into a new More drop-down menu.


96% 09:44
ıy.webrootanywhere.com
3
rides
Alerts
Reports
Settings
More
Website Terms of Service
License Agreement

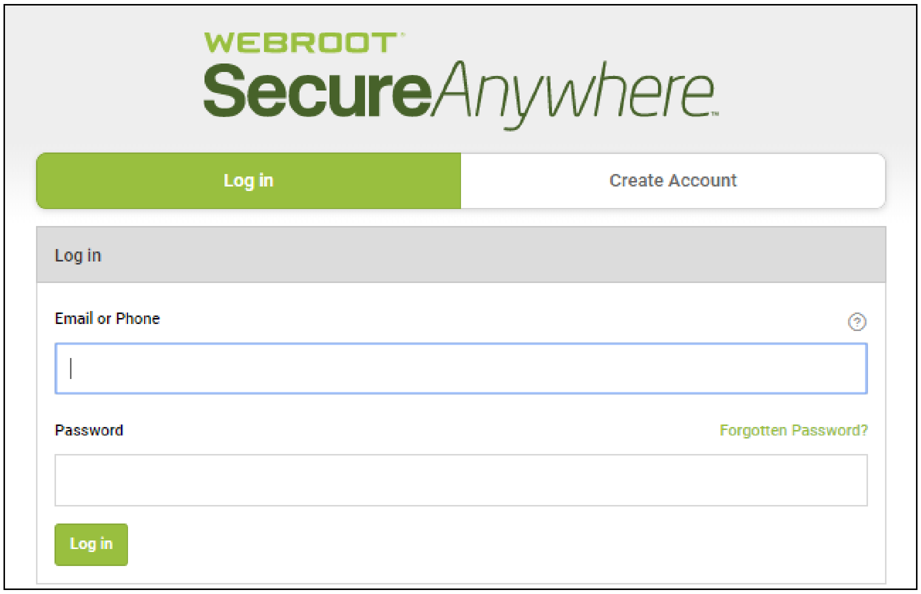
# Changing Consoles

Follow this procedure to switch between consoles.

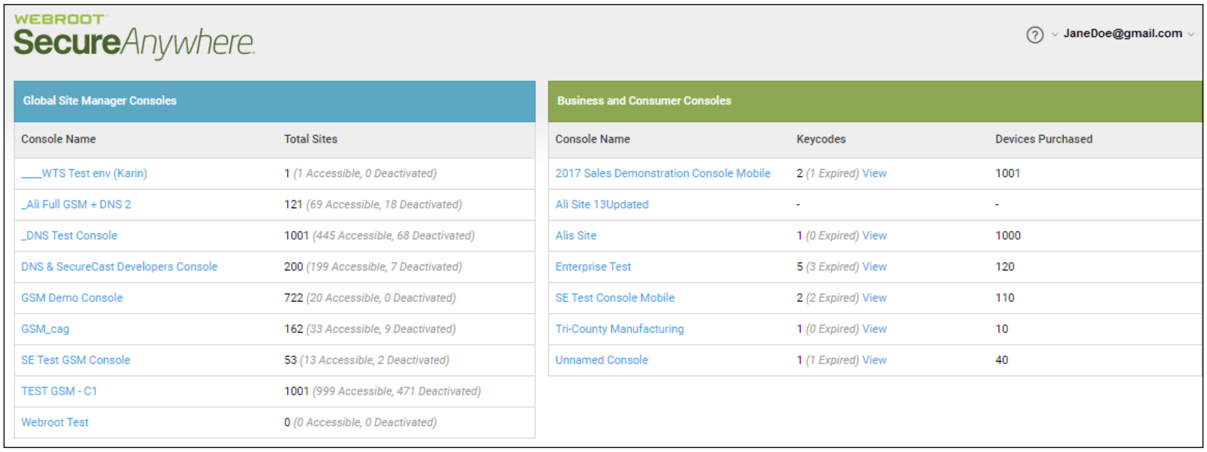
**Note:** This option is only available if you have created more than one console.

**To change consoles:**

1. Log in to the management console.



The Console Selection screen displays.



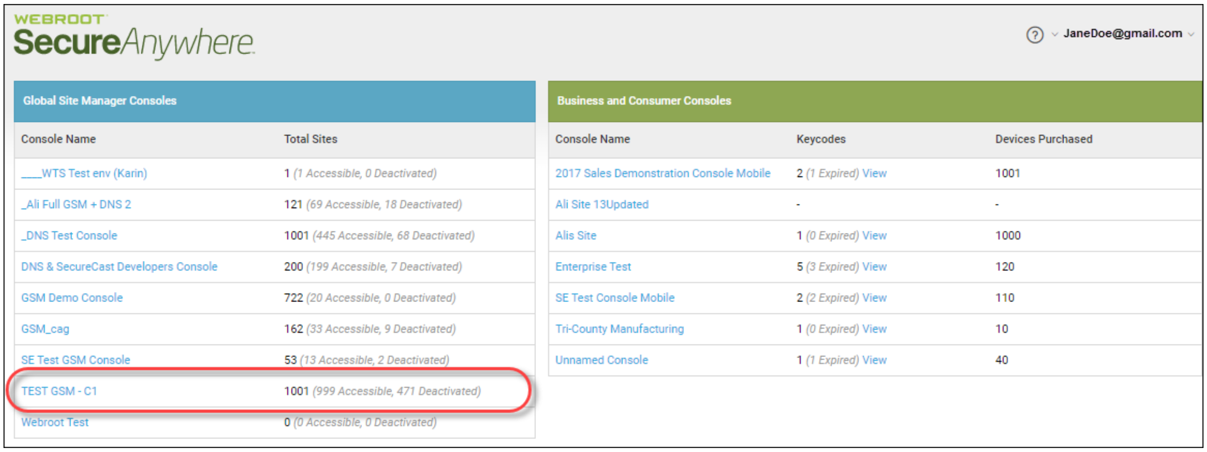
**Global Site Manager Consoles**

| Console Name | Total Sites |
|---|---|
| ___WTS Test env (Karin) | 1 *(1 Accessible, 0 Deactivated)* |
| _Ali Full GSM + DNS 2 | 121 *(69 Accessible, 18 Deactivated)* |
| _DNS Test Console | 1001 *(445 Accessible, 68 Deactivated)* |
| DNS & SecureCast Developers Console | 200 *(199 Accessible, 7 Deactivated)* |
| GSM Demo Console | 722 *(20 Accessible, 0 Deactivated)* |
| GSM_cag | 162 *(33 Accessible, 9 Deactivated)* |
| SE Test GSM Console | 53 *(13 Accessible, 2 Deactivated)* |
| TEST GSM - C1 | 1001 *(999 Accessible, 471 Deactivated)* |
| Webroot Test | 0 *(0 Accessible, 0 Deactivated)* |

**Business and Consumer Consoles**

| Console Name | Keycodes | Devices Purchased |
|---|---|---|
| 2017 Sales Demonstration Console Mobile | 2 *(1 Expired)* View | 1001 |
| Ali Site 13Updated | - | - |
| Alis Site | 1 *(0 Expired)* View | 1000 |
| Enterprise Test | 5 *(3 Expired)* View | 120 |
| SE Test Console Mobile | 2 *(2 Expired)* View | 110 |
| Tri-County Manufacturing | 1 *(0 Expired)* View | 10 |
| Unnamed Console | 1 *(1 Expired)* View | 40 |

2. Select a console to open it.



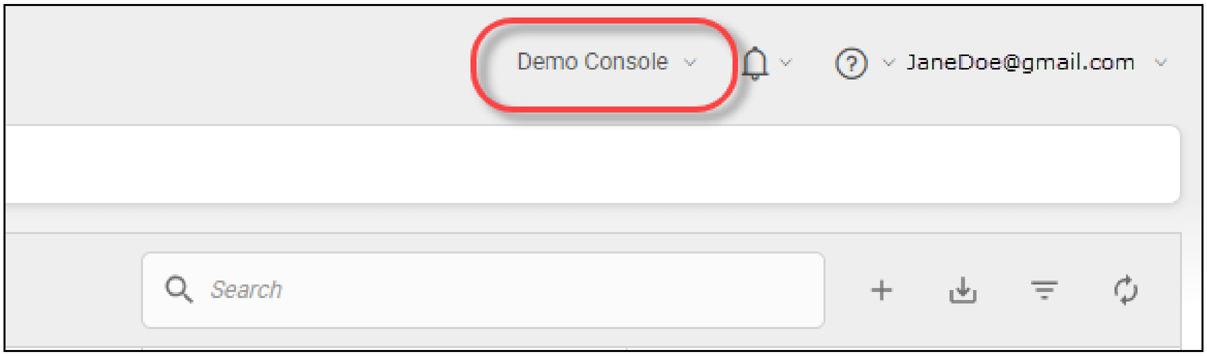
**Global Site Manager Consoles**

| Console Name | Total Sites |
|---|---|
| ___WTS Test env (Karin) | 1 *(1 Accessible, 0 Deactivated)* |
| _Ali Full GSM + DNS 2 | 121 *(69 Accessible, 18 Deactivated)* |
| _DNS Test Console | 1001 *(445 Accessible, 68 Deactivated)* |
| DNS & SecureCast Developers Console | 200 *(199 Accessible, 7 Deactivated)* |
| GSM Demo Console | 722 *(20 Accessible, 0 Deactivated)* |
| GSM_cag | 162 *(33 Accessible, 9 Deactivated)* |
| SE Test GSM Console | 53 *(13 Accessible, 2 Deactivated)* |
| TEST GSM - C1 | 1001 *(999 Accessible, 471 Deactivated)* |
| Webroot Test | 0 *(0 Accessible, 0 Deactivated)* |

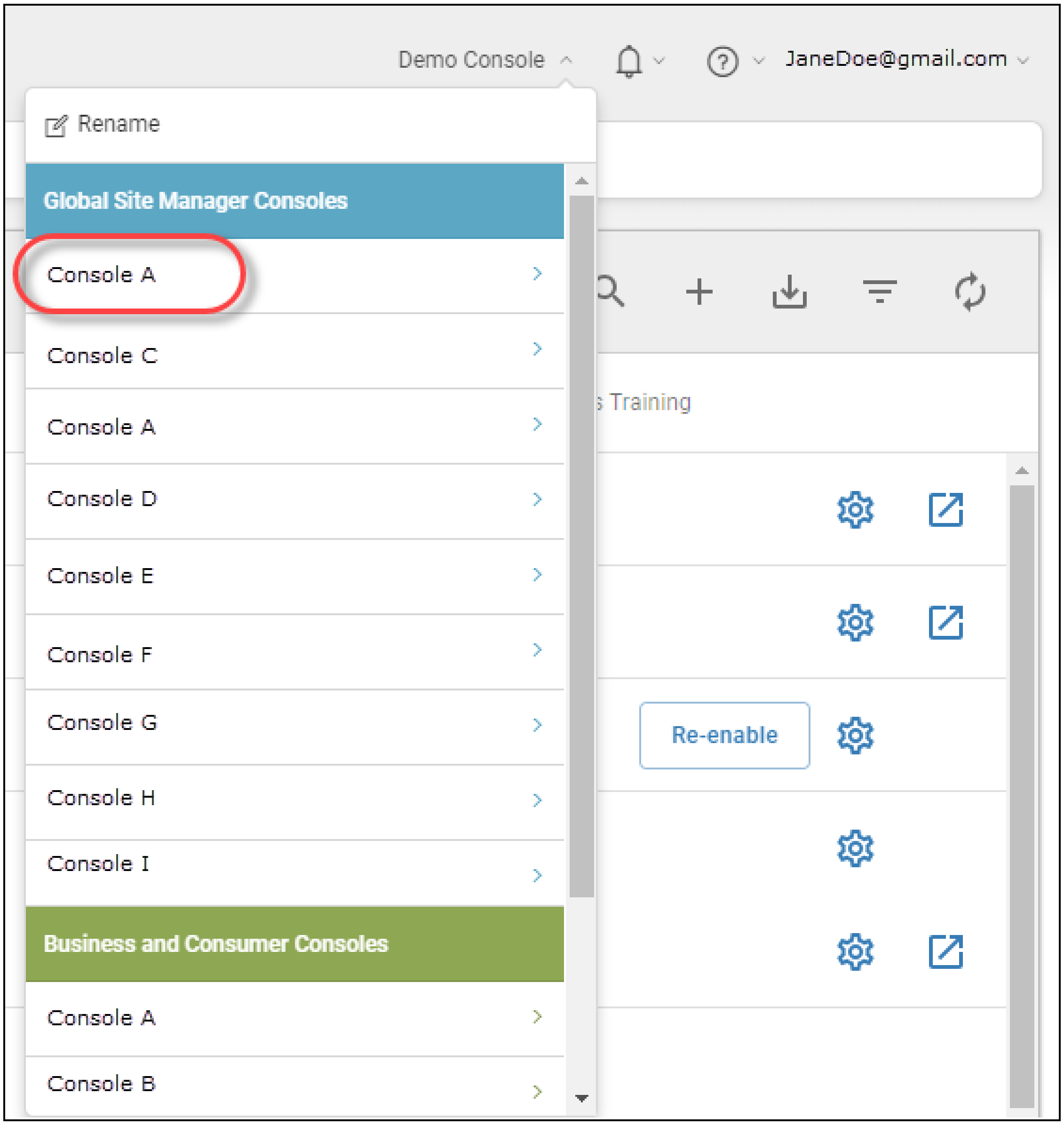
**Business and Consumer Consoles**

| Console Name | Keycodes | Devices Purchased |
|---|---|---|
| 2017 Sales Demonstration Console Mobile | 2 *(1 Expired)* View | 1001 |
| Ali Site 13Updated | - | - |
| Alis Site | 1 *(0 Expired)* View | 1000 |
| Enterprise Test | 5 *(3 Expired)* View | 120 |
| SE Test Console Mobile | 2 *(2 Expired)* View | 110 |
| Tri-County Manufacturing | 1 *(0 Expired)* View | 10 |
| Unnamed Console | 1 *(1 Expired)* View | 40 |

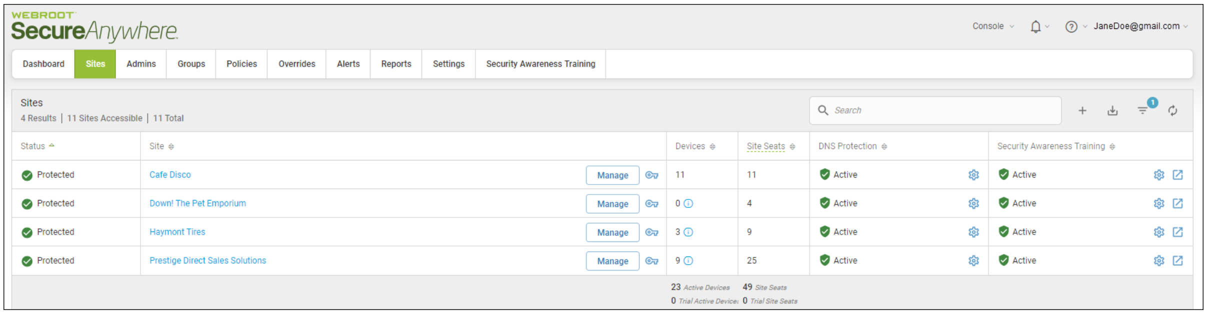
3. Once inside a console, to change consoles, go to the console name in the upper right corner.



4. From the drop-down menu, select the name of the console you want to switch to.



The system switches you to the console that you selected, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

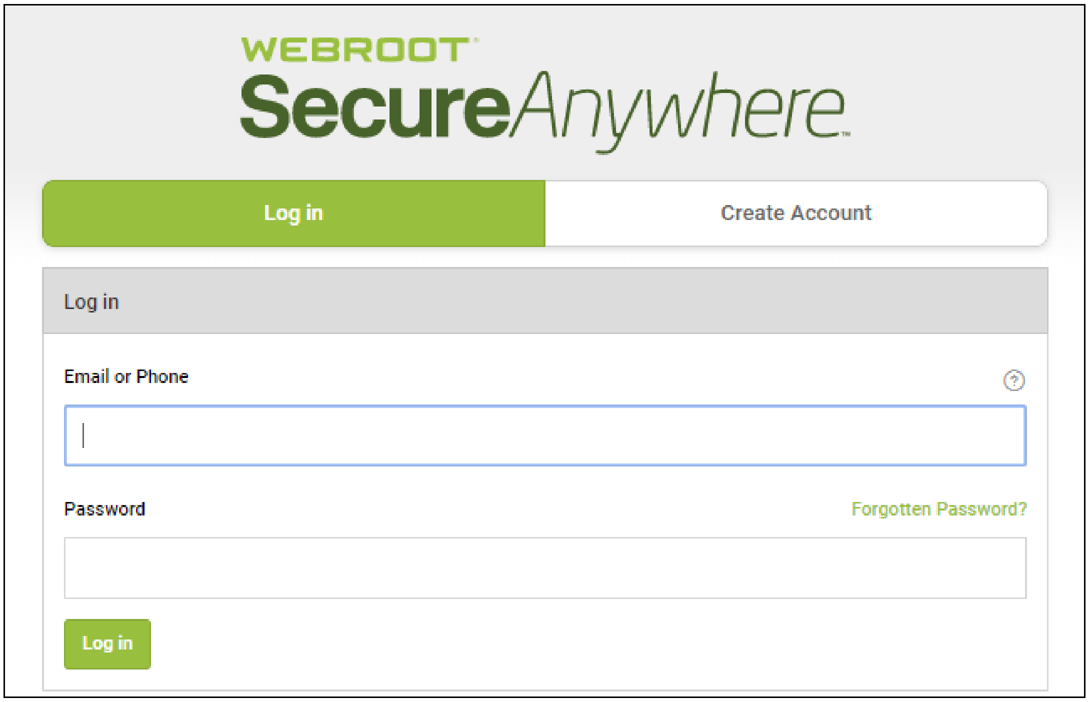
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| ✓ Protected | Cafe Disco | Manage | 11 | 11 | ✓ Active | ✓ Active |
| ✓ Protected | Down! The Pet Emporium | Manage | 0 | 4 | ✓ Active | ✓ Active |
| ✓ Protected | Haymont Tires | Manage | 3 | 9 | ✓ Active | ✓ Active |
| ✓ Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | ✓ Active | ✓ Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

# Renaming Consoles

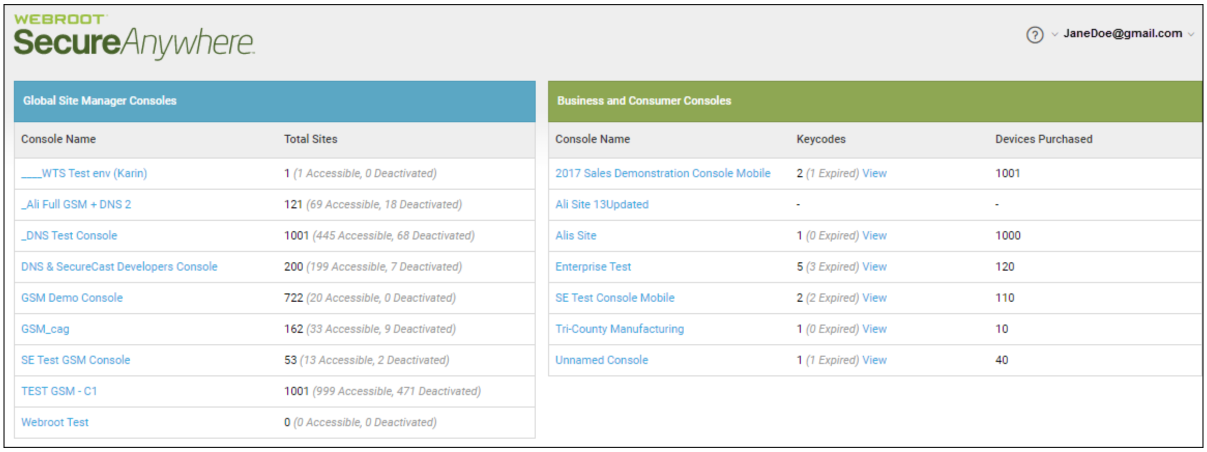
Follow this procedure to rename consoles.

**To rename a console:**

1. Log in to the management console.



The Console Selection screen displays.



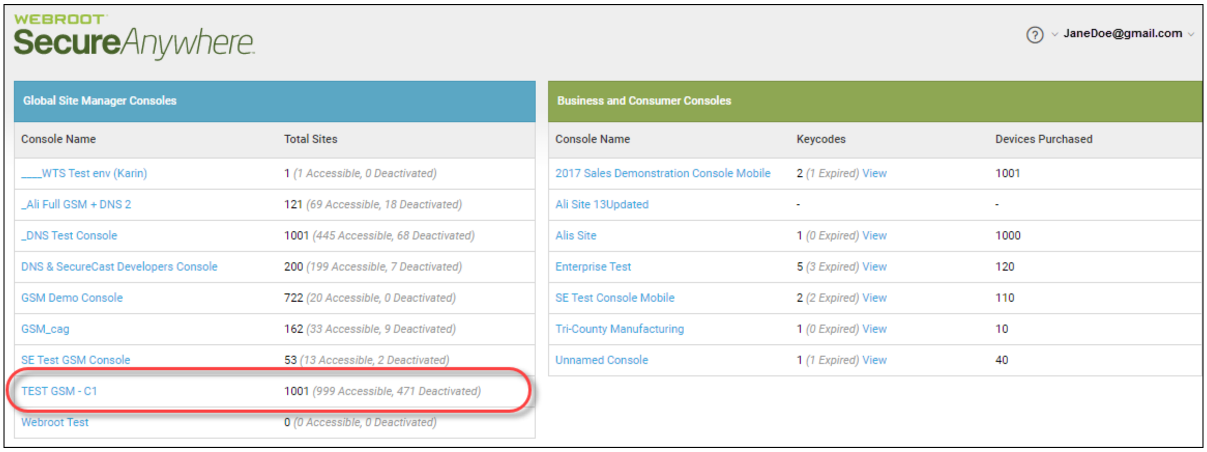
**Global Site Manager Consoles**

| Console Name | Total Sites |
|---|---|
| ___WTS Test env (Karin) | 1 *(1 Accessible, 0 Deactivated)* |
| _Ali Full GSM + DNS 2 | 121 *(69 Accessible, 18 Deactivated)* |
| _DNS Test Console | 1001 *(445 Accessible, 68 Deactivated)* |
| DNS & SecureCast Developers Console | 200 *(199 Accessible, 7 Deactivated)* |
| GSM Demo Console | 722 *(20 Accessible, 0 Deactivated)* |
| GSM_cag | 162 *(33 Accessible, 9 Deactivated)* |
| SE Test GSM Console | 53 *(13 Accessible, 2 Deactivated)* |
| TEST GSM - C1 | 1001 *(999 Accessible, 471 Deactivated)* |
| Webroot Test | 0 *(0 Accessible, 0 Deactivated)* |

**Business and Consumer Consoles**

| Console Name | Keycodes | Devices Purchased |
|---|---|---|
| 2017 Sales Demonstration Console Mobile | 2 *(1 Expired)* View | 1001 |
| Ali Site 13Updated | - | - |
| Alis Site | 1 *(0 Expired)* View | 1000 |
| Enterprise Test | 5 *(3 Expired)* View | 120 |
| SE Test Console Mobile | 2 *(2 Expired)* View | 110 |
| Tri-County Manufacturing | 1 *(0 Expired)* View | 10 |
| Unnamed Console | 1 *(1 Expired)* View | 40 |

2. Select a console to open it.



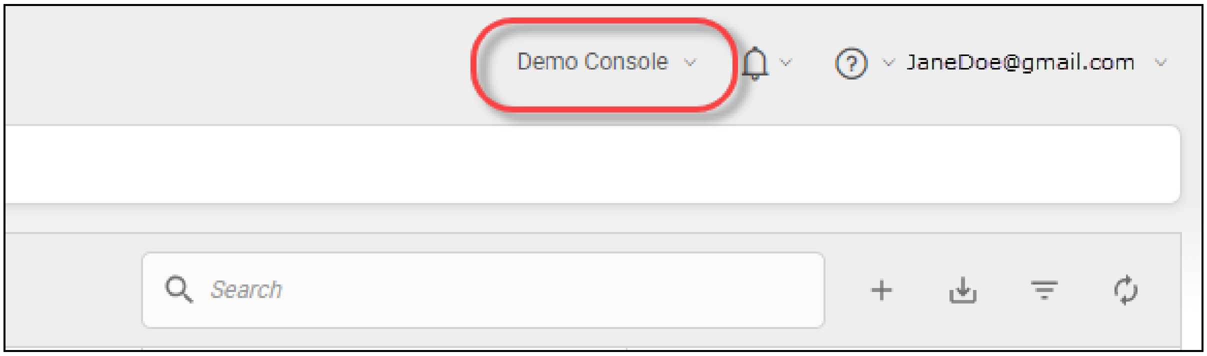
**Global Site Manager Consoles**

| Console Name | Total Sites |
|---|---|
| ___WTS Test env (Karin) | 1 *(1 Accessible, 0 Deactivated)* |
| _Ali Full GSM + DNS 2 | 121 *(69 Accessible, 18 Deactivated)* |
| _DNS Test Console | 1001 *(445 Accessible, 68 Deactivated)* |
| DNS & SecureCast Developers Console | 200 *(199 Accessible, 7 Deactivated)* |
| GSM Demo Console | 722 *(20 Accessible, 0 Deactivated)* |
| GSM_cag | 162 *(33 Accessible, 9 Deactivated)* |
| SE Test GSM Console | 53 *(13 Accessible, 2 Deactivated)* |
| TEST GSM - C1 | 1001 *(999 Accessible, 471 Deactivated)* |
| Webroot Test | 0 *(0 Accessible, 0 Deactivated)* |

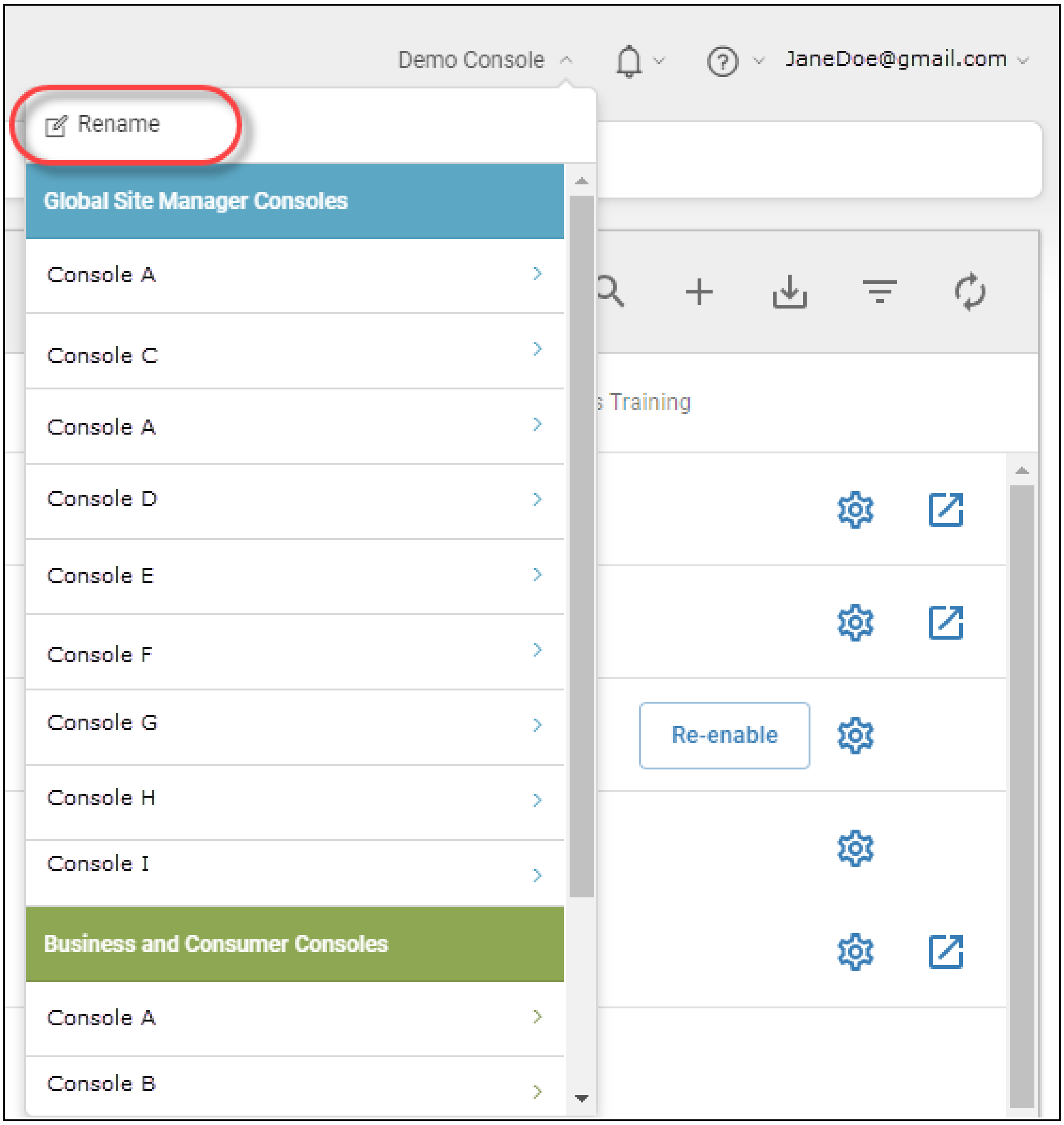
**Business and Consumer Consoles**

| Console Name | Keycodes | Devices Purchased |
|---|---|---|
| 2017 Sales Demonstration Console Mobile | 2 *(1 Expired)* View | 1001 |
| Ali Site 13Updated | - | - |
| Alis Site | 1 *(0 Expired)* View | 1000 |
| Enterprise Test | 5 *(3 Expired)* View | 120 |
| SE Test Console Mobile | 2 *(2 Expired)* View | 110 |
| Tri-County Manufacturing | 1 *(0 Expired)* View | 10 |
| Unnamed Console | 1 *(1 Expired)* View | 40 |

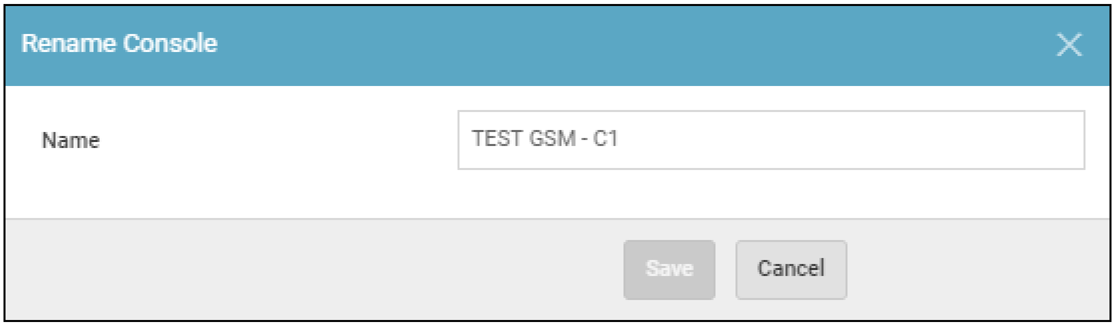
Once inside a console, to change consoles, go to the console name in the upper right corner.



3. From the drop-down menu, select **Rename**.

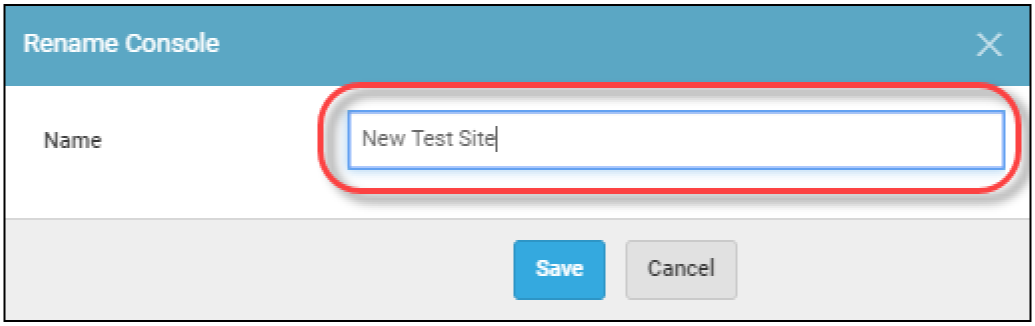


The Rename Console window displays.


Rename Console

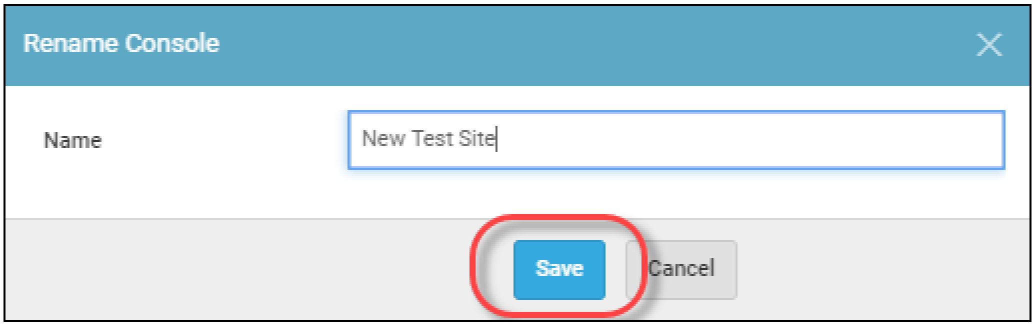
Name TEST GSM - C1

4. In the Name field, enter the new name for the console.


Rename Console

Name New Test Site

5. Click the **Save** button.


Rename Console

Name New Test Site

The console is now renamed.

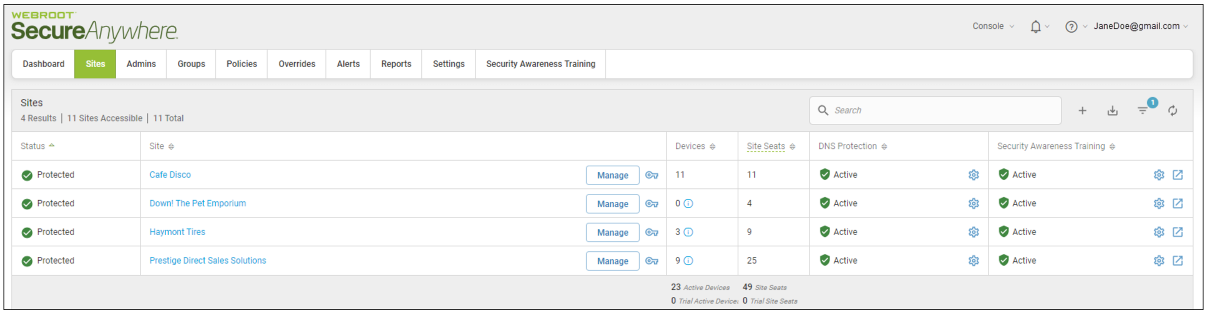
# Accessing the Endpoint Console

Follow this procedure to go to the Endpoint console when you are in the management console.

**To access the Endpoint console:**

1. Log in to the management console.

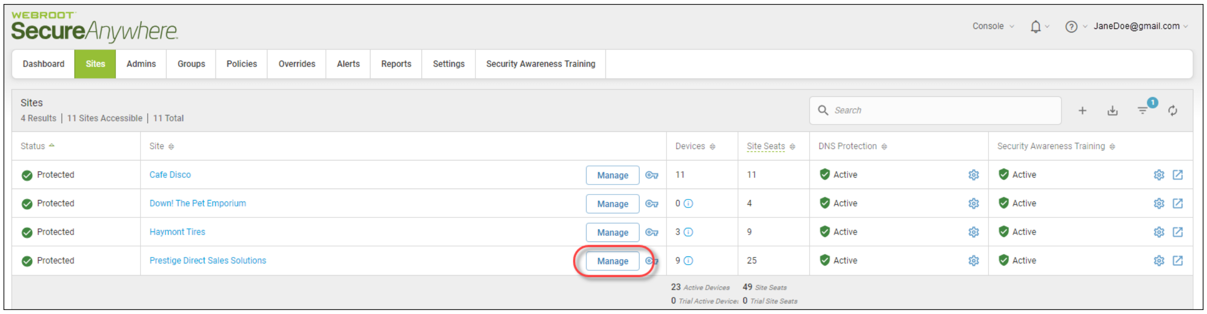
   The management console displays.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

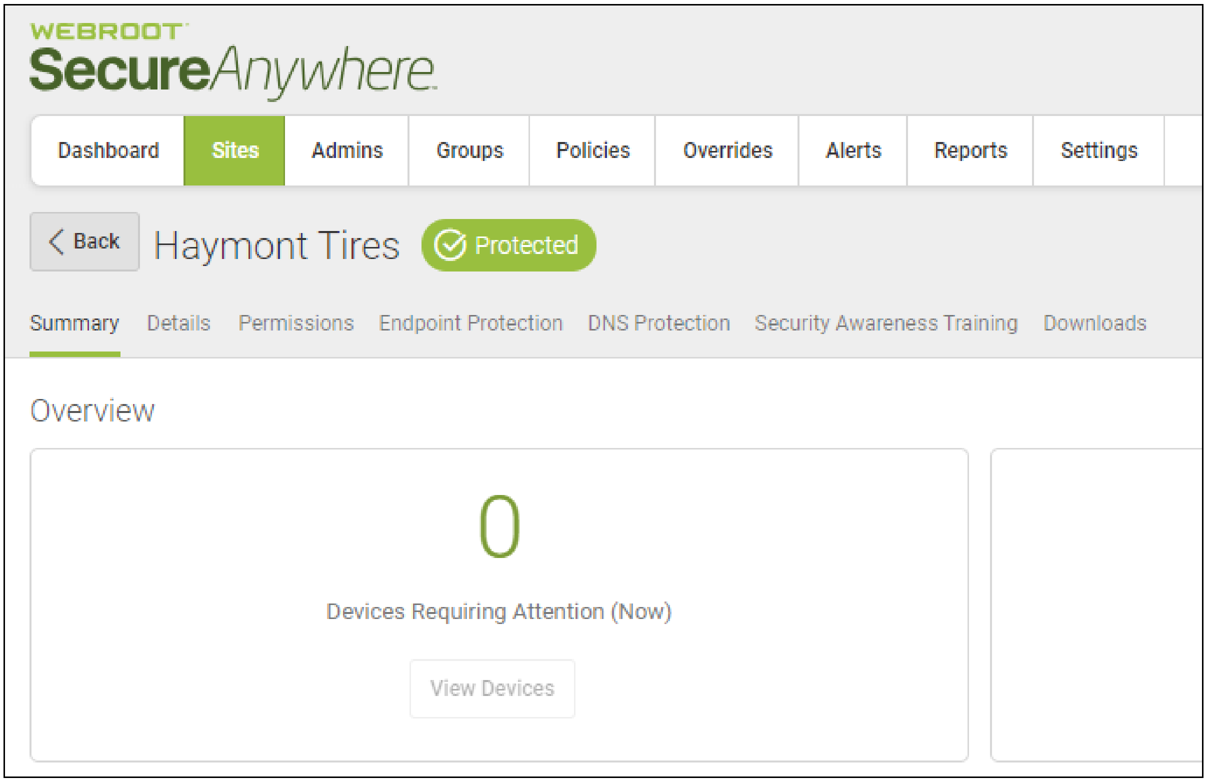
2. Click the **Manage** button for the site you want to access the Endpoint console for.



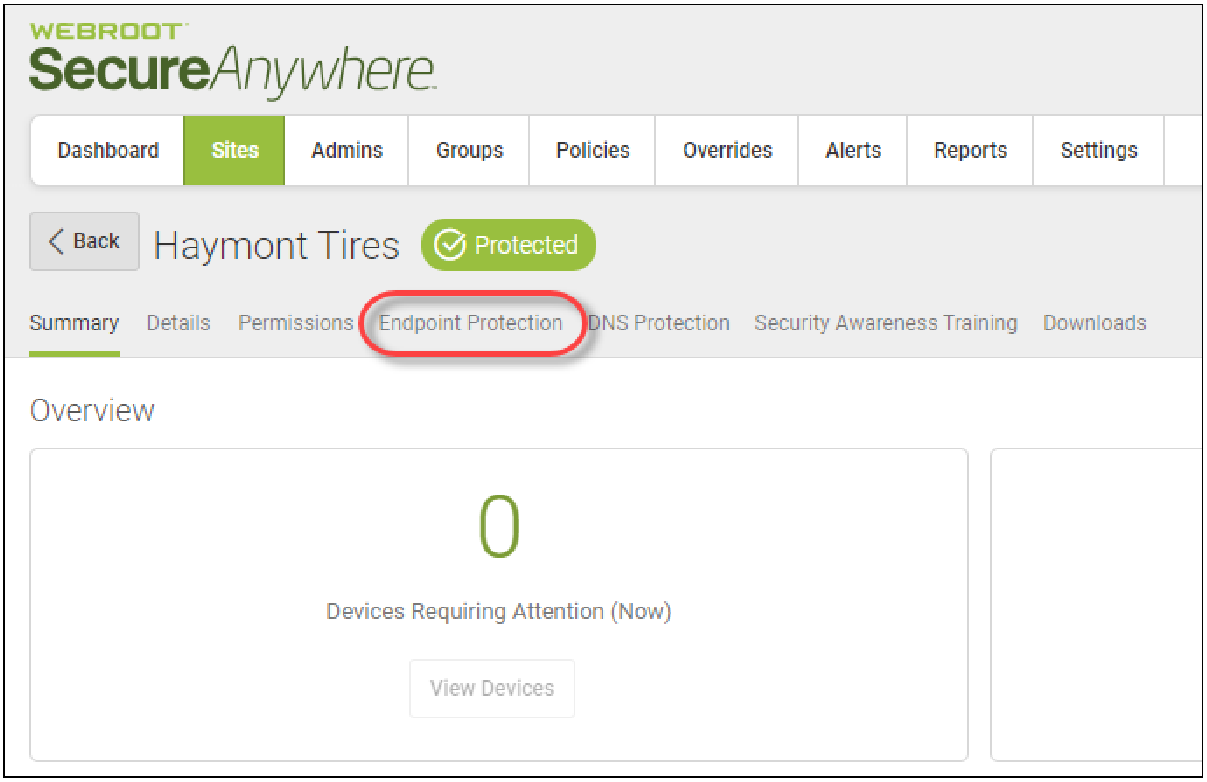
Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

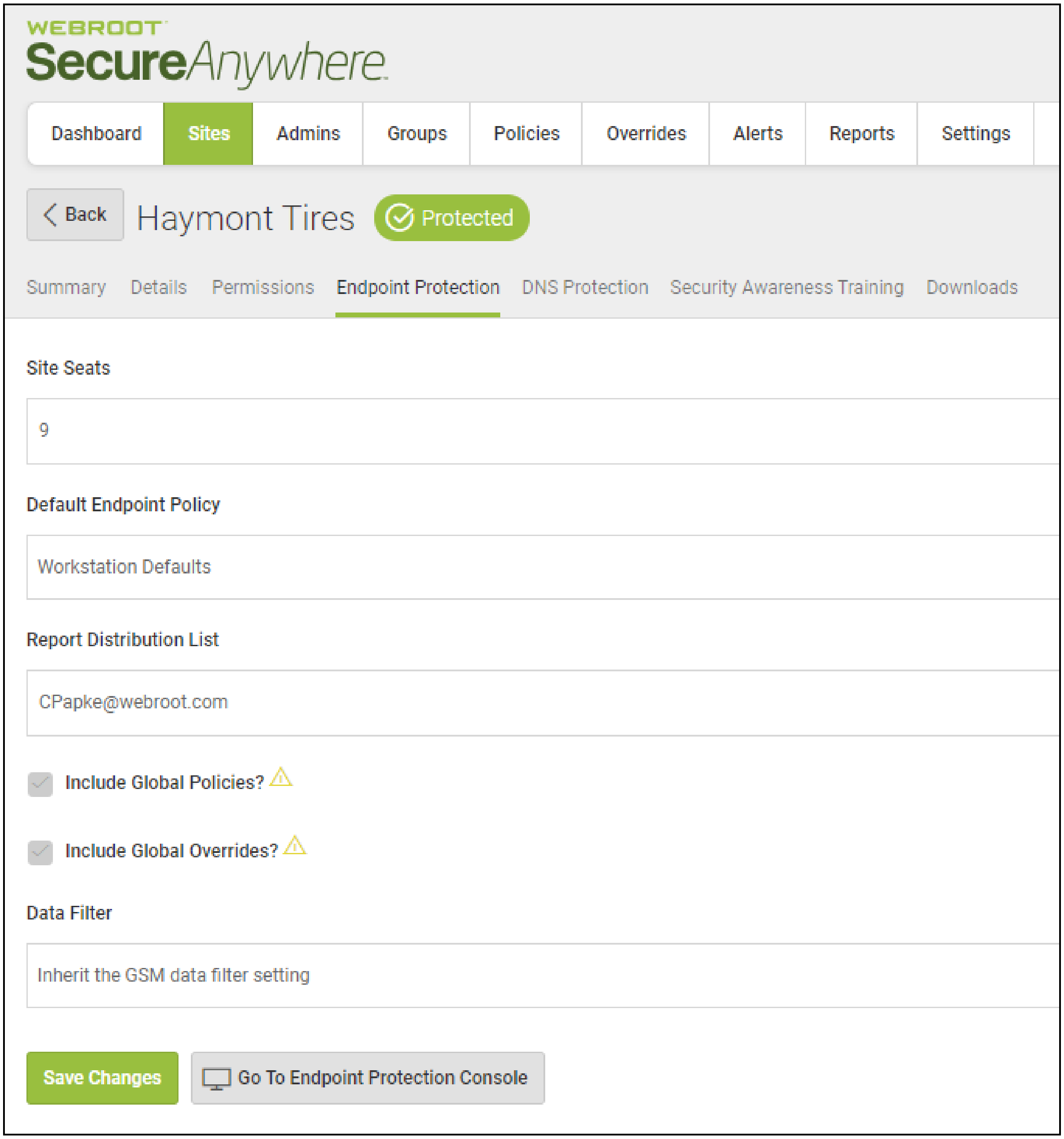
The Manage Sites panel displays, with the Summary tab active.


WEBROOT
SecureAnywhere
Dashboard
Sites
Admins
Groups
Policies
Overrides
Alerts
Reports
Settings
Back
Haymont Tires
Protected
Summary
Details
Permissions
Endpoint Protection
DNS Protection
Security Awareness Training
Downloads
Overview
0
Devices Requiring Attention (Now)
View Devices

3. Click the **Endpoint Protection** tab.



The Endpoint Protection tab displays.



Haymont Tires

Site Seats

9

Default Endpoint Policy

Workstation Defaults

Report Distribution List

CPapke@webroot.com

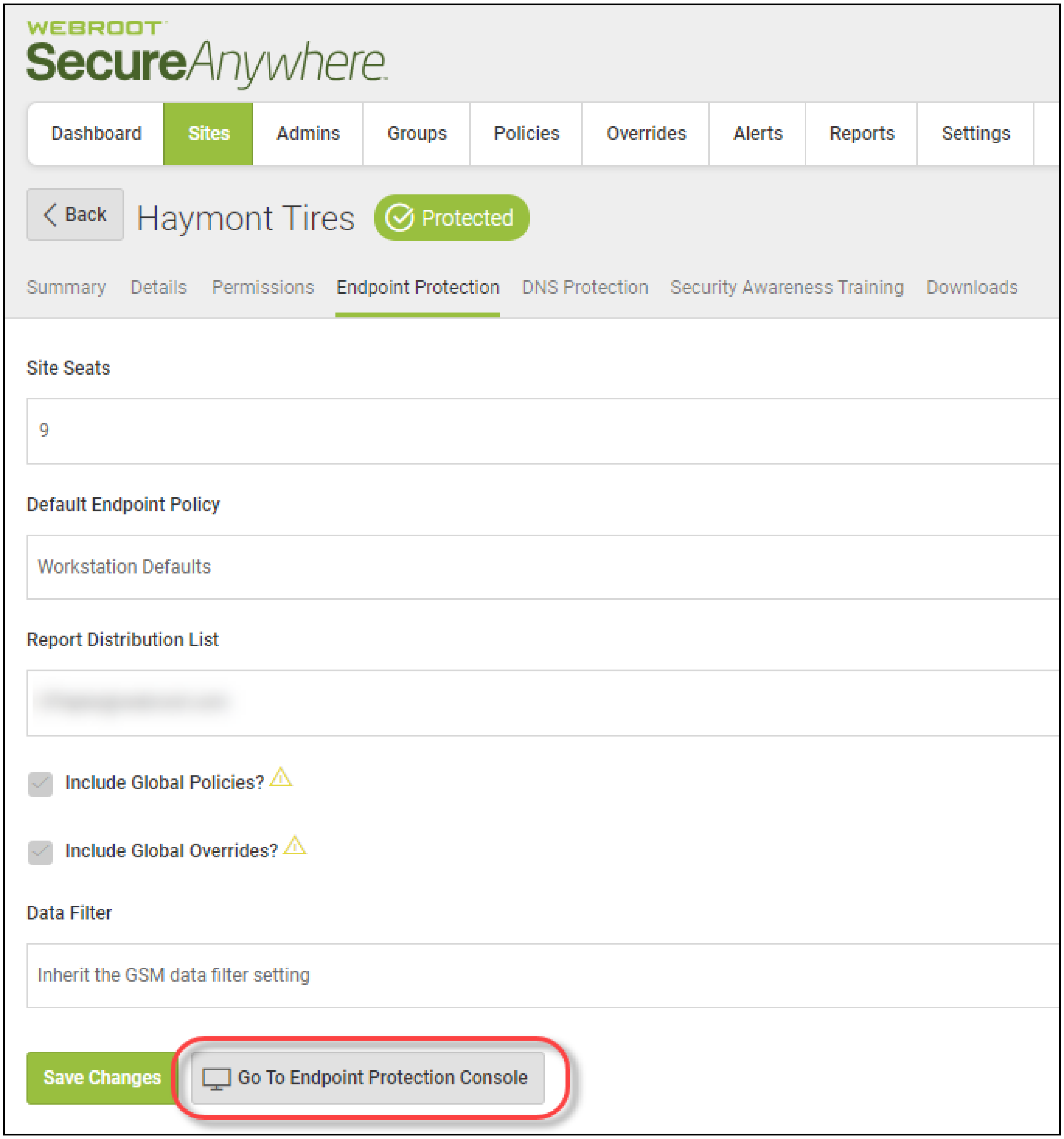
☑ Include Global Policies? ⚠

☑ Include Global Overrides? ⚠

Data Filter

Inherit the GSM data filter setting

4. At the bottom of the window, click the **Go To Endpoint Protection Console** button.



Site Seats

9

Default Endpoint Policy

Workstation Defaults

Report Distribution List

[redacted]

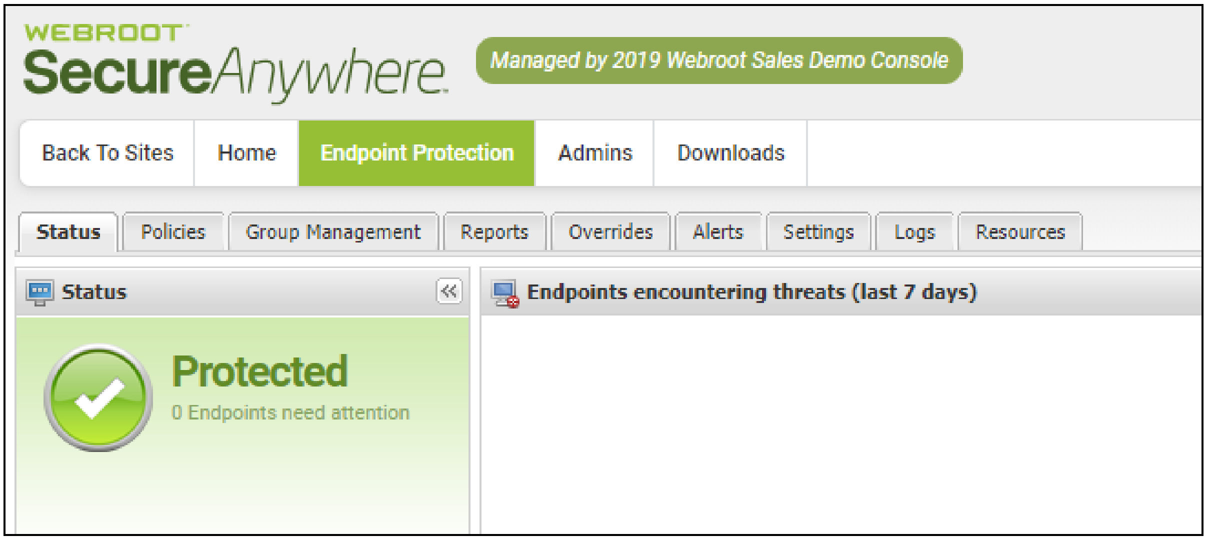
☑ Include Global Policies? ⚠

☑ Include Global Overrides? ⚠

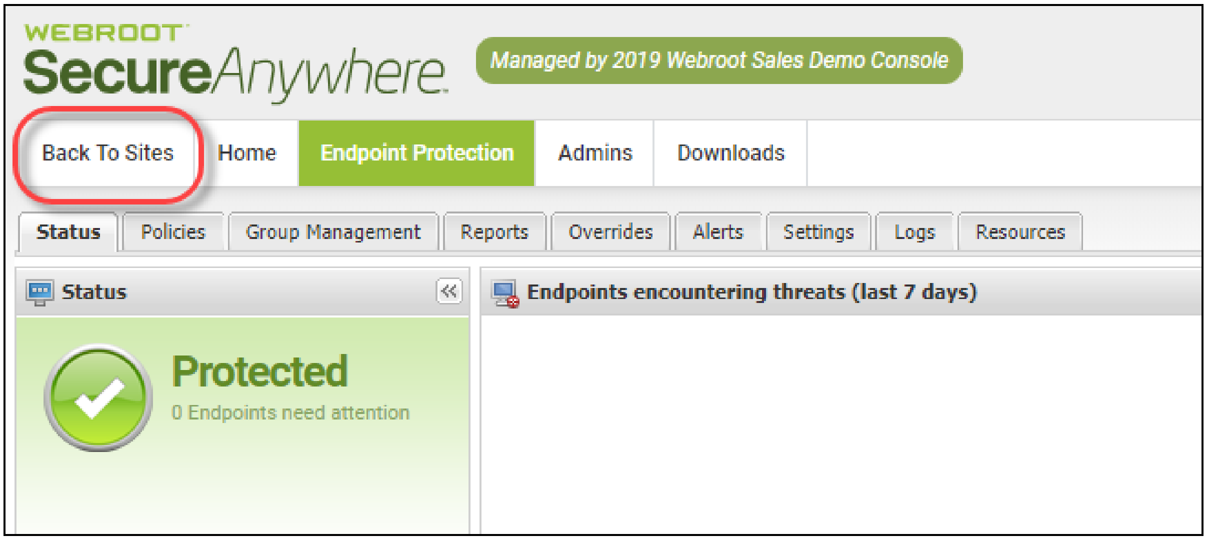
Data Filter

Inherit the GSM data filter setting

The Endpoint Protection console for the site you were on displays.



5. To return to the management console, click the **Back to Sites** button.



# System Requirements

The system requirements can be found here: System Requirements section of the Business Endpoint Protection webpage.

# Chapter 2: Working With Dashboards

To work with dashboards, see the following topics:

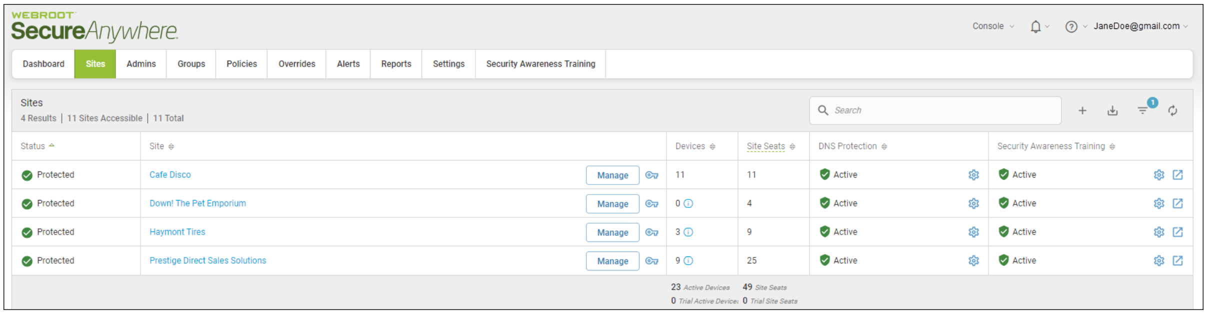
# Creating Dashboard Charts

Follow this procedure to create and add dashboard charts to your console.

### To create a dashboard chart:

1. Log in to the [management console](management console).

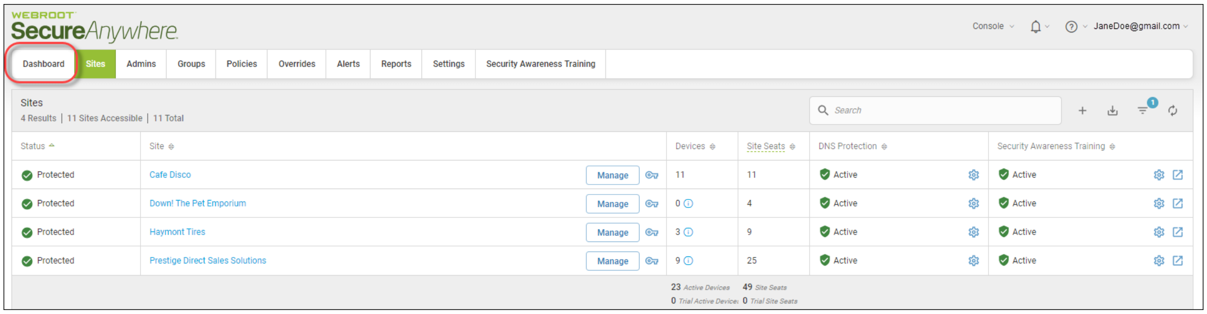
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

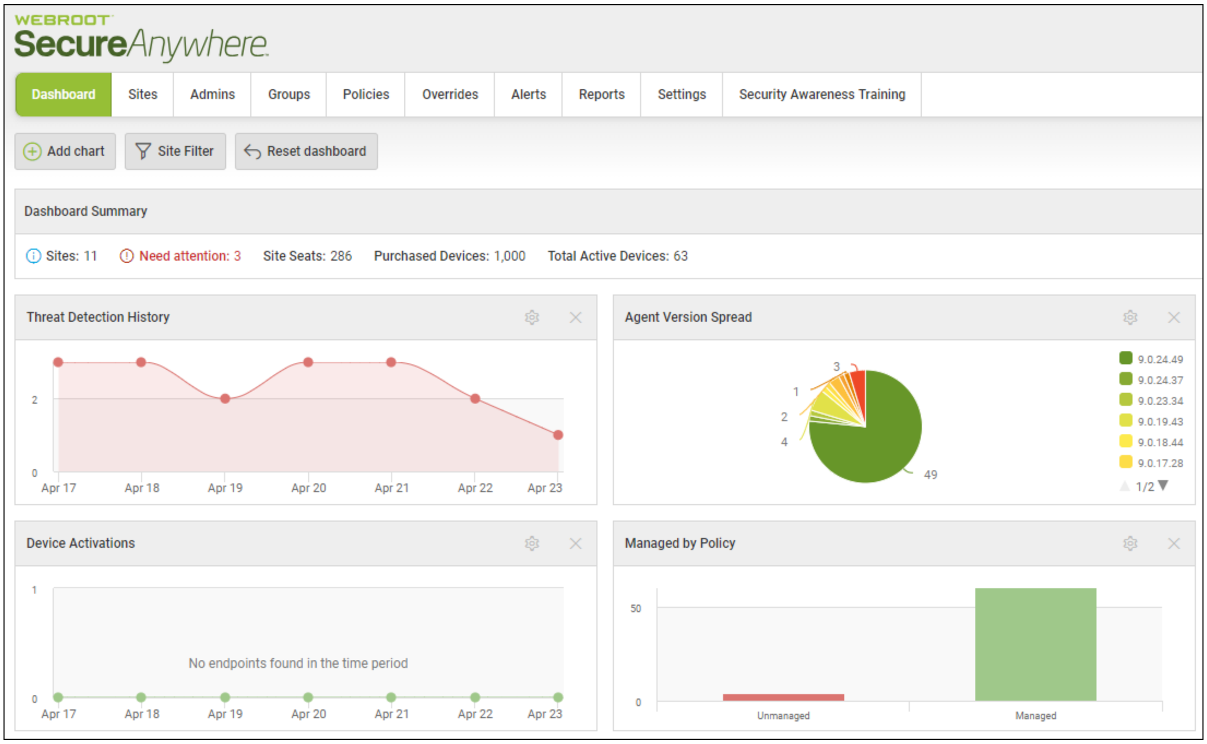
2. From the main menu, click the **Dashboard** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

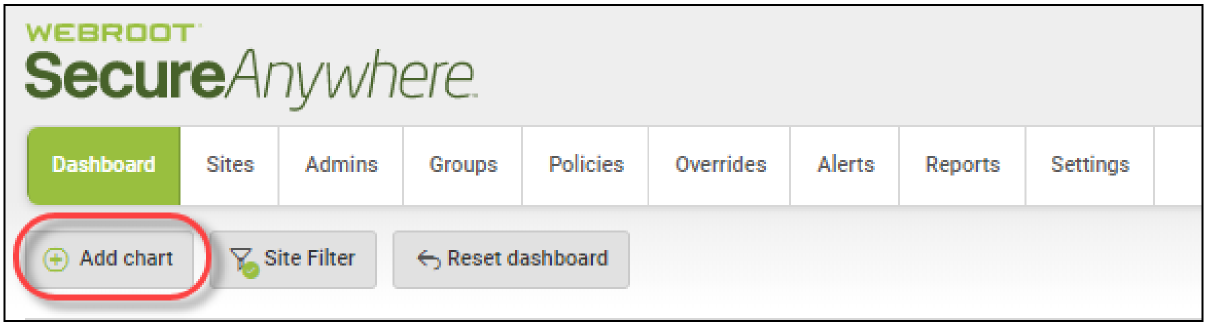
   The Dashboard tab displays.



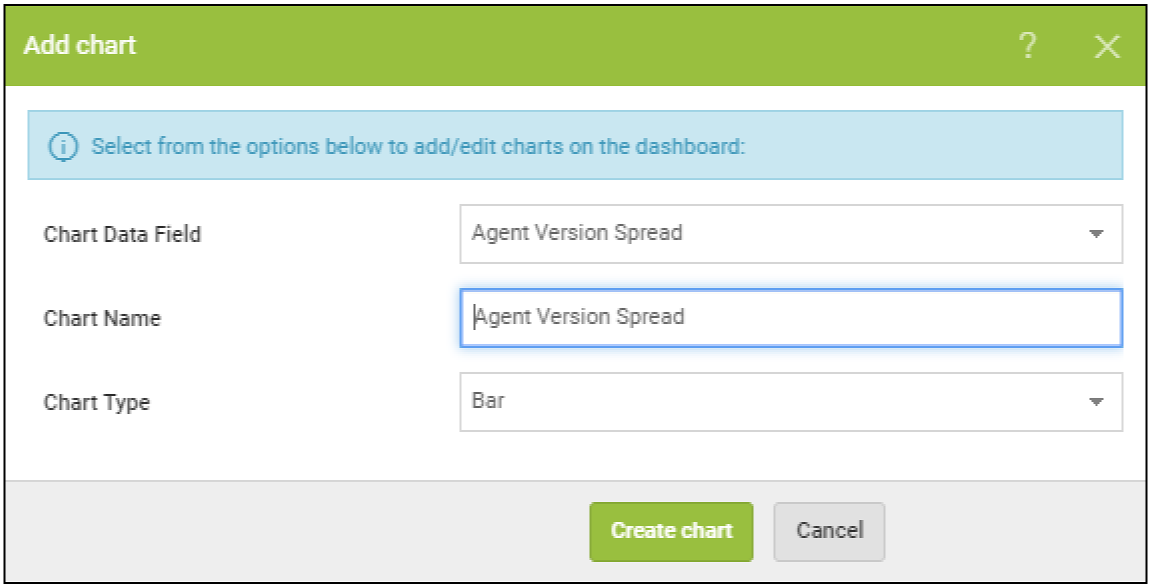
Dashboard Summary

Sites: 11 Need attention: 3 Site Seats: 286 Purchased Devices: 1,000 Total Active Devices: 63

3. Click the **Add chart** button.



The Add chart window displays.



Add chart

Select from the options below to add/edit charts on the dashboard:

Chart Data Field: Agent Version Spread

Chart Name: Agent Version Spread

Chart Type: Bar

4. From the Chart Data Field drop-down menu, select any of the following options:

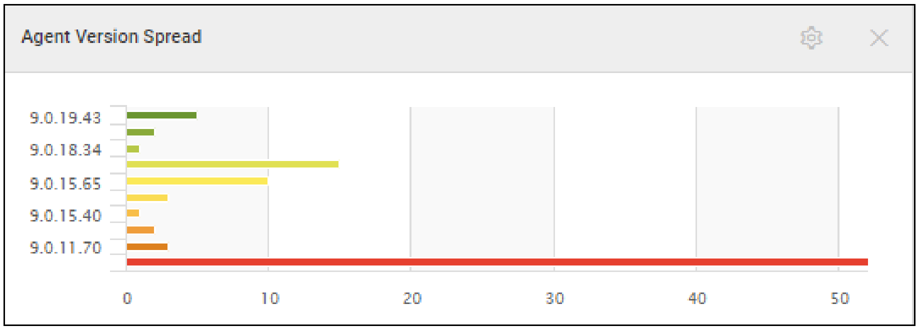
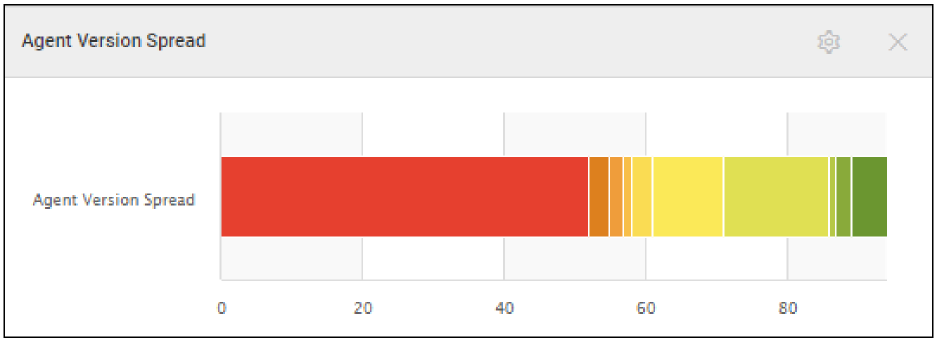
| | | | |
|---|---|---|---|
| Agent Version Spread | Firewall Status | Operating System Language | Rootkit Shield Status |
| Attention Required | Identity Shield Status | Operating System Platform | Scheduled Scans Status |
| Device Activations | Infrared Status | Phishing Shield Status | Silent Mode |
| Device Type | Installation Status | Primary Browser | Threat Detection History |
| Endpoint Status | Managed by Policy | Realtime Shield Status | USB Shield Status |
| Expired Status | Offline Shield Status | Remediation Status | Web Threat Shield Status |

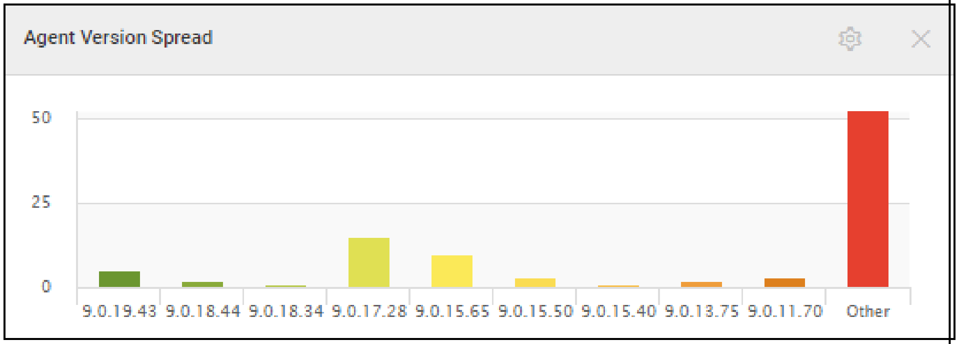
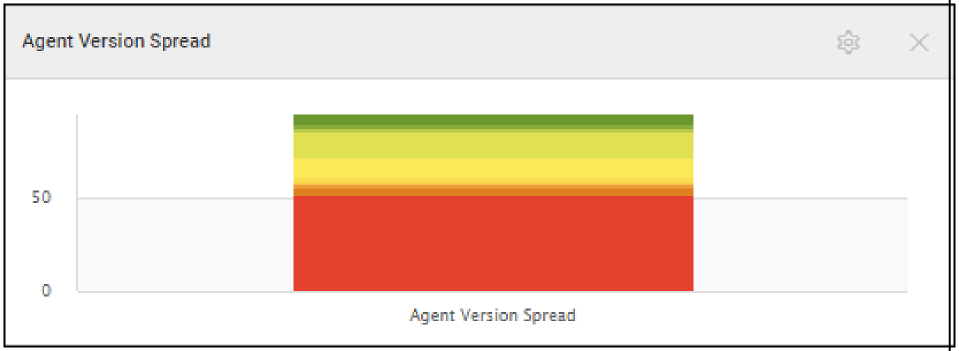
**Note:** The following data points are unsupported in the Mac agent: Firewall Status, Rootkit Shield Status, Infared Status. Silent Mode, Offline Shield Status.

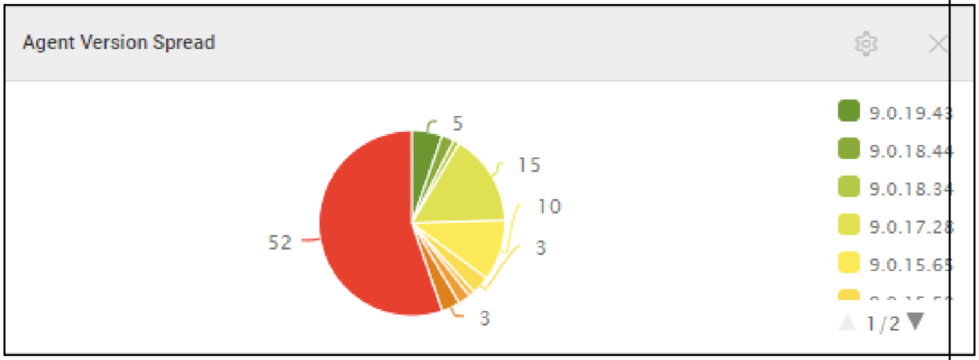
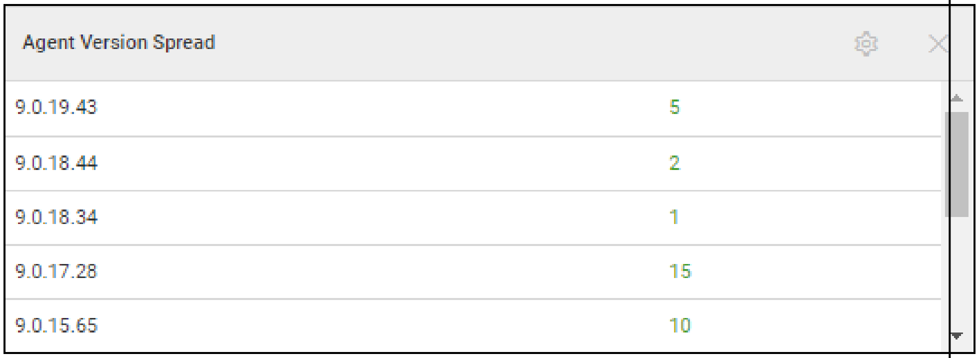
5. In the Chart Name field, enter the name of the chart.

Typically, the name of the chart reflects the name of the type of information within it, but this is a free-form field, and you can name the chart something else, as needed.

6. From the Chart Type drop-down menu, select one of the following chart types.

| NAME | DESCRIPTION |
|---|---|
| **Bar** |  |
| **Bar Stacked** |  |

| NAME | DESCRIPTION |
|---|---|
| **Column** |  |
| **Column Stacked** |  |

| NAME | DESCRIPTION |
|---|---|
| **Pie** | :<br><br> Agent Version Spread<br>5<br>15<br>10<br>3<br>3<br>52<br>9.0.19.43<br>9.0.18.44<br>9.0.18.34<br>9.0.17.28<br>9.0.15.65<br>1/2 |
| **Table** | <br>Agent Version Spread<br>9.0.19.43 5<br>9.0.18.44 2<br>9.0.18.34 1<br>9.0.17.28 15<br>9.0.15.65 10 |

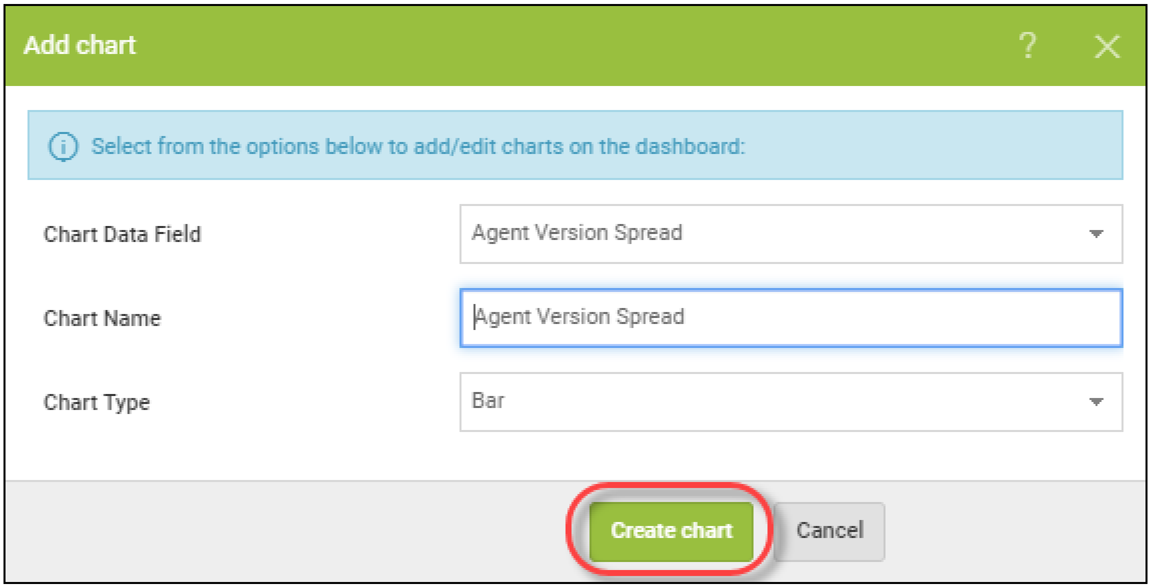
7. If you are creating the Threats Detection History or Device Activation dashboard charts, you can select one of the following different chart types:
   - Area
   - Area Spline
   - Column
   - Line

- Spline
- Table

8. If you are editing the Threats Detection History or Device Activation dashboard charts, you can configure the time period to one of the following:

| | | | |
|---|---|---|---|
| 24 hours | 2 days | 3 days | 7 days |
| 14 days | 30 days | 60 days | 90 days |

9. When you're finished populating the fields, click the **Create chart** button.



Add chart

Select from the options below to add/edit charts on the dashboard:

Chart Data Field: Agent Version Spread

Chart Name: Agent Version Spread

Chart Type: Bar

The system creates a dashboard with the required information.

> **Note:** For information on editing dashboard charts, see *Editing Dashboard Charts on page 51*.

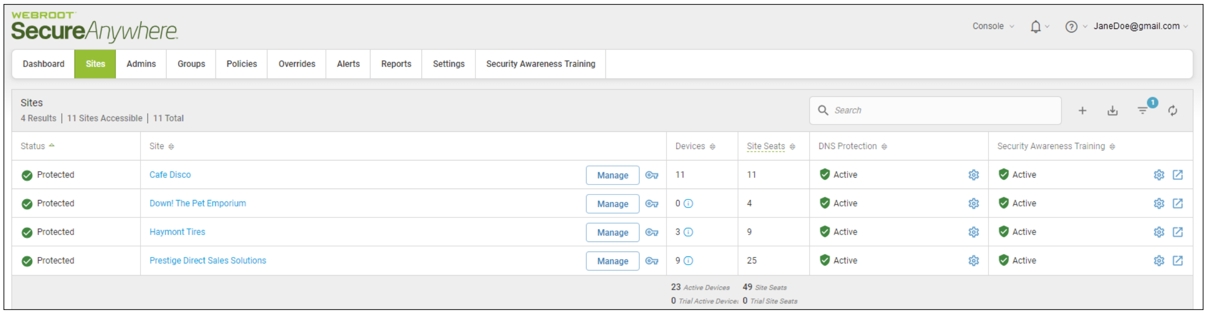
# Editing Dashboard Charts

After you've created a dashboard chart, you can follow this procedure to edit the chart, as needed.

**To edit a dashboard chart:**

1. Log in to the management console.

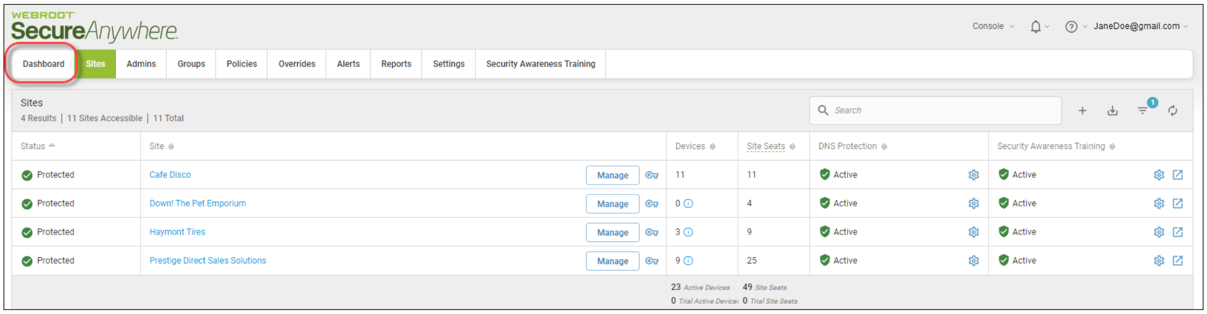
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

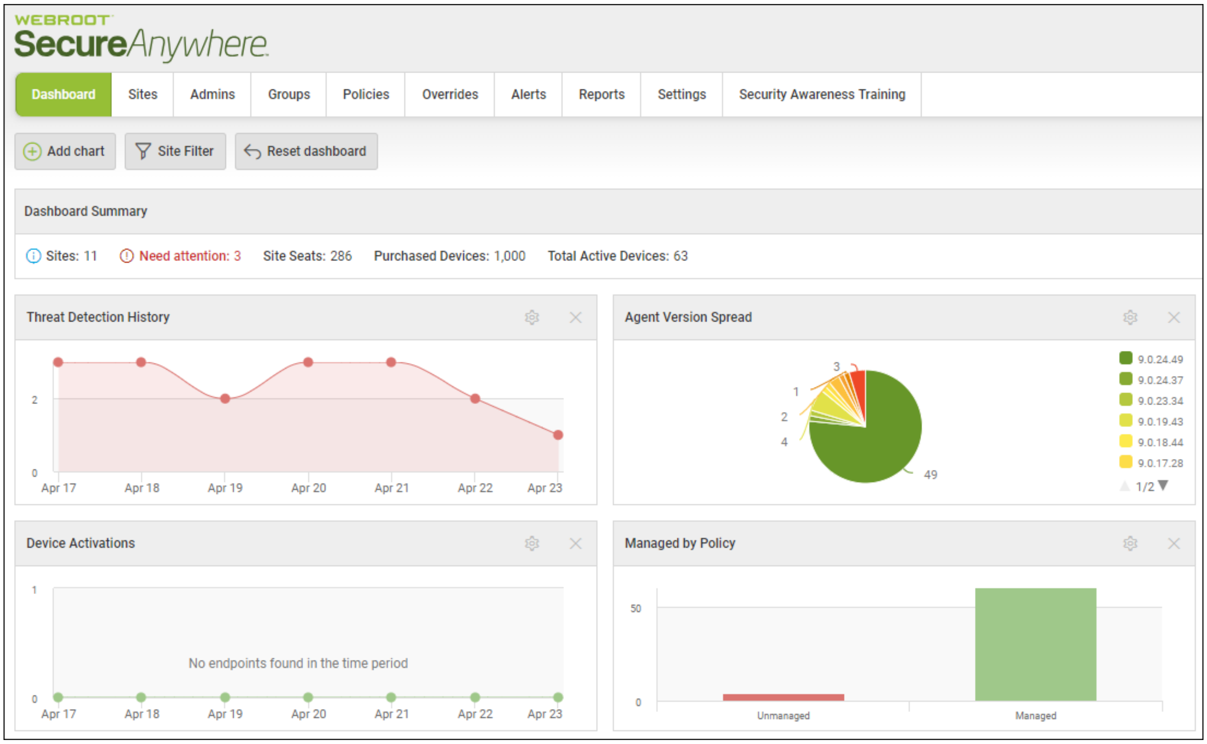
2. Click the **Dashboard** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

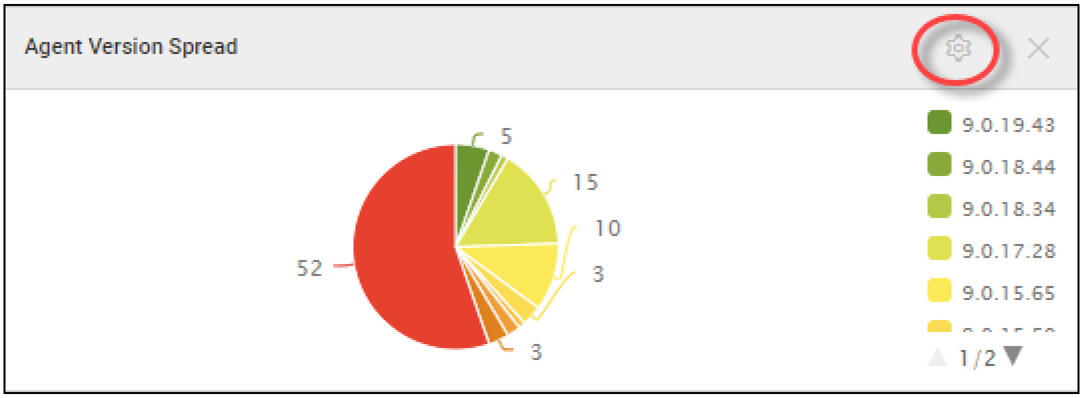
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

   The Dashboard tab displays.

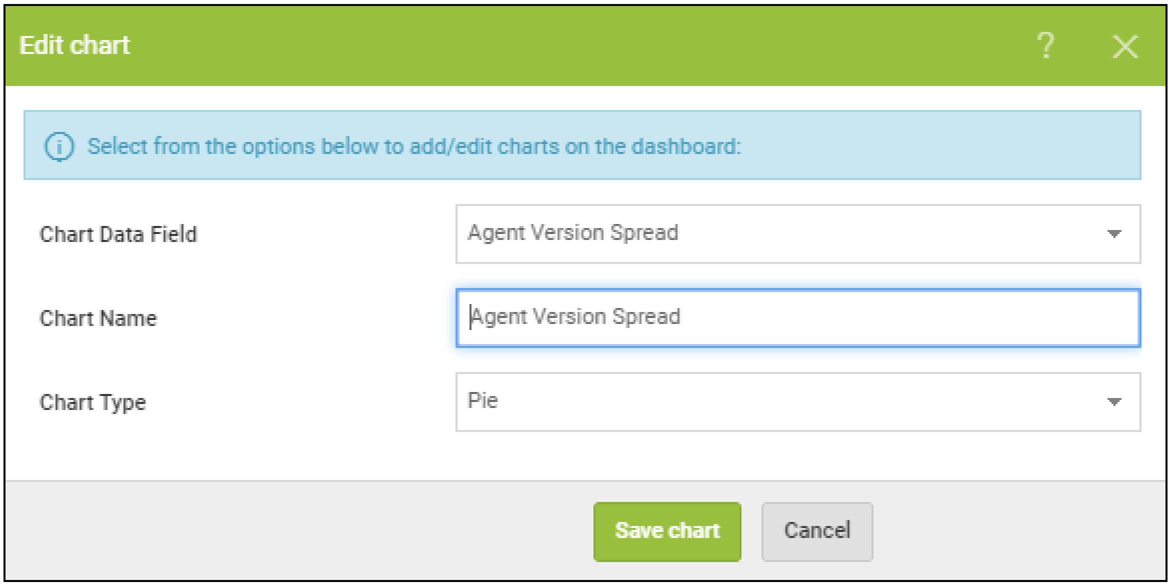


Sites: 11 Need attention: 3 Site Seats: 286 Purchased Devices: 1,000 Total Active Devices: 63

3. For the chart that you want to edit, in the upper right corner of the chart, click the **Gear** icon.



The Edit chart window displays.



Select from the options below to add/edit charts on the dashboard:

Chart Data Field: Agent Version Spread

Chart Name: Agent Version Spread

Chart Type: Pie

4. From the Chart Data Field drop-down field, select any of the following options:

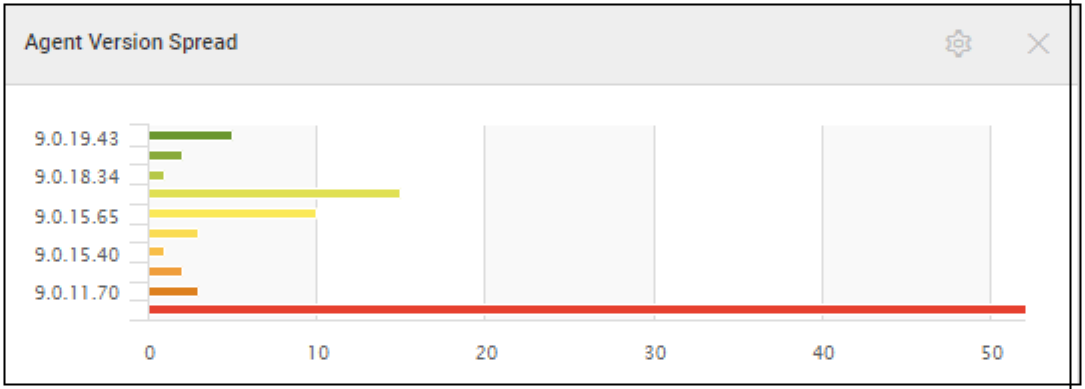
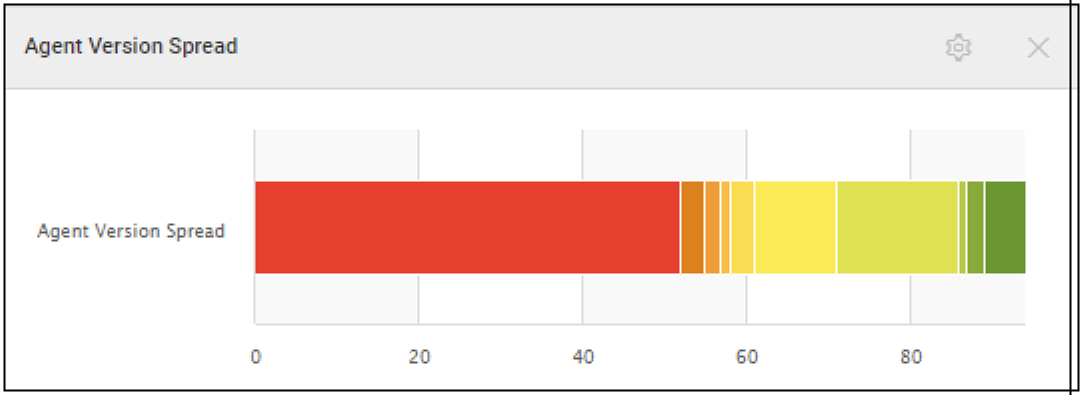
| | | | |
|---|---|---|---|
| Agent Version Spread | Firewall Status | Operating System Language | Rootkit Shield Status |
| Attention Required | Identity Shield Status | Operating System Platform | Scheduled Scans Status |
| Device Activations | Infrared Status | Phishing Shield Status | Silent Mode |
| Device Type | Installation Status | Primary Browser | Threat Detection History |
| Endpoint Status | Managed by Policy | Realtime Shield Status | USB Shield Status |
| Expired Status | Offline Shield Status | Remediation Status | Web Threat Shield Status |

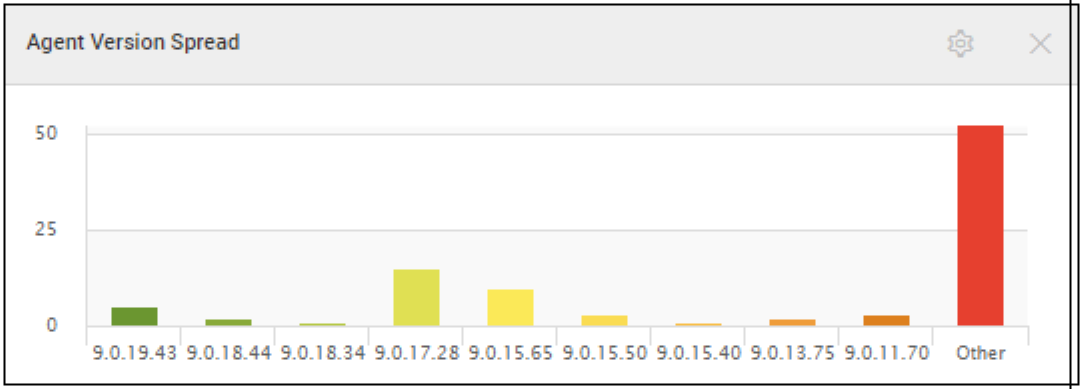
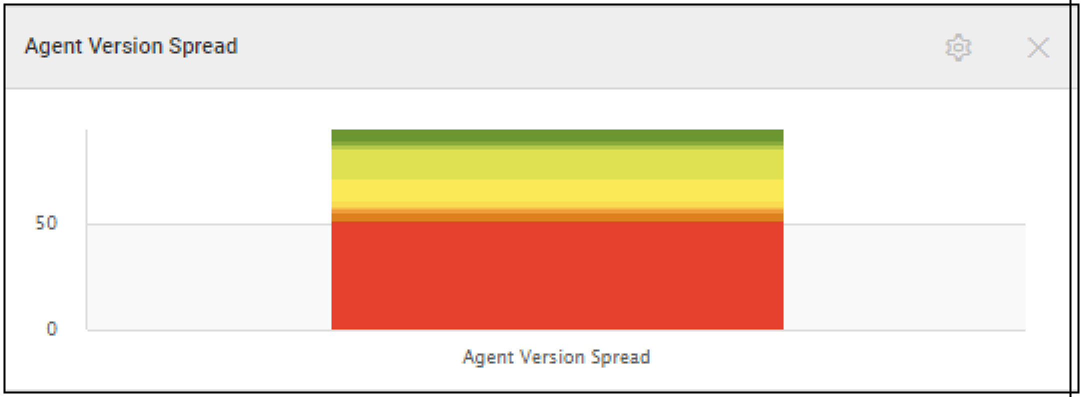
**Note:** The following data points are unsupported in the Mac agent: Firewall Status, Rootkit Shield Status, Infared Status. Silent Mode, Offline Shield Status.

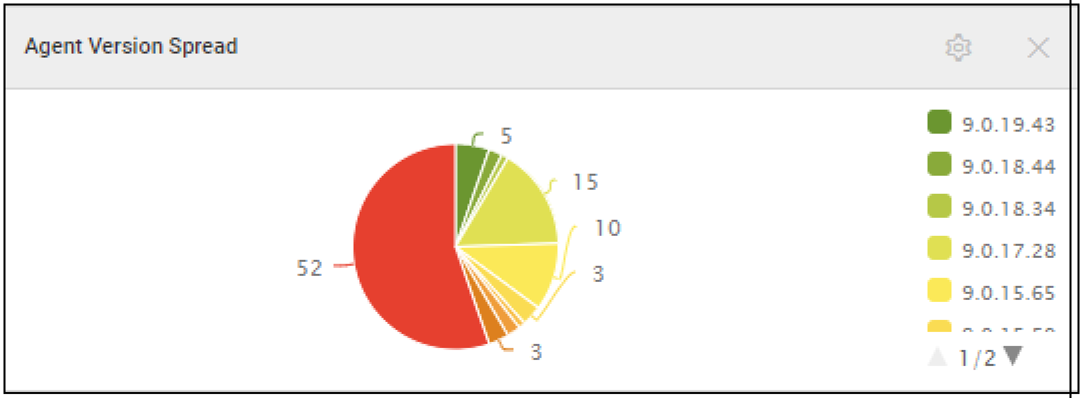
5. In the Chart Name field, enter the name of the chart.

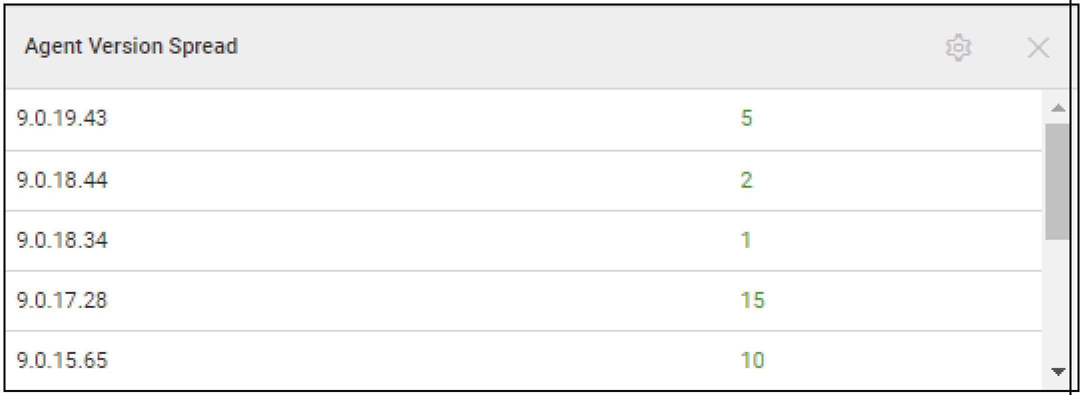
   Typically, the name of the chart reflects the name of the type of information within it, but this is a free-form field, and you can name the chart something else, as needed.

6. From the Chart Type drop-down menu, select one of the following chart types.

| NAME | DESCRIPTION |
|---|---|
| Bar |  |
| Bar Stacked |  |

| NAME | DESCRIPTION |
|---|---|
| **Column** |   Agent Version Spread<br>50<br>25<br>0<br>9.0.19.43<br>9.0.18.44<br>9.0.18.34<br>9.0.17.28<br>9.0.15.65<br>9.0.15.50<br>9.0.15.40<br>9.0.13.75<br>9.0.11.70<br>Other |
| **Column Stacked** |  |

<table>
<tr><th>NAME</th><th>DESCRIPTION</th></tr>
<tr><td><b>Pie</b></td><td>


</td></tr>
<tr><td><b>Table</b></td><td>

Agent Version Spread
<table>
<tr><td>9.0.19.43</td><td>5</td></tr>
<tr><td>9.0.18.44</td><td>2</td></tr>
<tr><td>9.0.18.34</td><td>1</td></tr>
<tr><td>9.0.17.28</td><td>15</td></tr>
<tr><td>9.0.15.65</td><td>10</td></tr>
</table>
</td></tr>
</table>

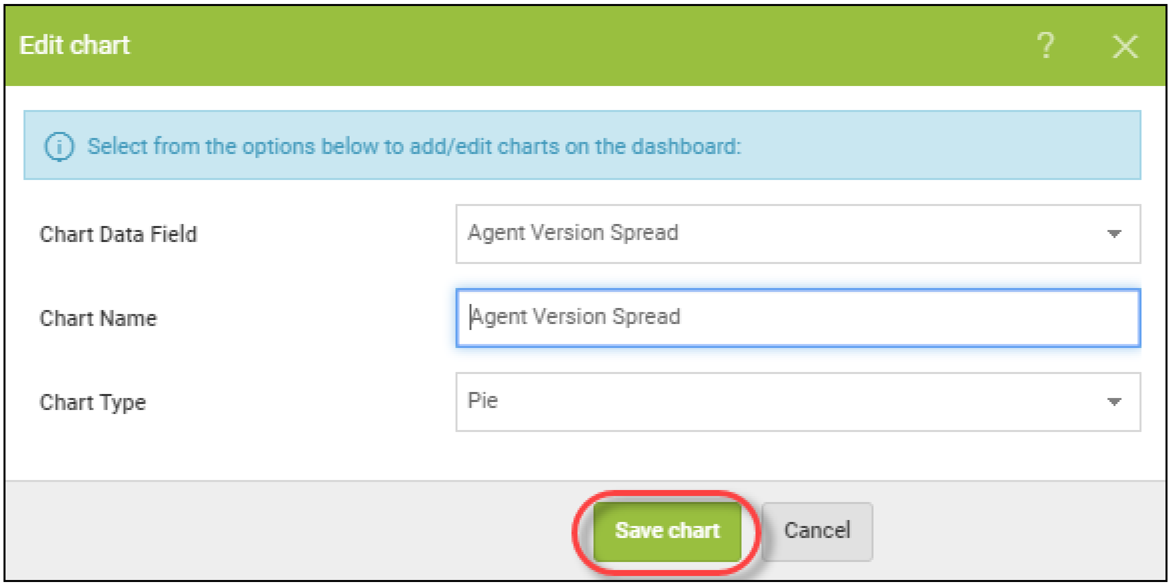
7. If you are editing the Threats Detection History or Device Activation dashboard charts, you can select from the following chart types:

- Area
- Area Spline
- Column
- Line
- Table

8. If you are editing the Threats Detection History or Device Activation dashboard charts, from the Period drop-down menu, select one of the following:

| | | | |
|---|---|---|---|
| 24 hours | 2 days | 3 days | 7 days |
| 14 days | 30 days | 60 days | 90 days |

9. When you are finished, click the **Save chart** button.



Select from the options below to add/edit charts on the dashboard:

Chart Data Field: Agent Version Spread

Chart Name: Agent Version Spread

Chart Type: Pie

**Note:** For information on deleting dashboard charts, see *Deleting Dashboard Charts on page 65*.

# Drilling Down in Dashboard Charts

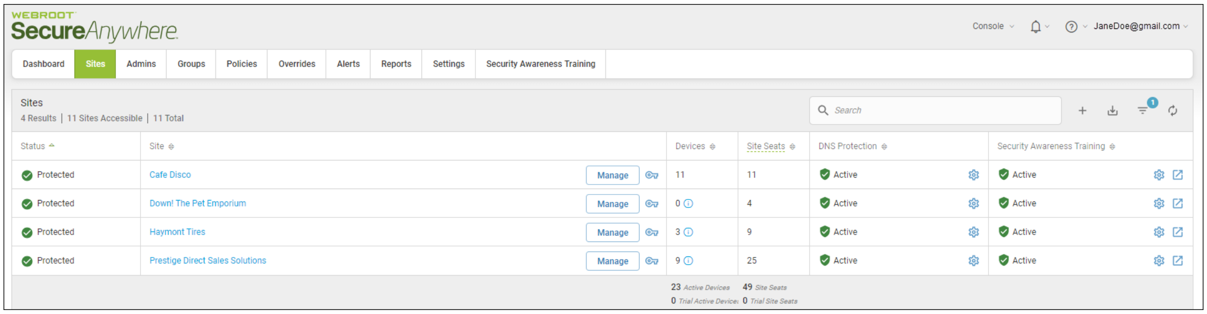
Follow this procedure to drill down into a dashboard to display additional information such as:

- Endpoint information
- Status of deployments

**To drill down in a dashboard chart:**

1. Log in to the management console.

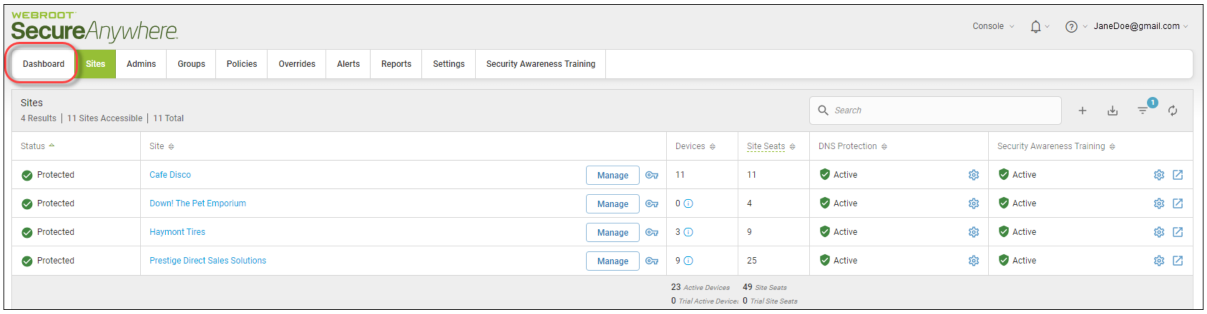
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

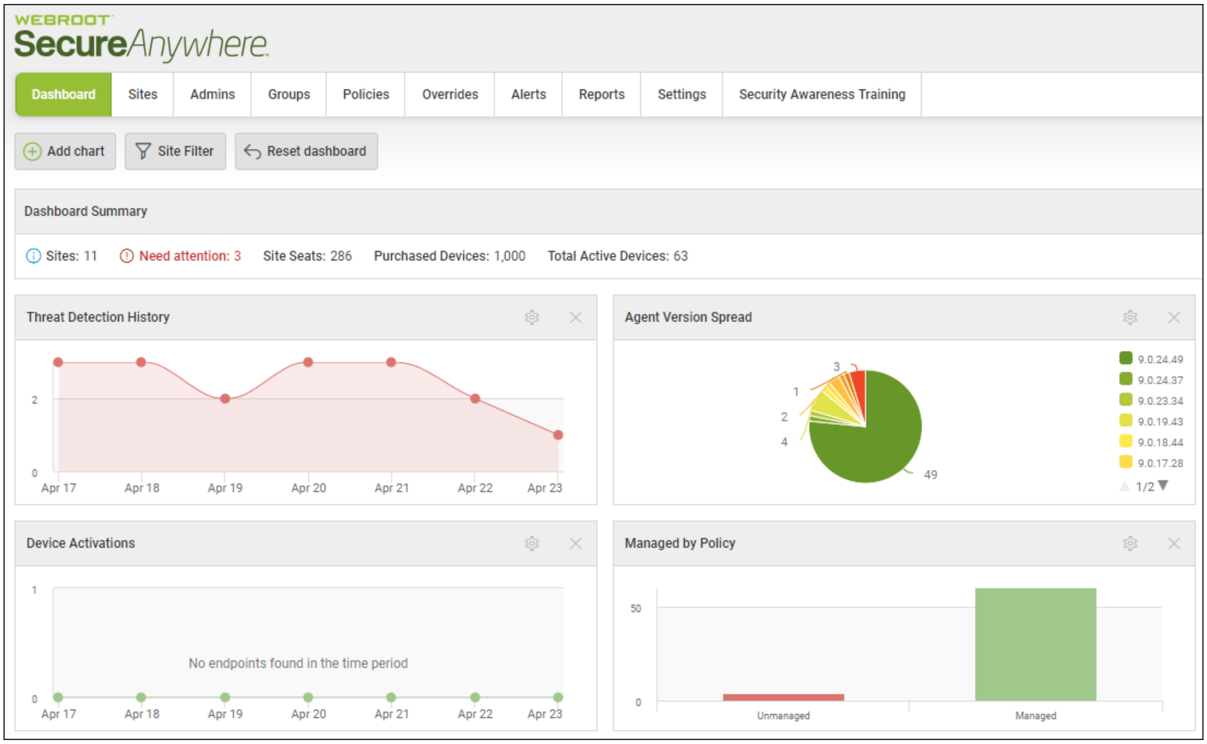
2. Click the **Dashboard** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

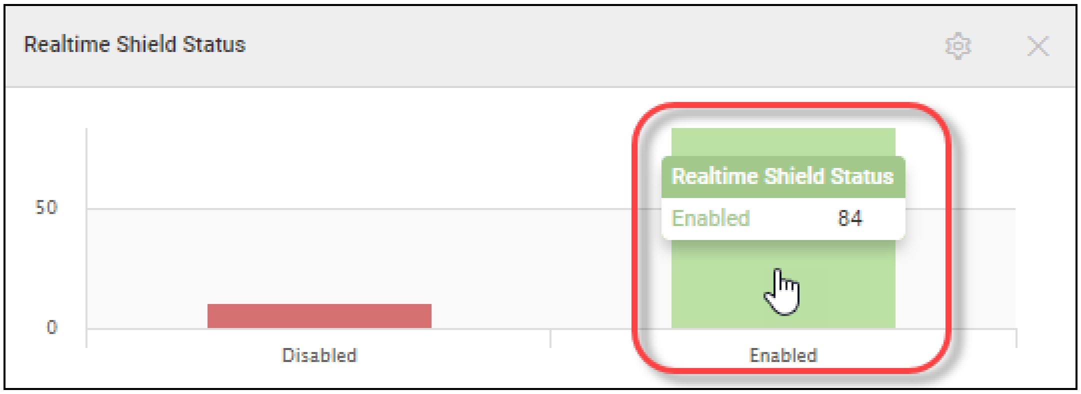
The Dashboard tab displays.



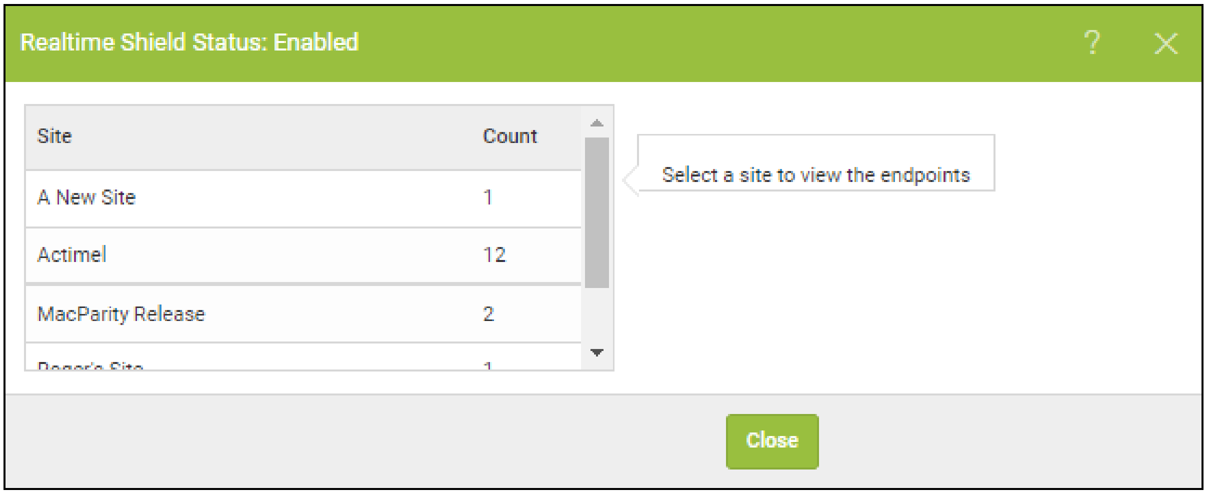
Dashboard Summary

Sites: 11 Need attention: 3 Site Seats: 286 Purchased Devices: 1,000 Total Active Devices: 63

3. Click on the chart that you want to drill down.



The first level of the drill-down displays, and includes information about the site name and the number of endpoints that the site has.

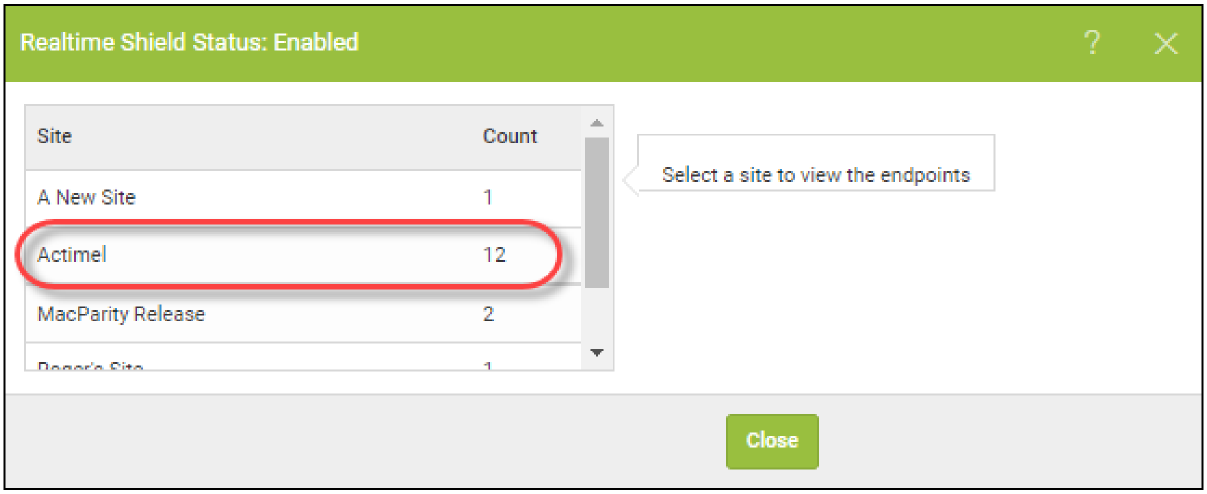


Realtime Shield Status: Enabled

| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 12 |
| MacParity Release | 2 |
| Roger's Site | 1 |

Select a site to view the endpoints

4. In the Site column, click on the site name to display the second level of drill-down.

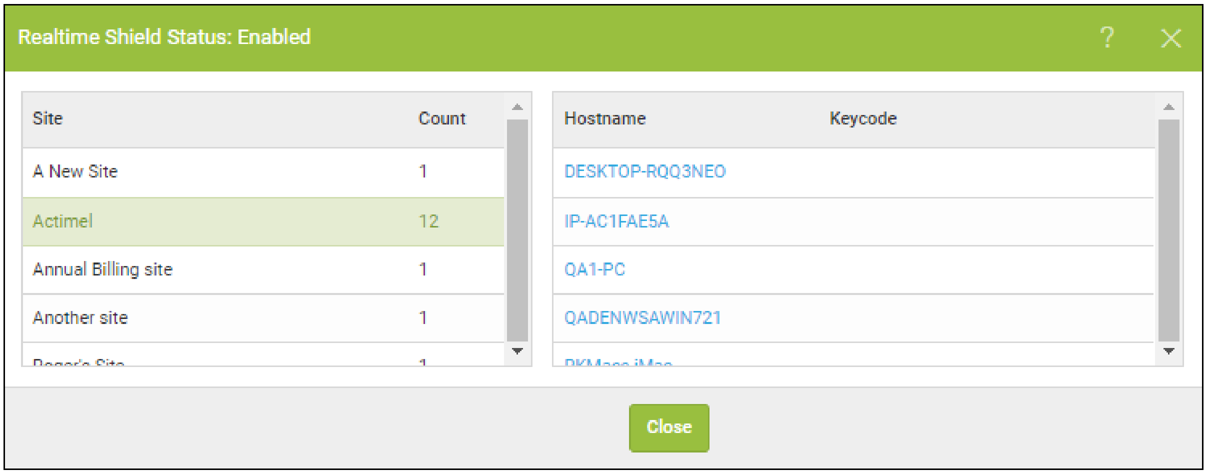


Realtime Shield Status: Enabled

| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 12 |
| MacParity Release | 2 |
| Roger's Site | 1 |

Select a site to view the endpoints

The drill-down expands to include information about the host name and the keycode associated with each endpoint.

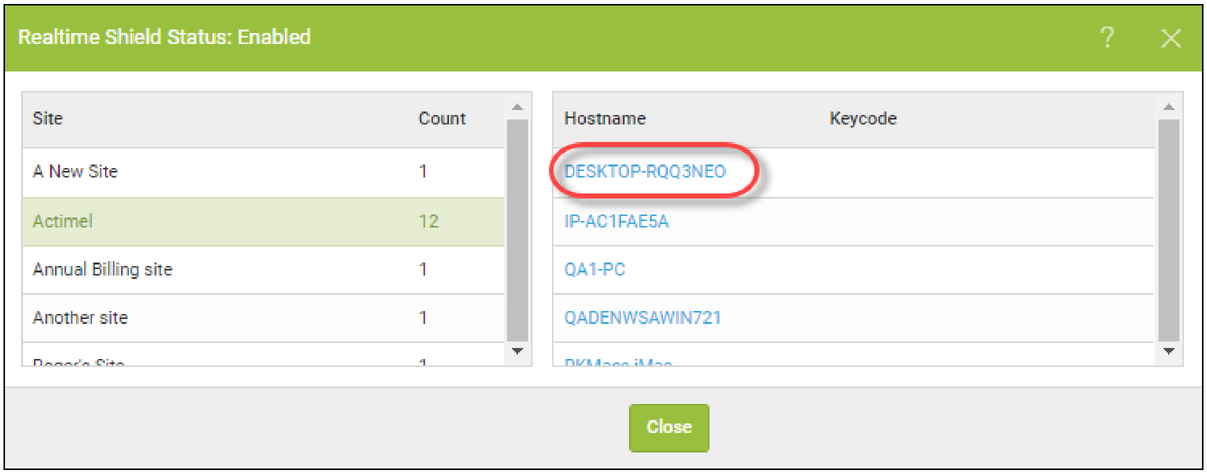


Realtime Shield Status: Enabled

| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 12 |
| Annual Billing site | 1 |
| Another site | 1 |
| Roger's Site | 1 |

| Hostname | Keycode |
|---|---|
| DESKTOP-RQQ3NEO | |
| IP-AC1FAE5A | |
| QA1-PC | |
| QADENWSAWIN721 | |
| PKMacs iMac | |

5. In the Hostname column, click on the host name to display in-depth information about the host.



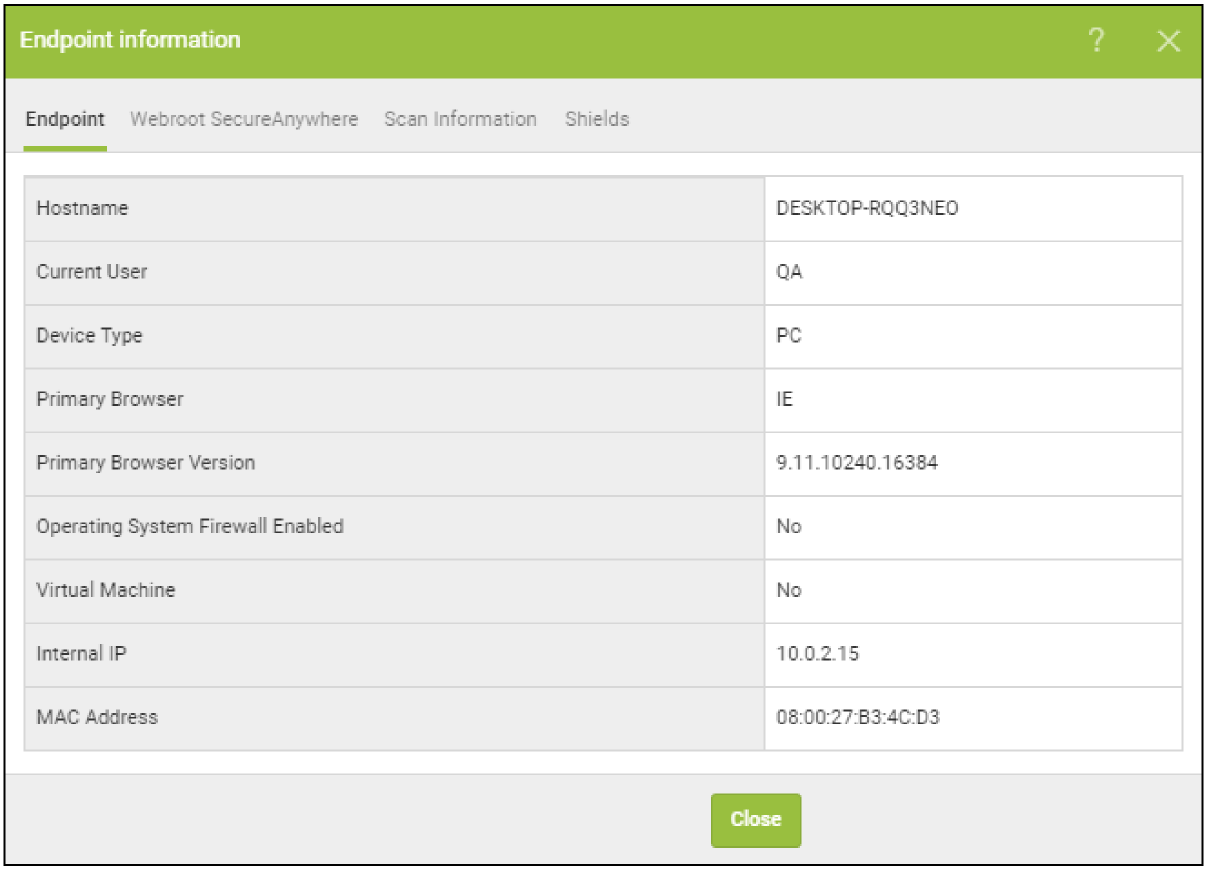
Realtime Shield Status: Enabled

| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 12 |
| Annual Billing site | 1 |
| Another site | 1 |
| Roger's Site | 1 |

| Hostname | Keycode |
|---|---|
| DESKTOP-RQQ3NEO | |
| IP-AC1FAE5A | |
| QA1-PC | |
| QADENWSAWIN721 | |
| PKMacs iMac | |

The Endpoint Information window displays information about the following:

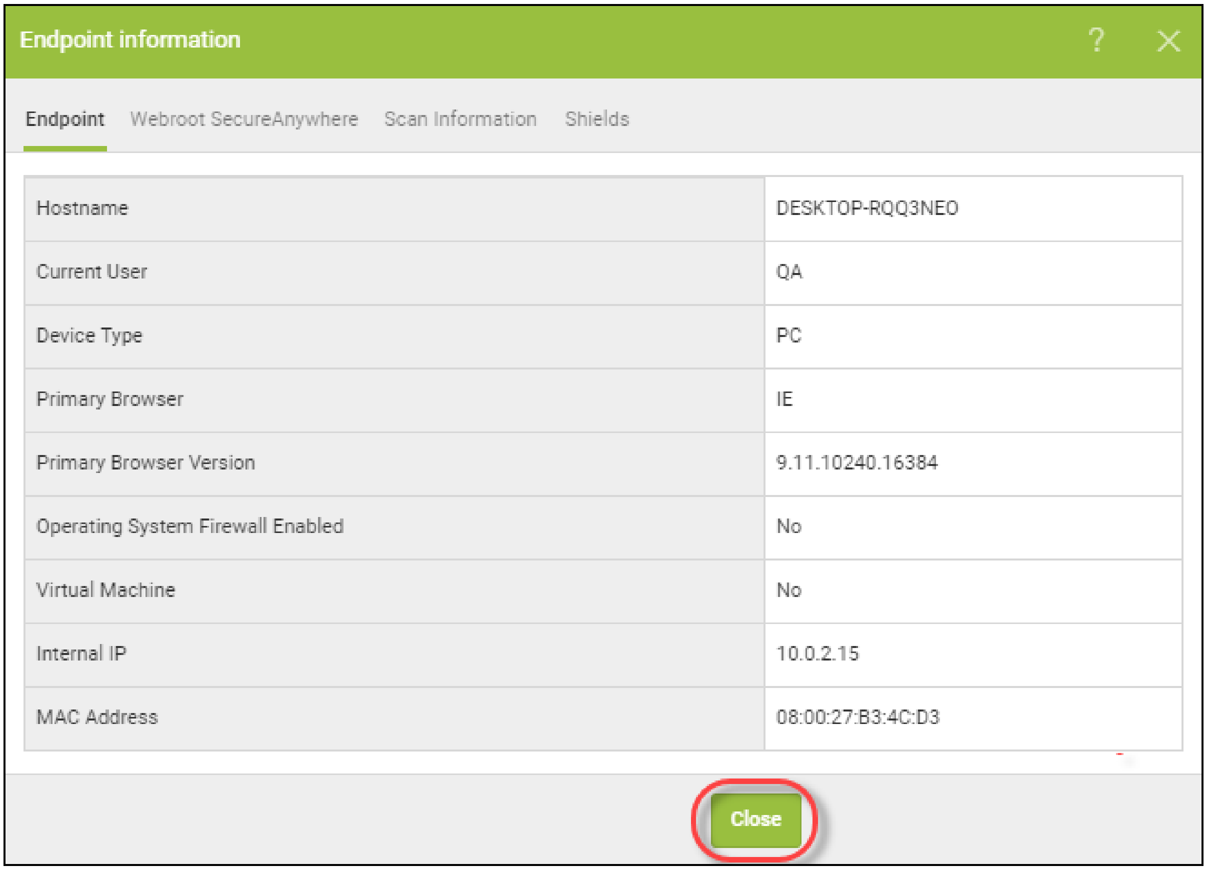
- Endpoint
- Webroot SecureAnywhere
- Scan Information
- Shields



| | |
|---|---|
| Hostname | DESKTOP-RQQ3NEO |
| Current User | QA |
| Device Type | PC |
| Primary Browser | IE |
| Primary Browser Version | 9.11.10240.16384 |
| Operating System Firewall Enabled | No |
| Virtual Machine | No |
| Internal IP | 10.0.2.15 |
| MAC Address | 08:00:27:B3:4C:D3 |

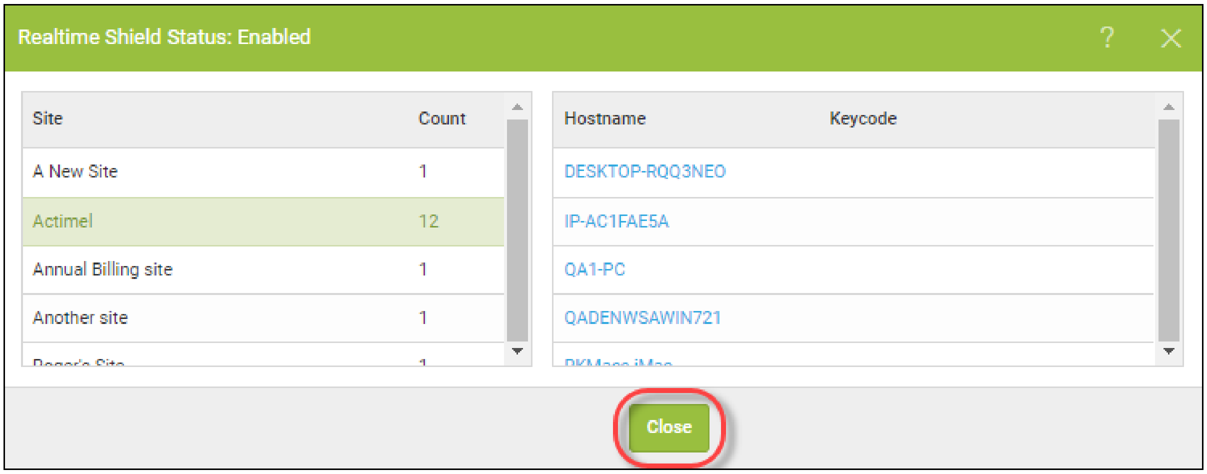
**Note:** The following data points are unsupported in the Mac agent: Firewall Status, Rootkit Shield Status, Infared Status. Silent Mode, Offline Shield Status.

6. When you are done, click the **Close** button to return to the drill-down window.



| | |
|---|---|
| Hostname | DESKTOP-RQQ3NEO |
| Current User | QA |
| Device Type | PC |
| Primary Browser | IE |
| Primary Browser Version | 9.11.10240.16384 |
| Operating System Firewall Enabled | No |
| Virtual Machine | No |
| Internal IP | 10.0.2.15 |
| MAC Address | 08:00:27:B3:4C:D3 |

7. Then on the drill-down window, click the **Close** button to return to the main dashboard.



Realtime Shield Status: Enabled

| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 12 |
| Annual Billing site | 1 |
| Another site | 1 |
| Roger's Site | 1 |

| Hostname | Keycode |
|---|---|
| DESKTOP-RQQ3NEO | |
| IP-AC1FAE5A | |
| QA1-PC | |
| QADENWSAWIN721 | |
| PKMacs-iMac | |

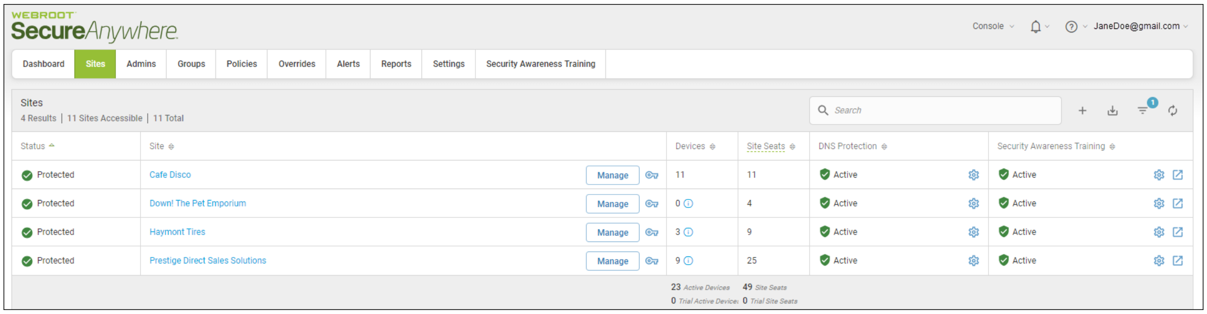
# Deleting Dashboard Charts

Follow this procedure to delete any dashboard charts that you no longer need.

**To delete a dashboard chart:**

1. Log in to the management console.

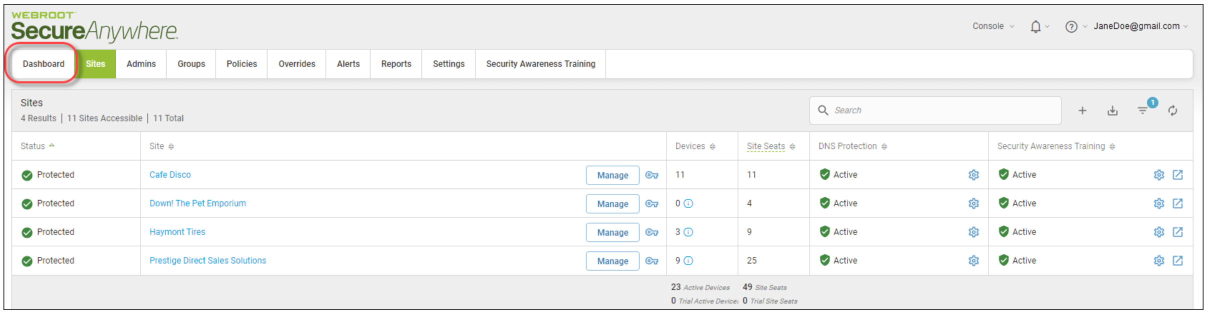
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

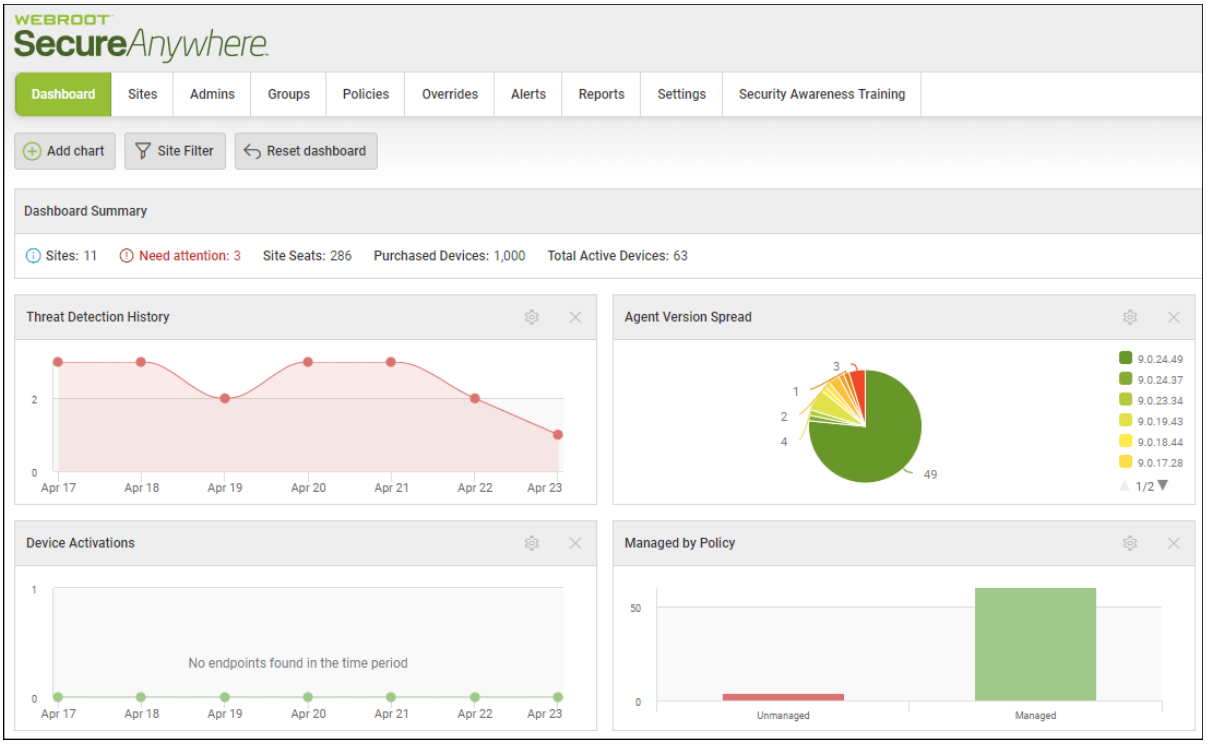
2. Click the **Dashboard** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

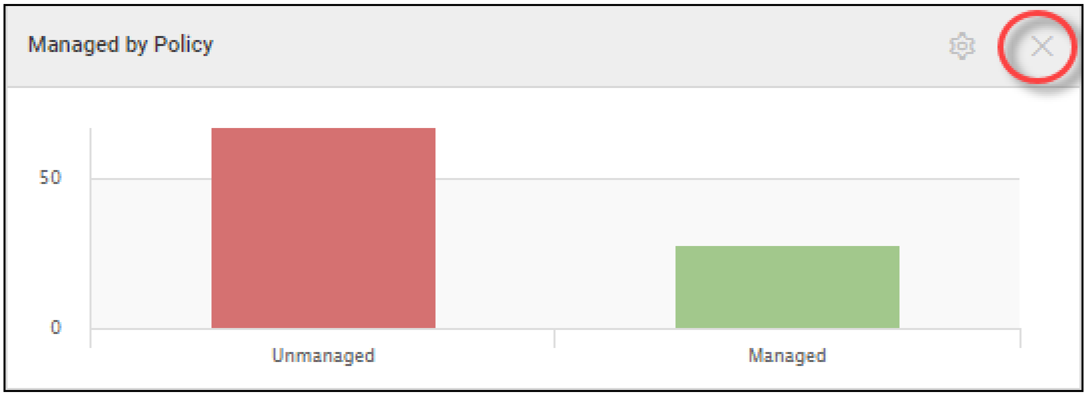
   The Dashboard tab displays.



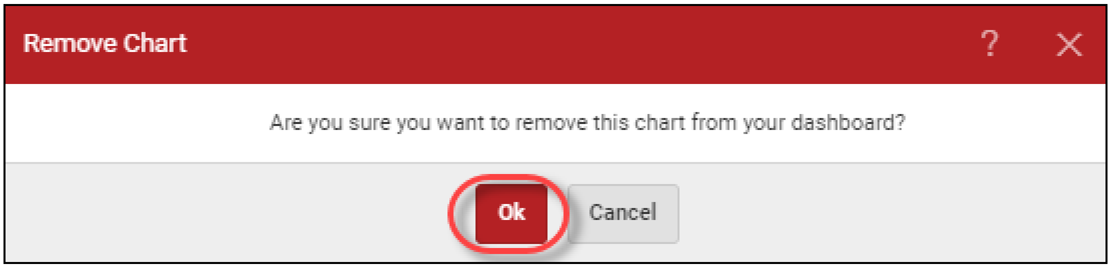
Dashboard Summary

Sites: 11 Need attention: 3 Site Seats: 286 Purchased Devices: 1,000 Total Active Devices: 63

3. For the chart that you want to delete, in the upper right corner of the chart, click the **X** icon.



4. When the Remove Chart message displays, to confirm the deletion, click the **OK** button.



Remove Chart

Are you sure you want to remove this chart from your dashboard?

The system removes the chart from your dashboard.

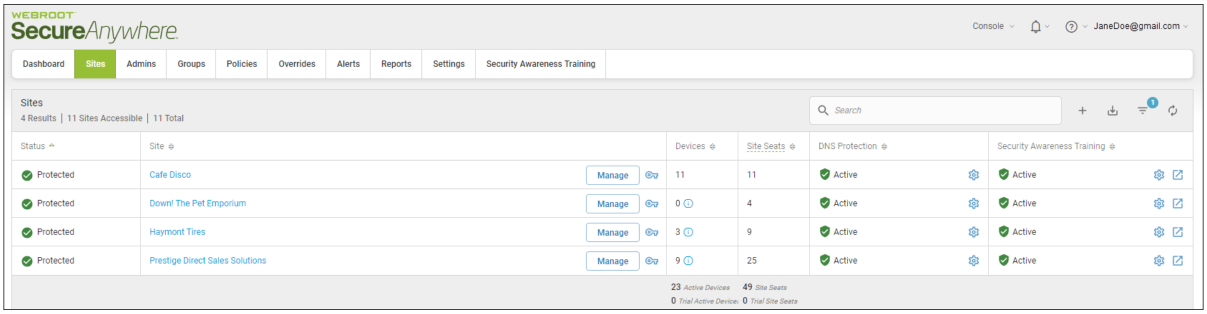
**Note:** For information about creating and editing dashboard charts, see and *Editing Dashboard Charts on page 51*.

# Chapter 3: Working With Sites

To work with sites, see the following topics:

# Management Console Sites Tab Overview

The Sites tab on the management console displays a list of all of your sites, with information about number of seats, settings, etc.



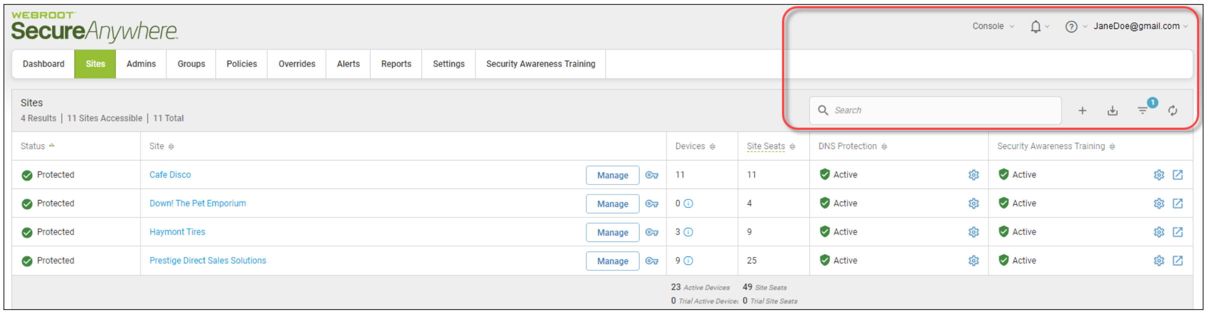
Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

In the upper right corner of the console is the following information and functionality:

- **Name of the Console** — Displays the name of the console and lets you rename and change the console you are viewing. For more information, see *Renaming Consoles on page 32* and *Changing Consoles on page 28*.
- **Bell Icon** — Displays any alerts and updates.
- **Question Mark Icon** — Displays a drop-down menu with the following options:
  - **Help Documentation** — Displays the online guide related to the console you are viewing.
  - **DNS Help Documentation** — Displays the online guides for DNS Protection.
  - **Webroot Education Videos** — Takes you to Webroot's YouTube channel.
  - **Product Training** — Takes you to the Webroot Partner Certification website.
  - **Service Status** — Takes you to a website that displays the status of all known incidents.
  - **Spotlight Tour** — Takes you through a tour of the management console. For more information, see *About the Spotlight Tour on page 22*.
  - **Support** — Displays the Contact Support page, where you can enter a support ticket.
- **User Name Drop-Down** — Includes a Logout button.
- **Search Field** — Lets you enter information to search on. For more information, see *Searching for Sites on page 86*.
- **Add Site Button** — Lets you add sites to your dashboard. For more information, see *Adding Sites on page 73*.
- **Download Button** — Let's you download CSV files. For more information, see *Downloading CSV Files on page 88*.

- **Filters Button** — Lets you chose a set of criteria to filter sites upon, and then display only sites that match that criteria. For more information, see *Filtering Sites on page 81*.
- **Refresh Sites Button** — Refreshes the information on the console.

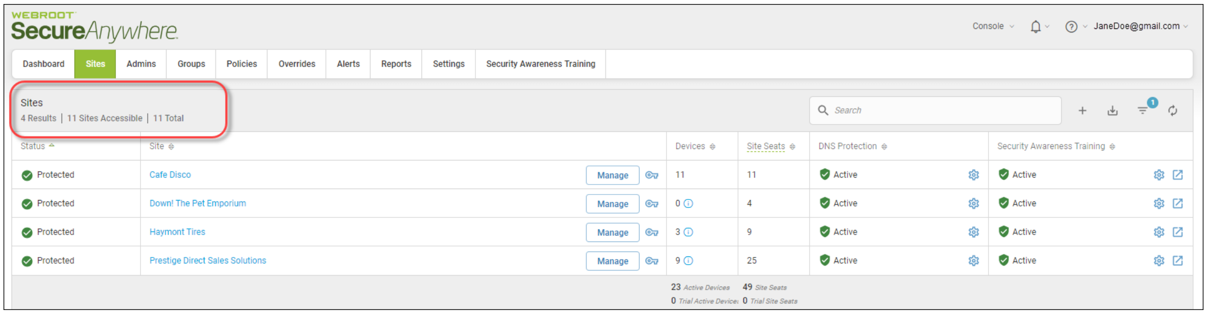


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

The top row contains the following information and functionality:

- **Results** — Displays the number of sites that are returned, based on your filter settings.
- **Sites Accessible** — Displays the number of sites that the logged-on user has access to.
- **Total** — Displays the number of sites that are active under the current management console.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

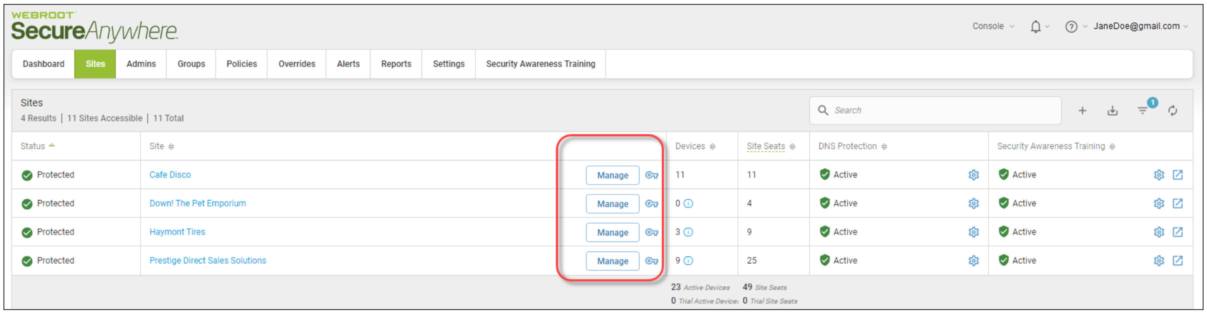
The columns display the following information and functionality:

- **Status** — Displays one of the following statuses:
  - Protected
  - Suspended
  - Expired
  - Needs Attention
  - Deactivated

- **Site** — The name of the company. This information is entered when you create a site. For more information, see *Adding Sites on page 73*. You can edit the name of the company, also. For more information, see *Editing Site Details on page 114*.

- **Manage Button** — Click to display additional information about each site. For more information about the actions that are available when you click the **Manage** button, see the following topics:

  - *Viewing Site Summaries on page 92*
  - *Suspending and Resuming Site Protection on page 108*
  - *Deactivating Site Protection on page 111*
  - *Editing Site Details on page 114*
  - *Editing Site Settings on page 136*
  - *Setting Site-Level Data Filters on page 142*
  - *Tagging Sites on page 122*
  - *Updating Site Admin Permissions on page 132*



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

> **Note:** Click the Manage button to access the Endpoint Protection console. For more information, see *Accessing the Endpoint Console on page 36*.

- **Keycode** — The site's keycode; click the **Key** icon to display the keycode. This information is entered when you create a site. For more information, see *Adding Sites on page 73*. You can edit the name of the company, also. For more information, see *Editing Site Details on page 114*.

- **Devices** — The number of devices for that site. This information is entered when you create a site. For more information, see *Adding Sites on page 73*. You can edit the name of the company, also. For more information, see *Editing Site Details on page 114*.

> **Note:** If there is an Exclamation icon (!) next to the number of devices, it means that a data filter has been applied other than the Show All Data. For more information, see *Setting Site-Level Data Filters on page 142*.

- **Site Seats** — The number of seats that have been allocated for that site. This information is entered when you create a site. For more information, see *Adding Sites on page 73*. You can edit the name of the company, also. For more information, see *Editing Site Details on page 114*.
- **DNS Protection** — Displays whether or not DNS Protection has been activated. For more information, see *DNS Protection Overview on page 559*.
- **Security Awareness Training** — Displays whether or not Security Awareness Training has been activated. For more information, see *Security Awareness Training Overview on page 568*.

# Adding Sites

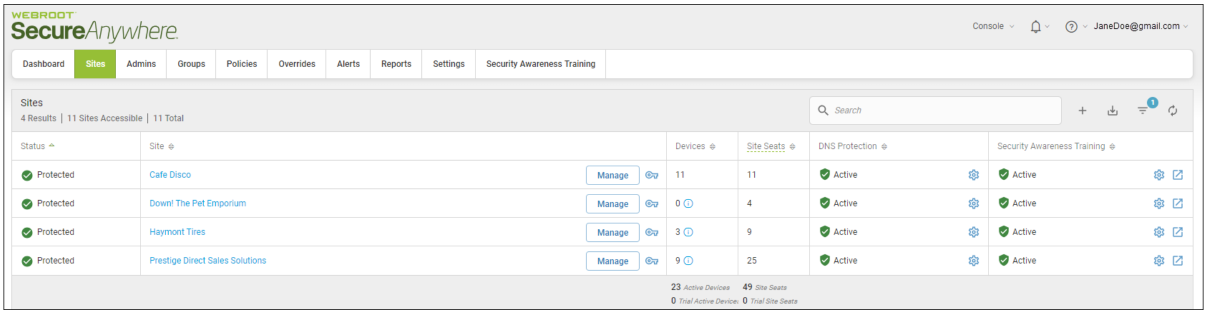
Use this procedure to add sites to the management console. For information on editing site information, see any of the following:

- *Editing Site Details on page 114*
- *Updating Site Admin Permissions on page 132*
- *Editing Site Settings on page 136*

**To add a site:**

1. Log in to the management console.

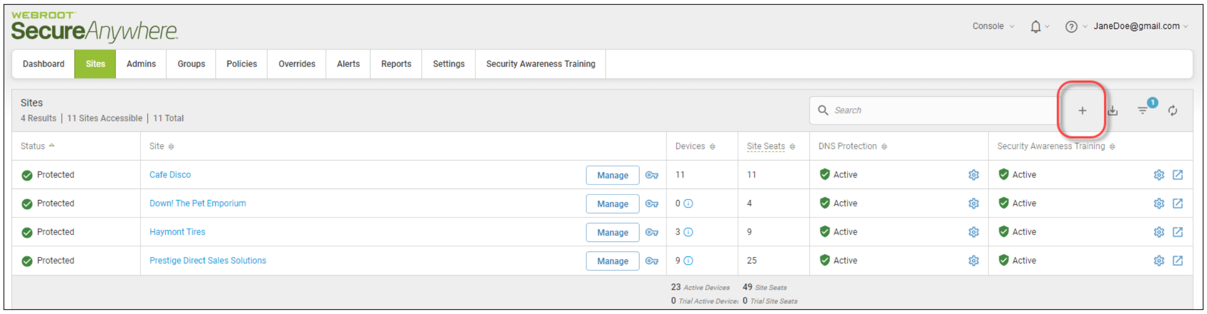
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats |  |  |

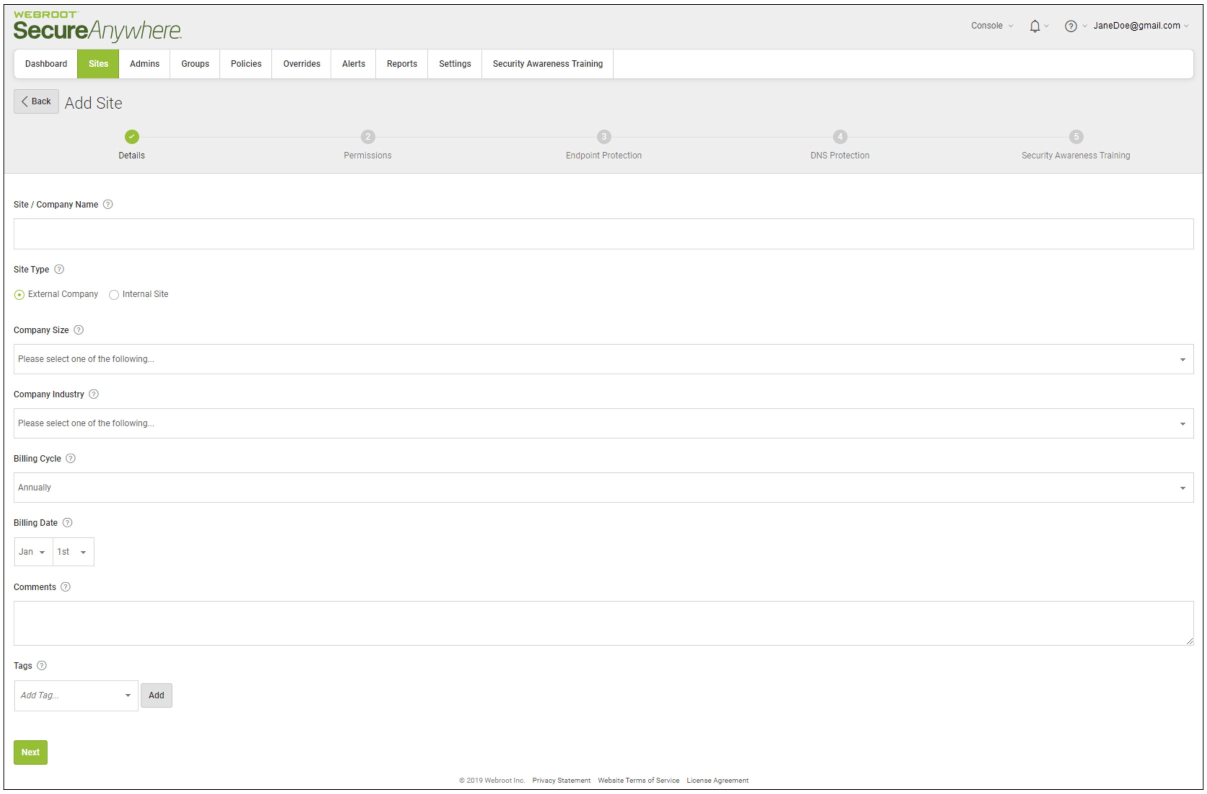
2. Click the **Add Site** button.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats |  |  |

The Add Site panel displays with the Details area active.



Add Site

Site / Company Name

Site Type

● External Company ○ Internal Site

Company Size: Please select one of the following...

Company Industry: Please select one of the following...

Billing Cycle: Annually

Billing Date: Jan 1st

Comments

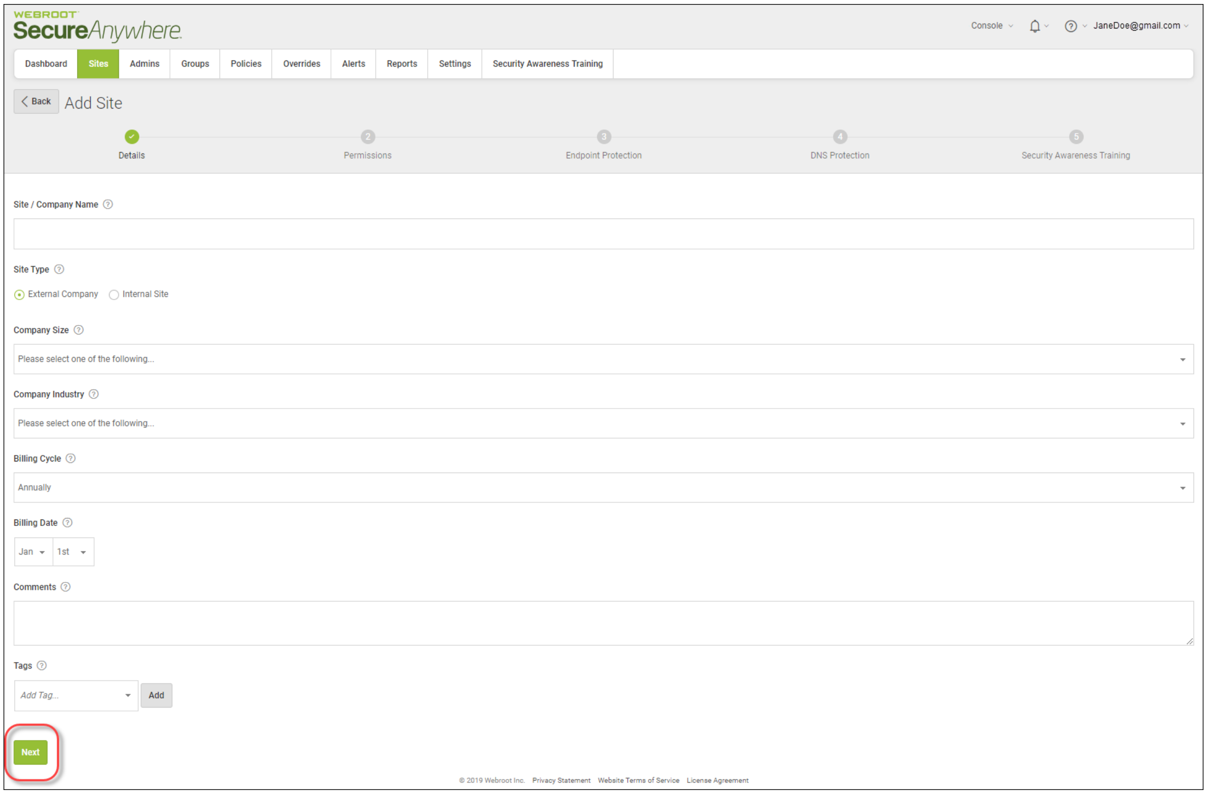
Tags: Add Tag...

3. In the Site/Company Name field, enter the name of the site.
4. In the Site Type field, do one of the following:
   - If you are creating a site that is an external customer purchasing services from you, select the **External Company** radio button, then continue with step 5.
   - If you are creating a site that is an additional location or office within your own company, select the **Internal Site** radio button, then click the **Next** button, and continue with step 9.

> **Note:** If you selected the Internal Site radio button, the Company Size, Company Industry, Billing Cycle, and Billing Date fields do not display, and you do not have to populate them.

5. In the Company Size field, from the drop-down menu, select the range that best represents the size of your company.
6. In the Company Industry field, from the drop-down menu, select the industry that best represents your company.

7. In the Billing Cycle field, from the drop-down menu, select one of the following billing cycles:
   - **Annually**
   - **Quarterly**
   - **Monthly**
   - **Weekly**
8. In the Billing Date field, use the drop-down menus to select both the month and the date for billing.
9. In the Comments field, enter any information. This is an optional field.
10. From the Tags drop-down menu, select or add tags to associate with this site. This is an optional field.
11. When you're done, click the **Next** button.



Add Site

Site / Company Name

Site Type

● External Company ○ Internal Site

Company Size: Please select one of the following...

Company Industry: Please select one of the following...

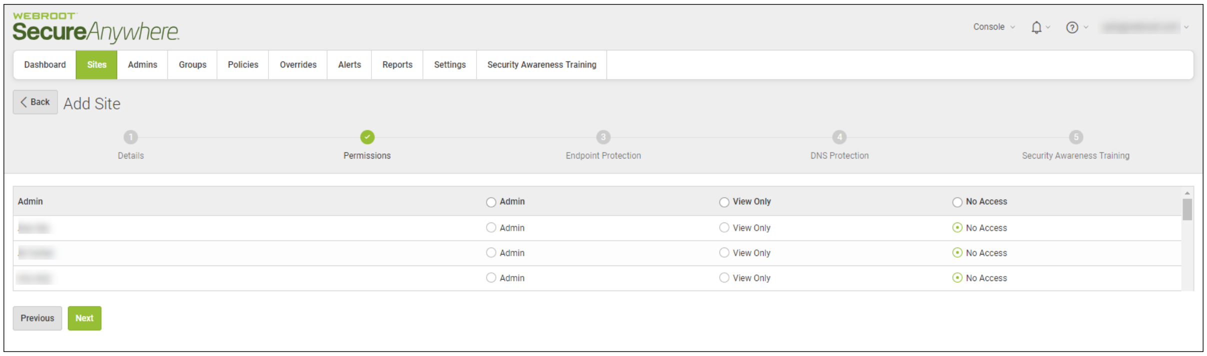
Billing Cycle: Annually

Billing Date: Jan 1st

Comments

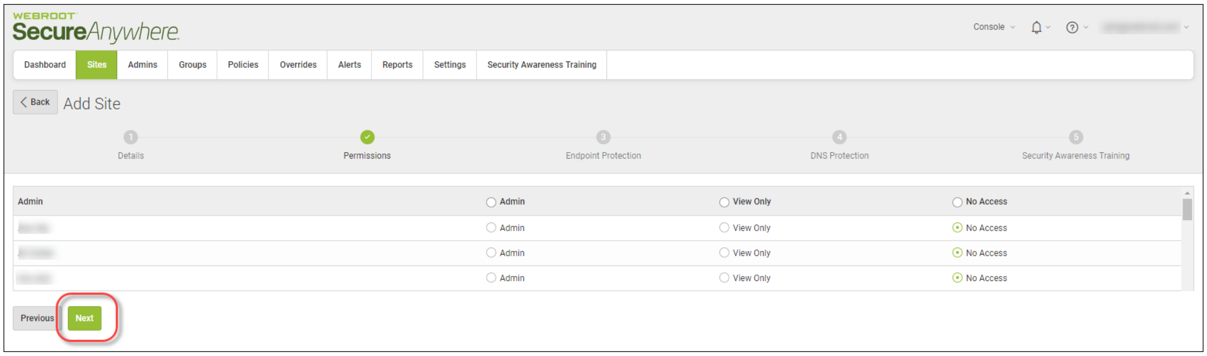
Tags: Add Tag...

The system displays the Permissions area.



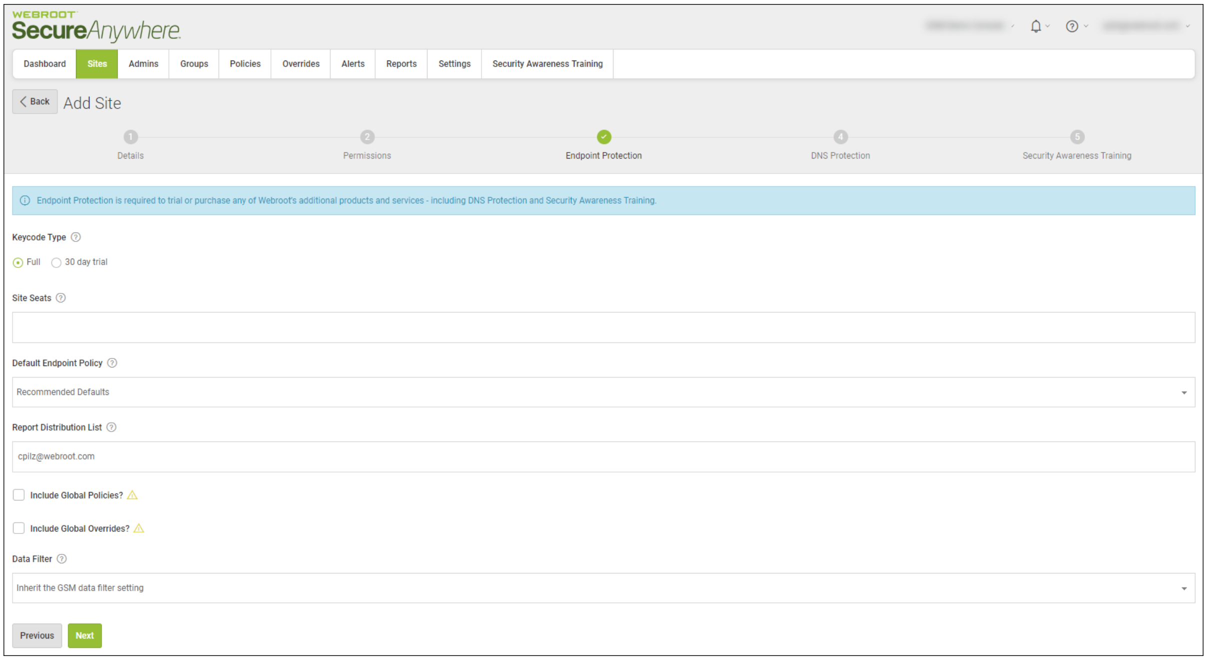
| Admin | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| [redacted] | ○ Admin | ○ View Only | ● No Access |
| [redacted] | ○ Admin | ○ View Only | ● No Access |
| [redacted] | ○ Admin | ○ View Only | ● No Access |

12. For each user at the site, select one of the following permission levels:
    - **Admin**
    - **View Only**
    - **No Access**
13. When you're done, click the **Next** button.



| Admin | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| [redacted] | ○ Admin | ○ View Only | ● No Access |
| [redacted] | ○ Admin | ○ View Only | ● No Access |
| [redacted] | ○ Admin | ○ View Only | ● No Access |

The system displays the Endpoint Protection area.



Add Site

ⓘ Endpoint Protection is required to trial or purchase any of Webroot's additional products and services - including DNS Protection and Security Awareness Training.

Keycode Type

● Full ○ 30 day trial

Site Seats

Default Endpoint Policy: Recommended Defaults

Report Distribution List: cpilz@webroot.com

□ Include Global Policies? ⚠

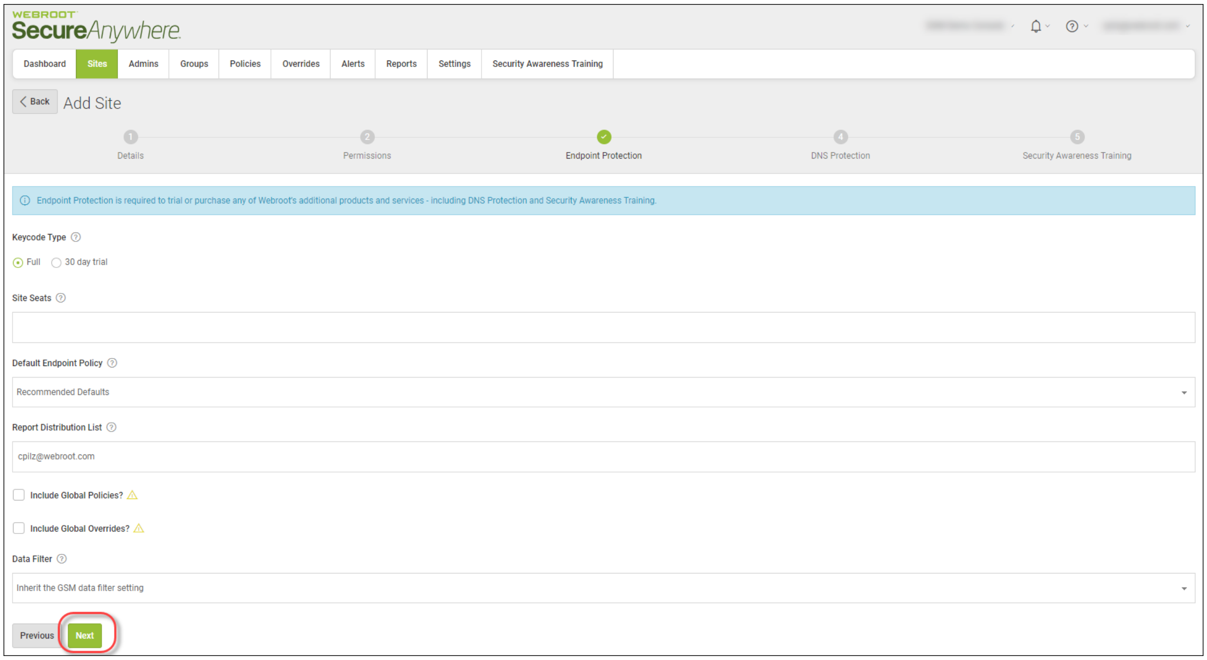
□ Include Global Overrides? ⚠

Data Filter: Inherit the GSM data filter setting

14. In the Keycode type area, select either the Full or 30 day trial radio button, depending on your needs.
15. In the Site Seats field, enter the number of seats for the new site.
16. From the Default Policy drop-down, select one of the following:
    - **Recommended Defaults**
    - **Recommended Server Defaults**
    - **Silent Audit**
    - **Unmanaged**
17. For the Include Global Policies? checkbox, do either of the following:
    - To include global policies, select the checkbox.
    - To disinclude global policies, do not select the checkbox.
18. For the Include Global Overrides? checkbox, do either of the following:
    - To include global overrides, select the checkbox.
    - To not include global overrides, do not select the checkbox.
19. In the Report Distribution List field, enter the email addresses of the individuals to whom reports will be sent.

- Use commas to separate email addresses.
- For more information on report distribution, see *Global Site Manager Reports Overview on page 441*.

20. In the Data Filter field, from the drop-down menu, select one of the filters to determine what data displays.
21. When you're done, click the **Next** button.



Endpoint Protection is required to trial or purchase any of Webroot's additional products and services - including DNS Protection and Security Awareness Training.

Keycode Type
● Full ○ 30 day trial

Site Seats

Default Endpoint Policy: Recommended Defaults

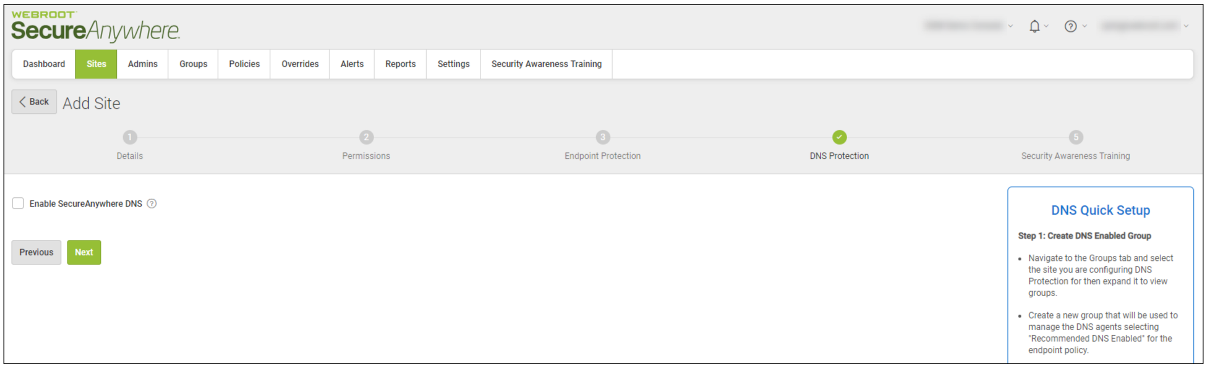
Report Distribution List: cpilz@webroot.com

□ Include Global Policies?

□ Include Global Overrides?

Data Filter: Inherit the GSM data filter setting

The system displays the DNS Protection area.



□ Enable SecureAnywhere DNS

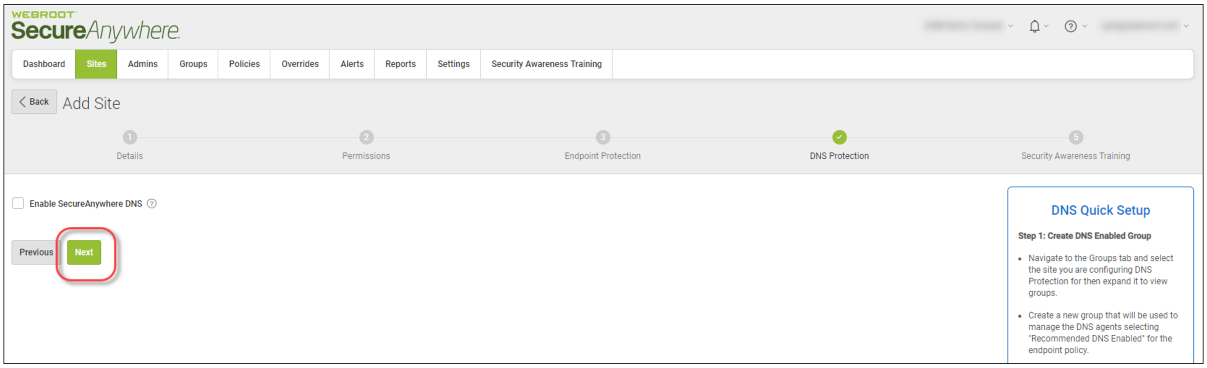
DNS Quick Setup

Step 1: Create DNS Enabled Group

- Navigate to the Groups tab and select the site you are configuring DNS Protection for then expand it to view groups.
- Create a new group that will be used to manage the DNS agents selecting "Recommended DNS Enabled" for the endpoint policy.

22. If you would like to enable DNS Protection, select the **Enable SecureAnywhere DNS** checkbox. For more information, see the SecureAnywhere DNS Protection Admin Guide.

23. When you're done, click the **Next** button.



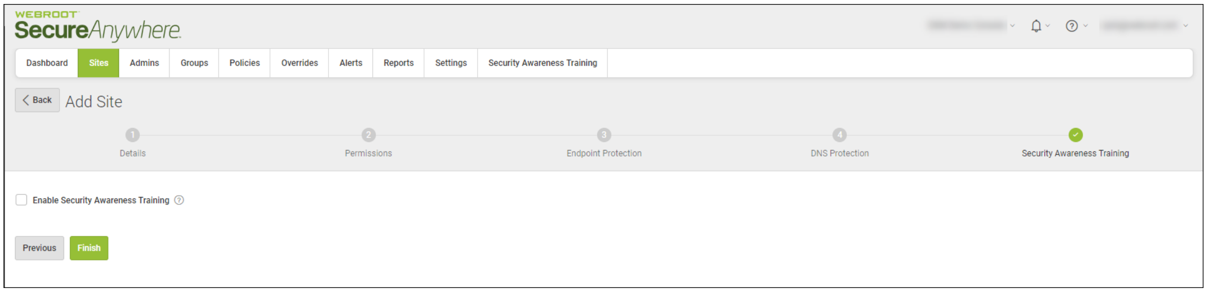
□ Enable SecureAnywhere DNS

DNS Quick Setup

**Step 1: Create DNS Enabled Group**

- Navigate to the Groups tab and select the site you are configuring DNS Protection for then expand it to view groups.
- Create a new group that will be used to manage the DNS agents selecting "Recommended DNS Enabled" for the endpoint policy.

The system displays the Security Awareness Training area.

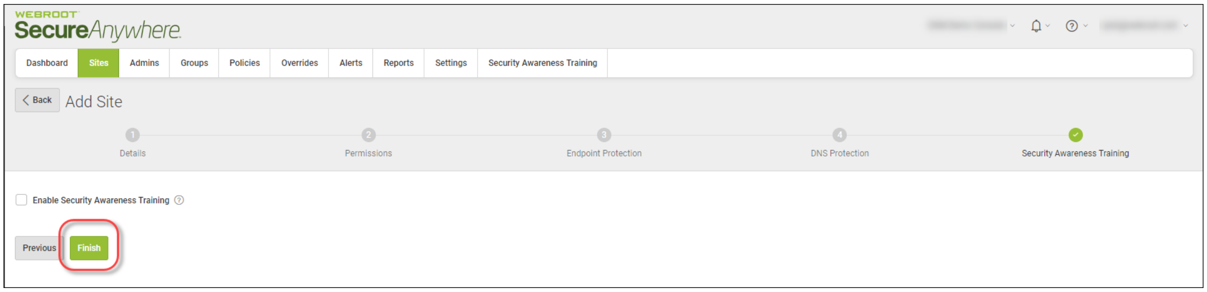


□ Enable Security Awareness Training

24. If you would like to enable Security Awareness Training, select the **Security Awareness Training** checkbox. For more information, see the Security Awareness Training online guides.
25. When you're are done, click the **Finish** button.

The system does the following:

- Creates a valid keycode
- Builds the required consoles
- Applies this keycode to the consoles
- Closes the window; the new site displays in the list on the Sites console.



Add Site

Details — Permissions — Endpoint Protection — DNS Protection — Security Awareness Training

□ Enable Security Awareness Training

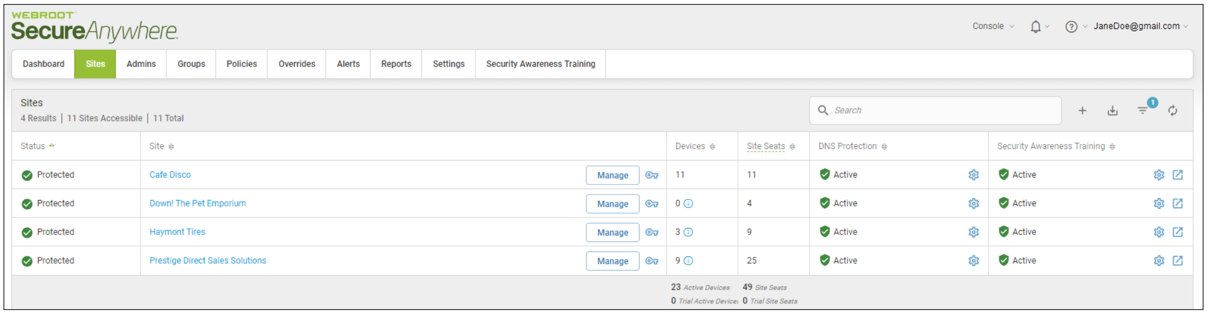
# Filtering Sites

The filter function allows admins to filter customer sites with based on the tags that were assigned to each site. Additionally, admins can filter sites based on the site name or site comments.

**To filter sites:**

1. Log in to the management console.

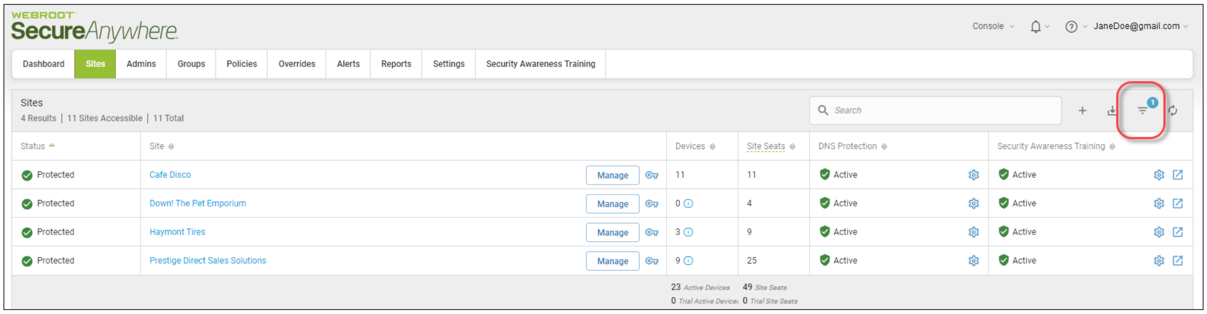
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

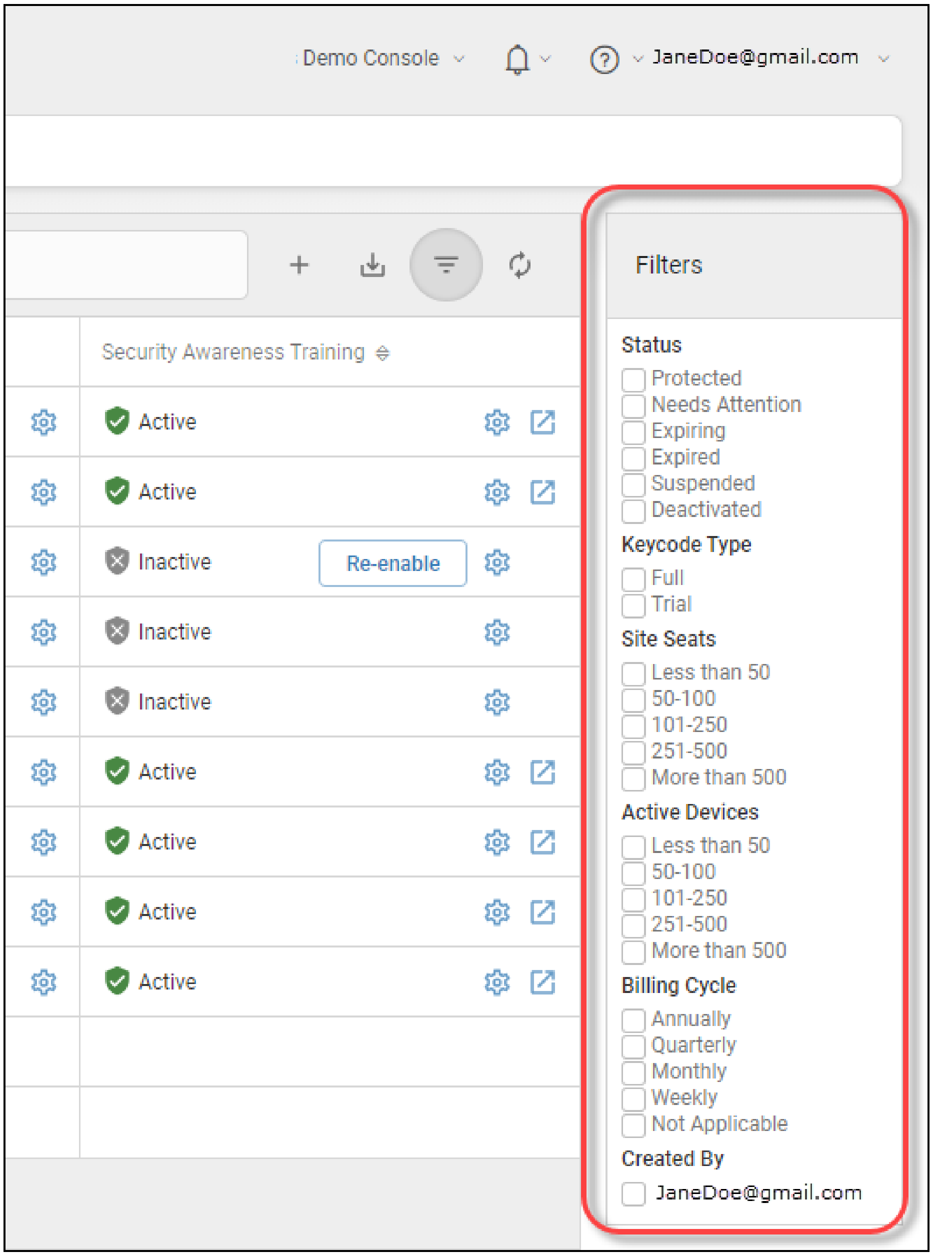
2. Click the **Filters** button.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

The system displays the Filters pane, where you can select the filters you want to apply.



**Note:** To hide the Filters pane, click the **Filters** icon again.

3. Click the button or enter information for any filter you want to apply, as described in the following table.

You can apply multiple filters.

| BUTTON | DESCRIPTION |
|---|---|
| **Status** | Select any or all of the following statuses:<br>• Protected<br>• Needs Attention<br>• Expiring<br>• Expired<br>• Suspended<br>• Deactivated |
| **Keycode Type** | Select either or both of the following keycode types:<br>• Full<br>• Trial |
| **Site Seats** | Select any or all of the following number of seats:<br>• Less than 50<br>• 50 - 100<br>• 101- 250<br>• 251 - 500<br>• More than 500 |

| BUTTON | DESCRIPTION |
|---|---|
| **Active Devices** | Select any or all of the following number of seats:<br>• Less than 50<br>• 50 - 100<br>• 101- 250<br>• 251 - 500<br>• More than 500 |
| **Billing Cycle** | Select any or all of the following billing cycles:<br>• Annually<br>• Quarterly<br>• Monthly<br>• Weekly<br>• Not applicable |
| **Created By** | Select any email address of the person who created that site.<br>If there are more than six email addresses, there is a scroll bar to the right of the list. |
| **Tags** | Select any tags that have been created and applied to a site.<br>If there are more than six email addresses, there is a scroll bar to the right of the list. |

4. Do any or all of the following, as needed:
   - To hide the Filters menu, click the **Filters** button. If you have any filters applied, the number of filters displays in a blue circle.
   - To display all of the filters, click the **Filters** button.

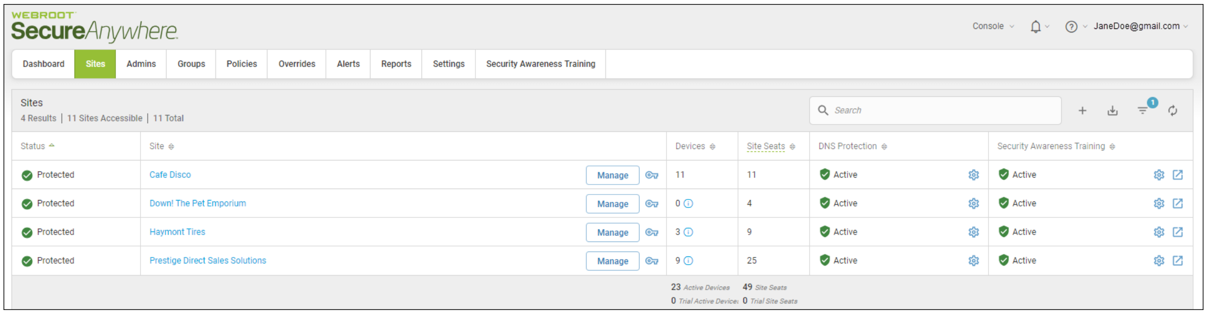
# Searching for Sites

The search function allows admins to search sites by site name.

**To search for sites:**

1. Log in to the management console.

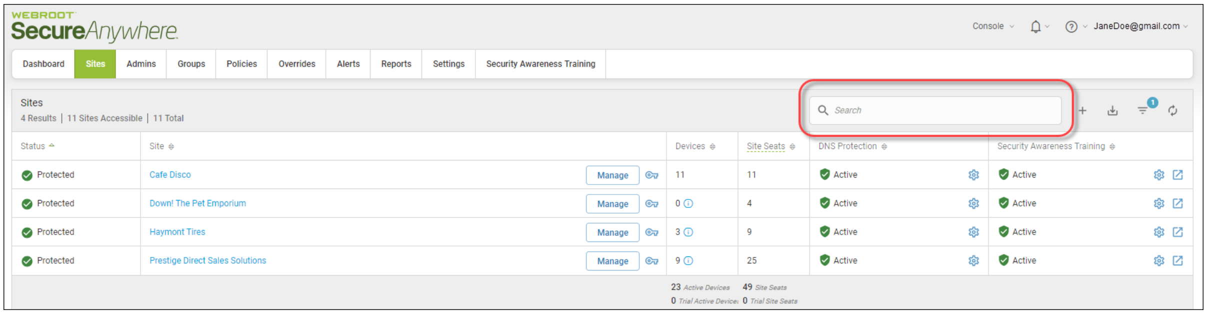
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

2. In the Search field, enter the name of the site you want to find.

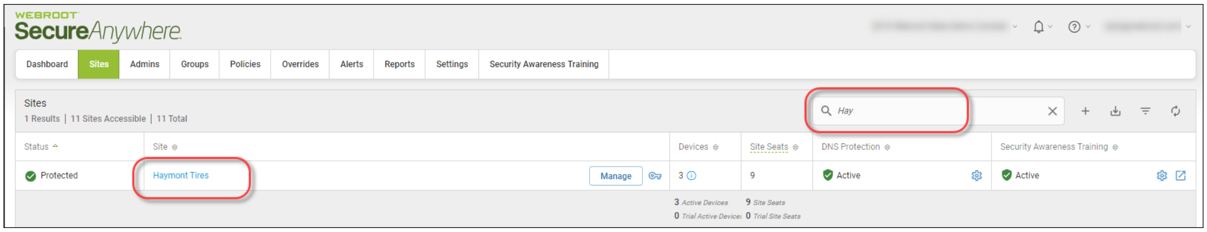


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

3. If needed, you can enter a partial name, and the system will display all sites that fit that criteria.

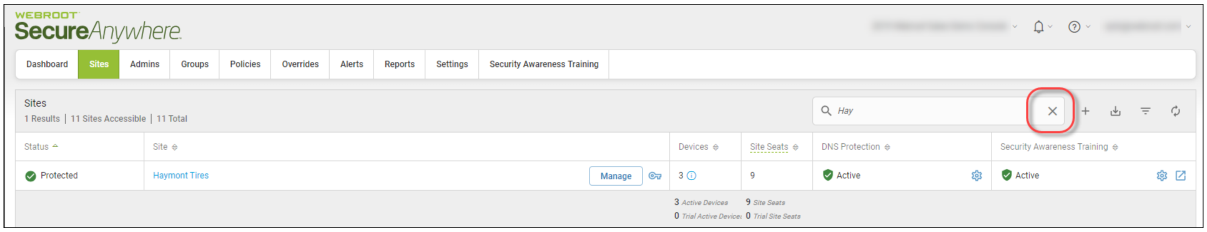
   For example, if you remember that part of the site name was "Hay" but don't remember the rest of the name, enter **Hay**. The system displays all sites that have "Hay" in the name.



Sites
1 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| | | 3 Active Devices<br>0 Trial Active Devices | 9 Site Seats<br>0 Trial Site Seats | | |

4. When you are done searching, click the **X** in the Search field to clear it. The system displays all sites.



Sites
1 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| | | 3 Active Devices<br>0 Trial Active Devices | 9 Site Seats<br>0 Trial Site Seats | | |

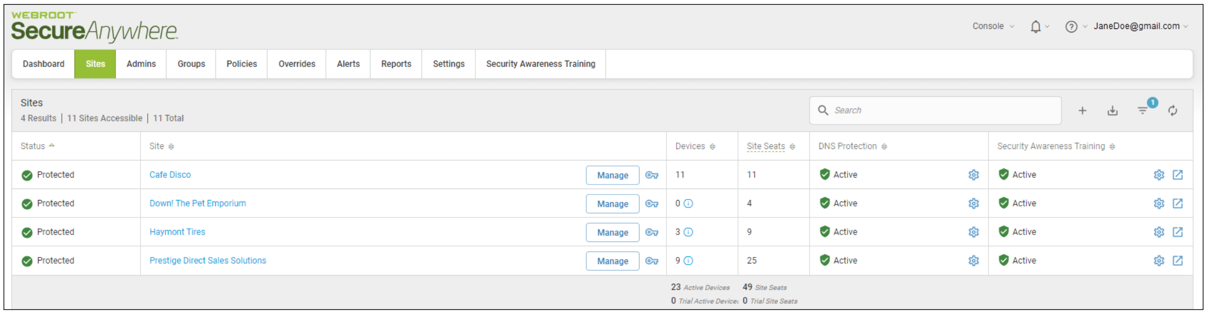
# Downloading CSV Files

Follow this procedure to download site information such as site name, keycode, or status.

### To download a CSV file:

1. Log in to the management console.

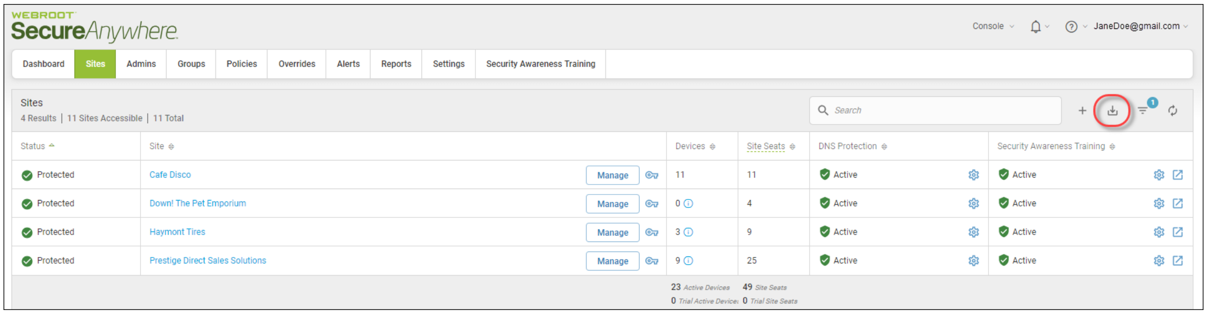
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats |  |  |

2. Click the **Download** icon.



Sites
4 Results | 11 Sites Accessible | 11 Total

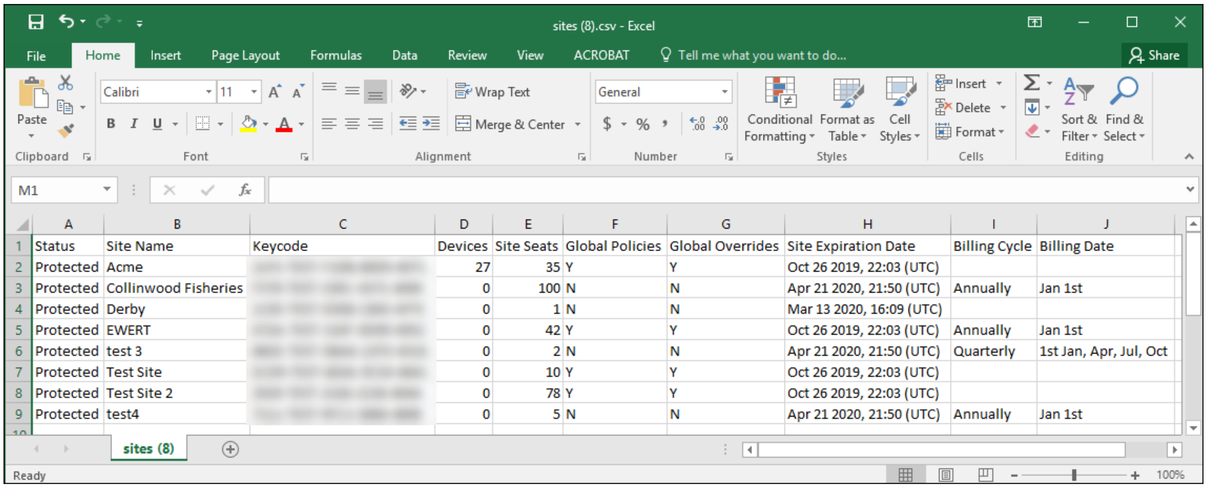
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats |  |  |

   The CSV file downloads.

> **Note:** The downloaded file contains information that reflects any filters you may have set. For more information, see *Filtering Sites on page 81*.

3. Click the CSV file to view information about the following:
   - Status
   - Site Name

- Keycode
- Devices
- Site Seats
- Global Policies
- Global Overrides
- Site Expiration Date
- Billing Cycle
- Billing Date



| Status | Site Name | Keycode | Devices | Site Seats | Global Policies | Global Overrides | Site Expiration Date | Billing Cycle | Billing Date |
|---|---|---|---|---|---|---|---|---|---|
| Protected | Acme | [redacted] | 27 | 35 | Y | Y | Oct 26 2019, 22:03 (UTC) | | |
| Protected | Collinwood Fisheries | [redacted] | 0 | 100 | N | N | Apr 21 2020, 21:50 (UTC) | Annually | Jan 1st |
| Protected | Derby | [redacted] | 0 | 1 | N | N | Mar 13 2020, 16:09 (UTC) | | |
| Protected | EWERT | [redacted] | 0 | 42 | Y | Y | Oct 26 2019, 22:03 (UTC) | Annually | Jan 1st |
| Protected | test 3 | [redacted] | 0 | 2 | N | N | Apr 21 2020, 21:50 (UTC) | Quarterly | 1st Jan, Apr, Jul, Oct |
| Protected | Test Site | [redacted] | 0 | 10 | Y | Y | Oct 26 2019, 22:03 (UTC) | | |
| Protected | Test Site 2 | [redacted] | 0 | 78 | Y | Y | Oct 26 2019, 22:03 (UTC) | | |
| Protected | test4 | [redacted] | 0 | 5 | N | N | Apr 21 2020, 21:50 (UTC) | Annually | Jan 1st |

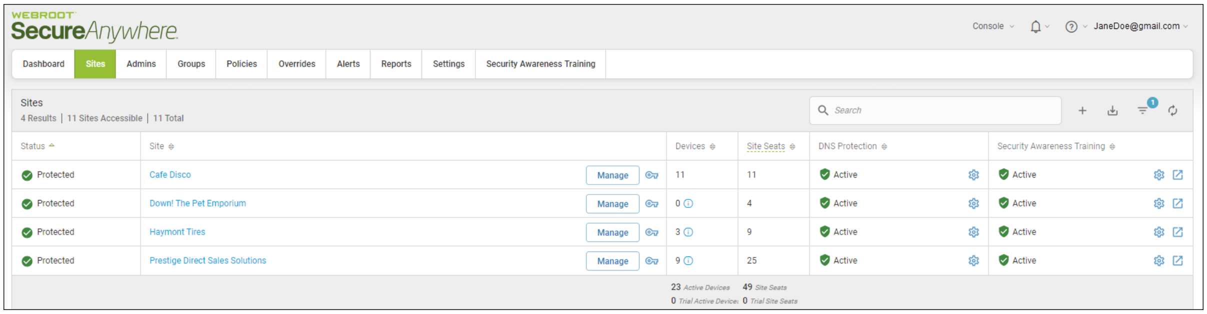
# Sorting Sites

The sorting function allows admins to sort based on site view headings.

**To sort sites:**

1. Log in to the management console.

   The management console displays with the Sites tab active.

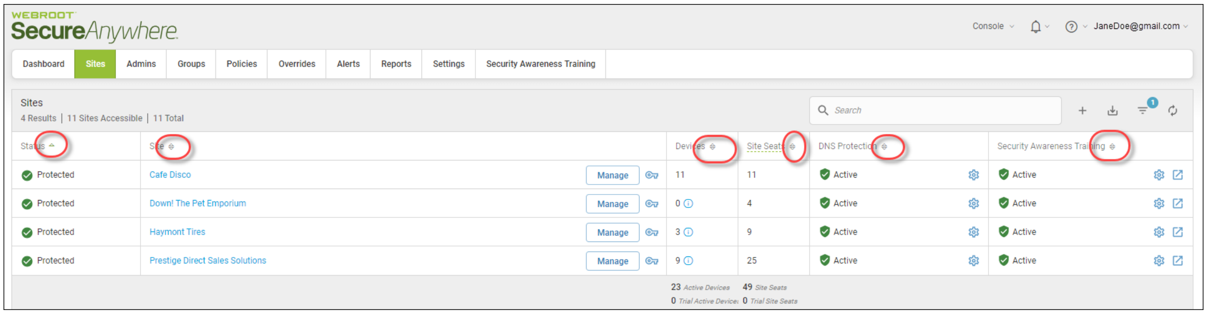


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

2. Click the **Up** or **Down** arrow to the right of each heading to sort the following columns:
   - Status
   - Site
   - Devices
   - Site Seats
   - DNS Protection
   - Security Awareness Training

**Note:** Click to the right of the heading to display the **Up** or **Down** Arrow.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

The system sorts in ascending or descending order, based on the type of information in each column, for example, lowest to highest number, or alphabetical.

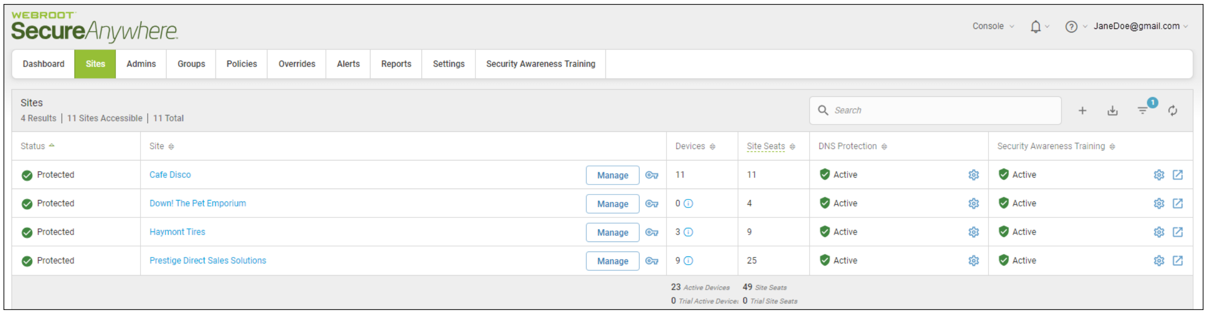
# Viewing Site Summaries

You can view additional site information such as admin names, billing cycles, and any comments related to a particular site.

### To view additional site information:

1. Log in to the management console.

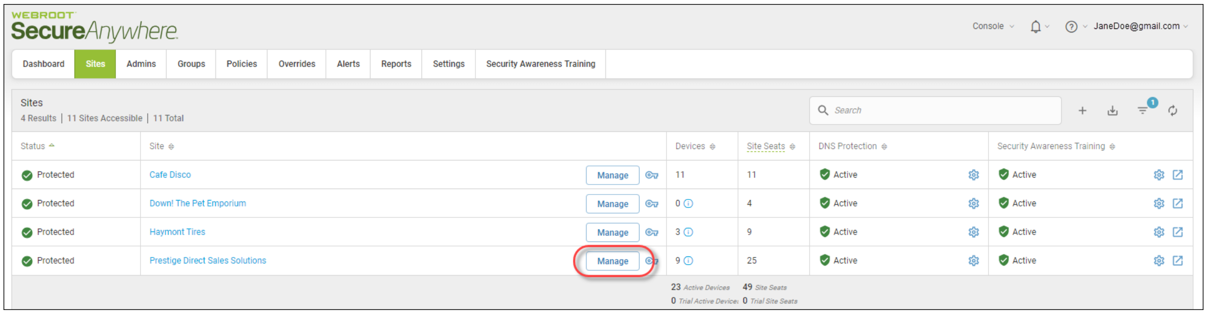
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

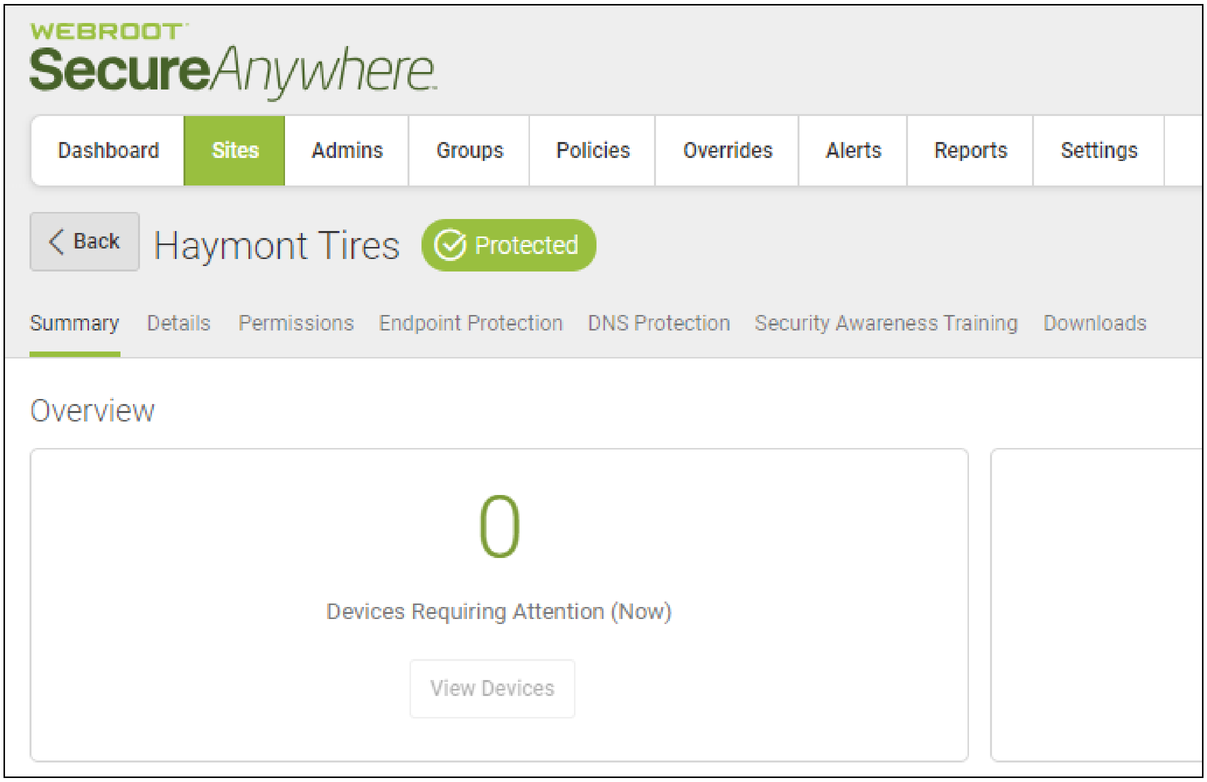
2. Click the **Manage** button.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Manage Sites panel displays, with the Summary tab active.



## Inside the Manage Button

Inside the Manage button, there are six tabs:

- Summary
- Details
- Permissions
- Endpoint Protection
- DNS Protection
- Security Awareness Training
- Downloads

## Summary Tab

In the Overview area, the system displays numbers reflecting that site's status.

- Devices Requiring Attention (Now)
- Devices Requiring Attention (Last 7 Days)
- Devices Installed (Last 7 Days)

The Admins area lists those admins who have been given access to the site, and then lists those admins who have View Only permissions. For more information on admin permission levels, see *Updating Site Admin Permissions on page 132*.

The Actions area includes the following:

- The ability to suspend and resume protection; for more information, see *Suspending and Resuming Site Protection on page 108*.
- The ability to deactivate a site; for more information, see *Deactivating Site Protection on page 111*.

## Details Tab

From this tab you can view or edit any of the following :

- Site/Company Name
- Keycode
- Site type, either internal or external.
- Comments about the site; this is a free-form field.
- The name of the person who created the site.
- Filter tags for the site.

For more information, see *Editing Site Details on page 114* and *Tagging Sites on page 122*.

## Permissions Tab

From this tab you can set site permissions for your admins to any of the following levels:

- Admin
- View Only
- No Access

For more information, see *Updating Site Admin Permissions on page 132*.

## Endpoint Protection Tab

From this tab you can view or edit any of the following settings:

- Site Seats
- Default Endpoint Policies
- Include Global Overrides and Global Policies
- Set the email for the Report Distribution List
- Set Data Filters
- Go directly to the Endpoint console. For more information, see *Accessing the Endpoint Console on page 36*.

For more information, see *Editing Site Settings on page 136*.

## DNS Protection Tab

From this tab you can do any of the following:

- Enable DNS Protection
- Upgrade from 30 day trail to full license for DNS Protection
- Edit policies
- Update network settings

For more information, see the DNS Protection online guides.

## Security Awareness Training Tab

From this tab you can do any of the following:

- Enable Security Awareness Training
- Upgrade from 30 day trail to full license for Security Awareness Training

For more information, see the Security Awareness Training guides.

## Downloads Tab

From this tab you can download copies of Webroot SecureAnywhere, with keycodes automatically applied. For more information, see *Downloading Webroot on page 149*.

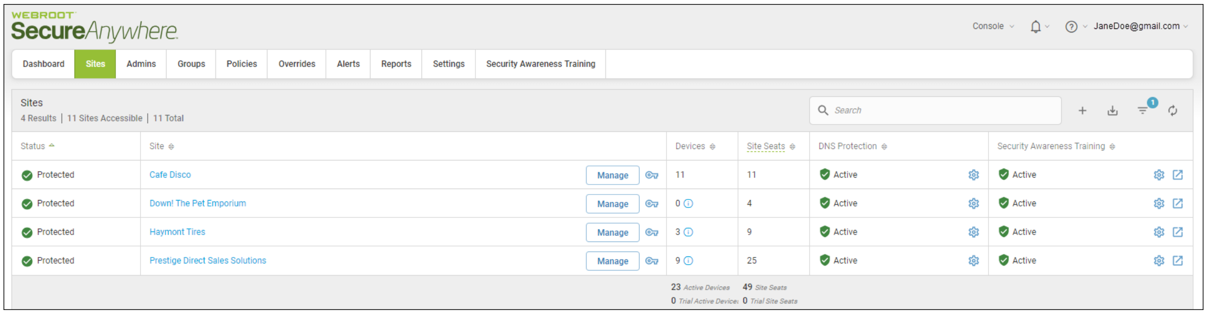
# Viewing Multi-Site Summaries

Your management console allows you to get an overview of your multi-site deployment. You can view multiple dashboards at the same time, get overviews for a specific dashboard, and drill down for additional information on a specific site.

**To view multi-site summaries:**

1. Log in to the management console.

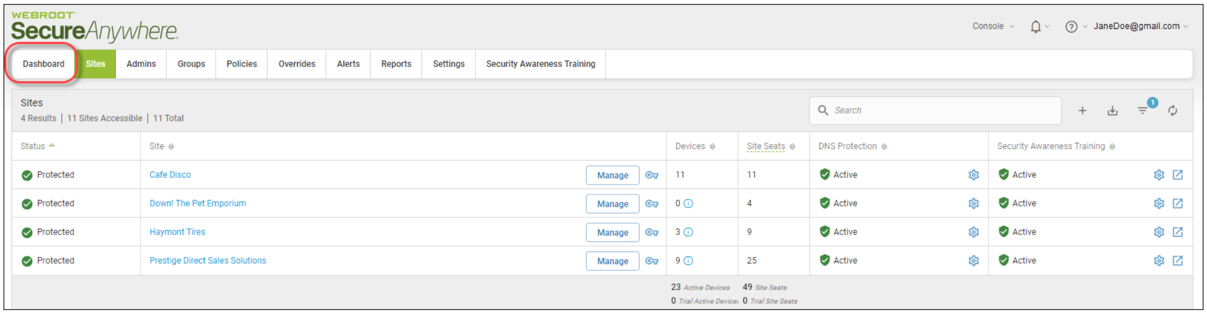
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

2. Click the **Dashboard** tab.

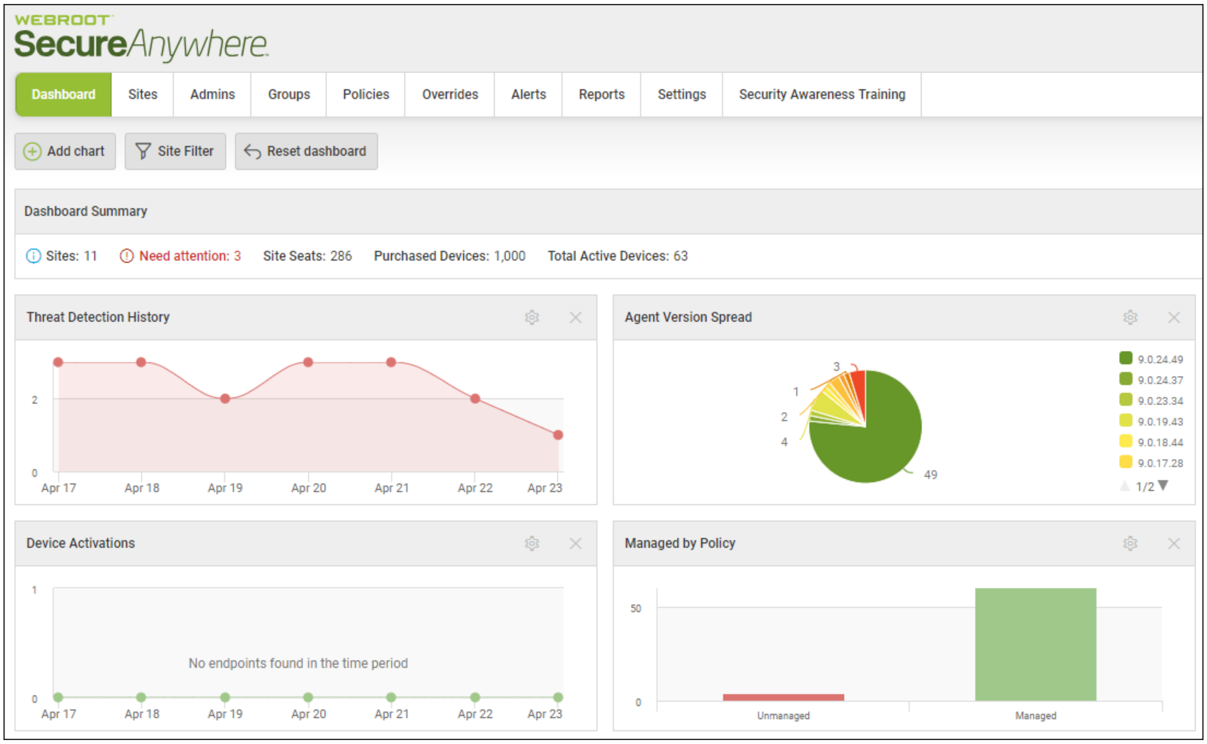


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

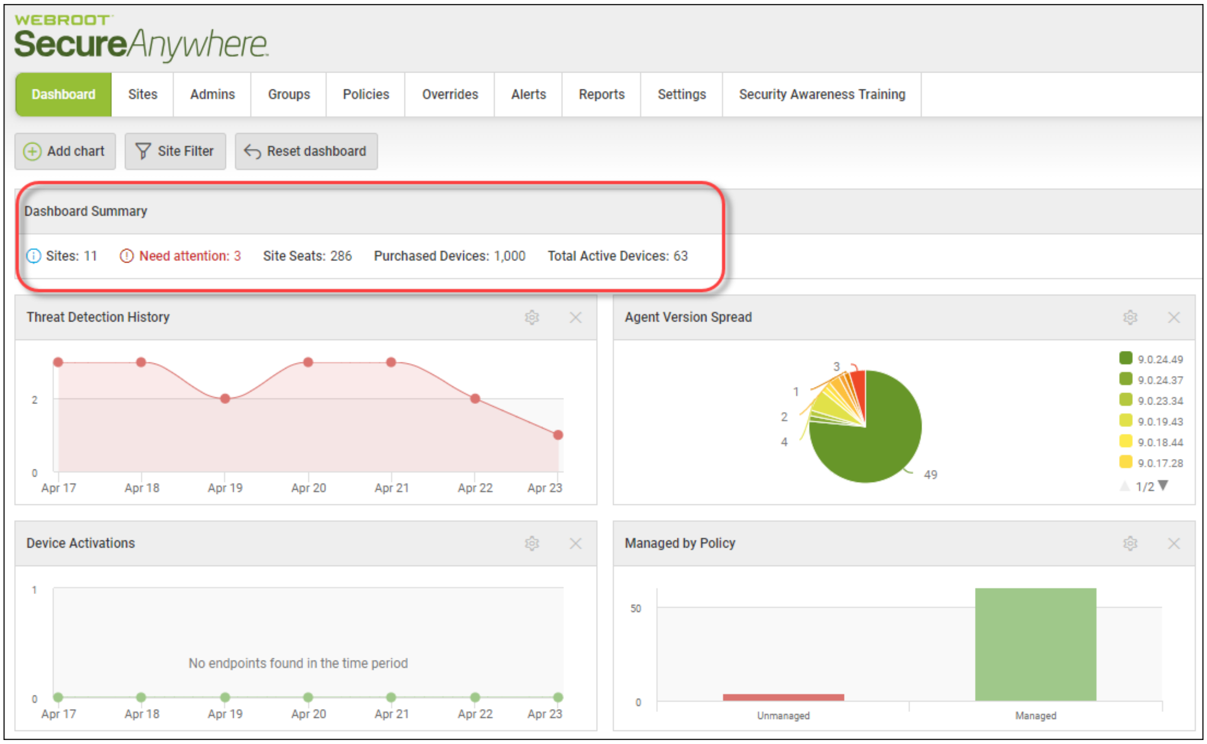
> **Note:** With the exception of the Threat Detection History and Device Activations charts, only endpoints running agent version 8.0.4.134 onwards will accurately be represented in the dashboard totals. Migrated keycodes may cause slight anomalies in counts during this Beta launch

The Dashboard tab displays.



Sites: 11 Need attention: 3 Site Seats: 286 Purchased Devices: 1,000 Total Active Devices: 63

In the upper left corner is a Dashboard Summary bar, which gives you an overview of all of your sites.

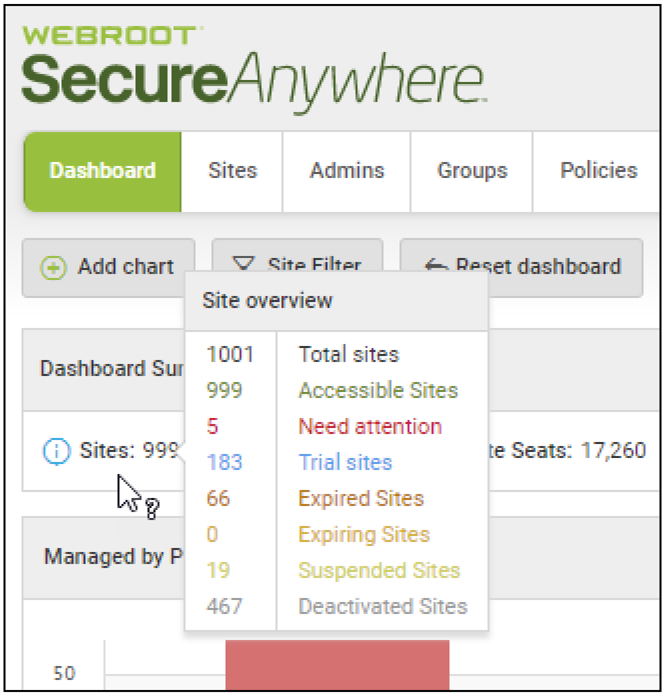


Dashboard Summary

Sites: 11 Need attention: 3 Site Seats: 286 Purchased Devices: 1,000 Total Active Devices: 63

3. To view additional site information, hover over the word **Sites**.

   The system displays a site overview.

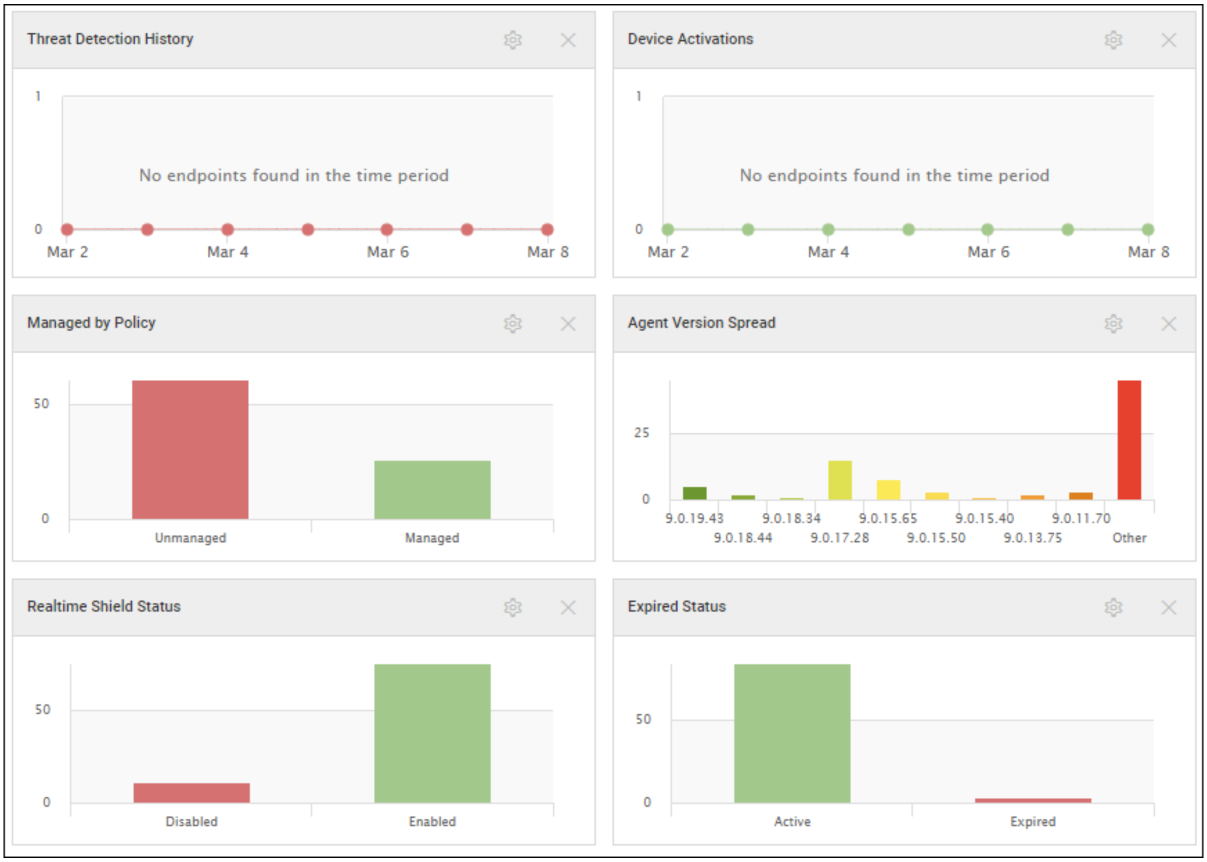


Site overview

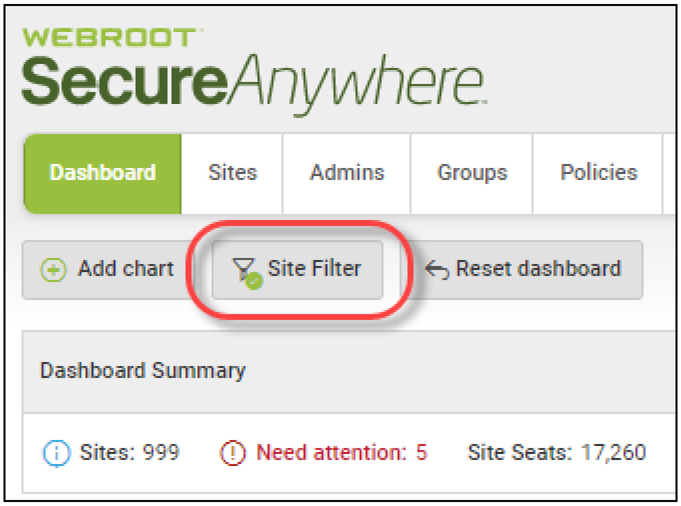
| | |
|---|---|
| 1001 | Total sites |
| 999 | Accessible Sites |
| 5 | Need attention |
| 183 | Trial sites |
| 66 | Expired Sites |
| 0 | Expiring Sites |
| 19 | Suspended Sites |
| 467 | Deactivated Sites |

In the Chart area, the system displays the following types of default charts:

- **Threat Detection History** — A historic view of all threats encountered over a seven day period.
- **Device Activations** — A historic view of new device activations over a seven day period.
- **Managed by Policy** — Count of devices which are managed versus unmanaged.
- **Agent version Spread** — Count of WSA agent versions installed.
- **Realtime Shield Status** — Count of devices with their Reatime shied on and off.
- **Expired Status** — Count of devices which are on an expired keycode.
- **Remediation Status** — Count of devices with remediation, or clean up, enabled by default.



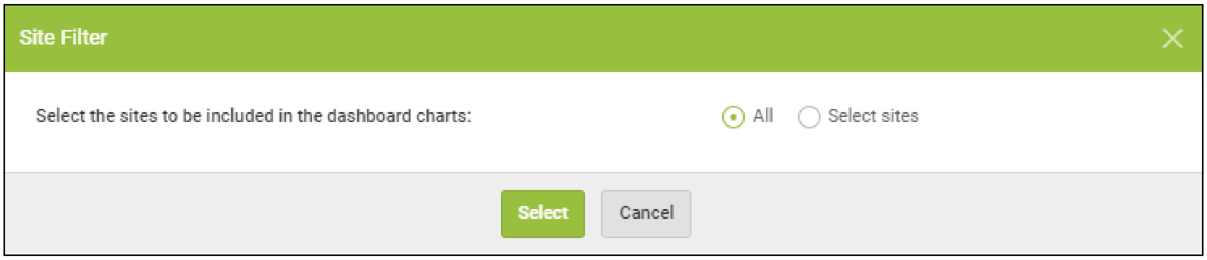
4. To configure which sites will display in the dashboard, click the **Site Filter** button.



Dashboard Summary

Sites: 999 Need attention: 5 Site Seats: 17,260

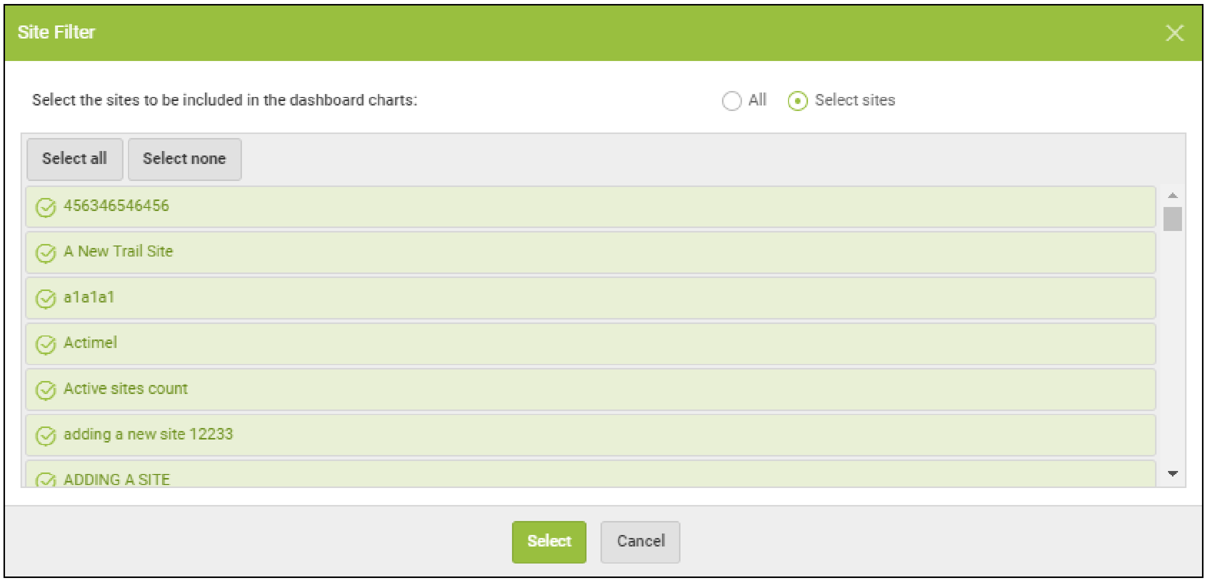
The system displays the Site Filter window.



Site Filter

Select the sites to be included in the dashboard charts: ● All ○ Select sites

5. Do one of the following:
   - Select the **All** radio button to display all sites.
   - Select the **Select sites** radio button, and then, in the window that displays, select the sites you want to display.
     - To select all sites, click the **Select all** button.
     - To select no sites, click the **Select none** button.



Site Filter

Select the sites to be included in the dashboard charts: ○ All ● Select sites

✓ 456346546456

✓ A New Trail Site

✓ a1a1a1

✓ Actimel

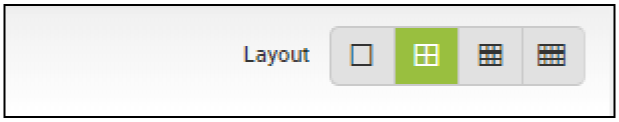
✓ Active sites count

✓ adding a new site 12233

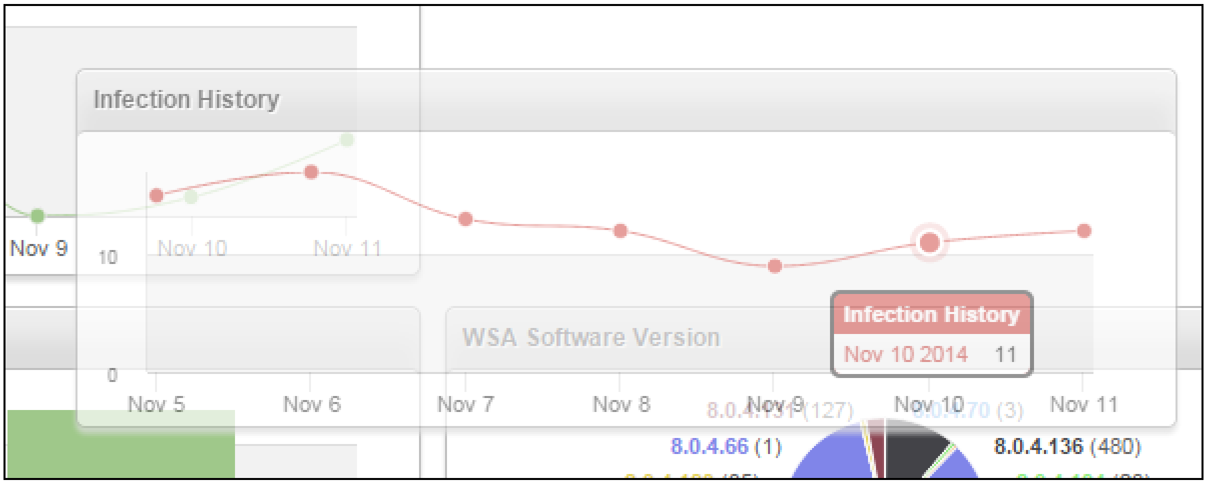
✓ ADDING A SITE

6. In the upper right corner, click on one of the following toggle buttons to change the layout of the dashboards:
   - **One column**
   - **Two columns**

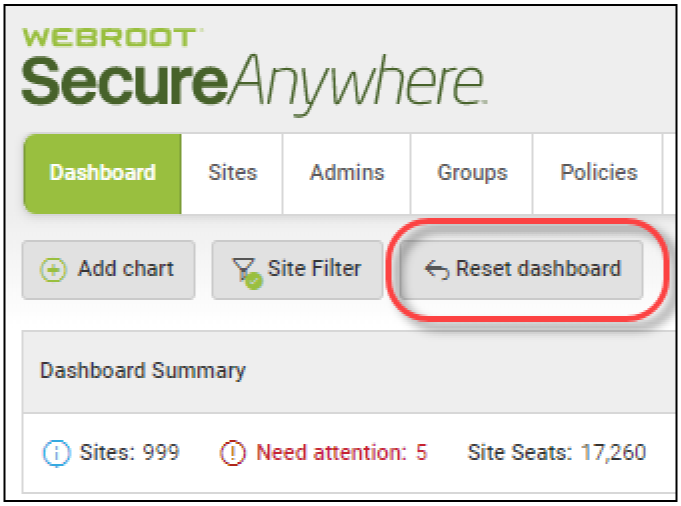
- **Three columns**
- **Four columns**



7. Additionally, you can drag and drop any of the dashboards to a new location.



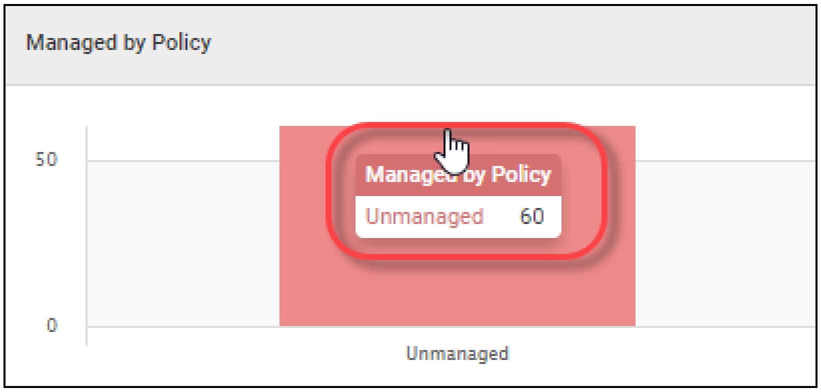
8. To put the dashboards in their original locations, click the **Reset dashboard** button.



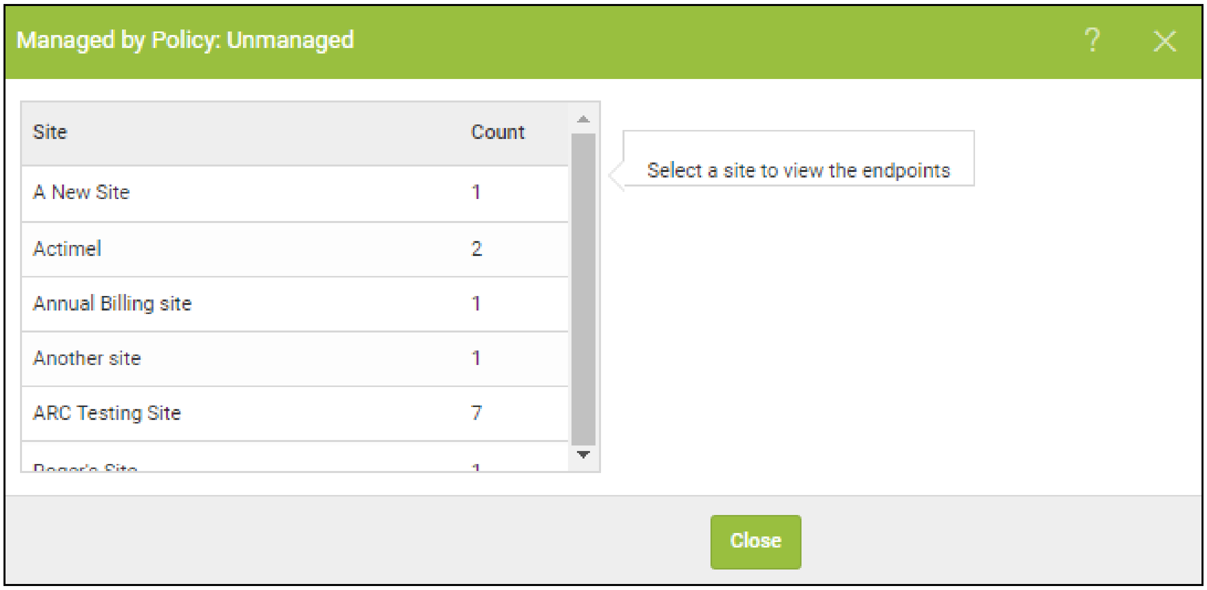
Dashboard Summary

Sites: 999 Need attention: 5 Site Seats: 17,260

9. To drill down for additional information about each site, hover over the chart, then click on the window that displays.



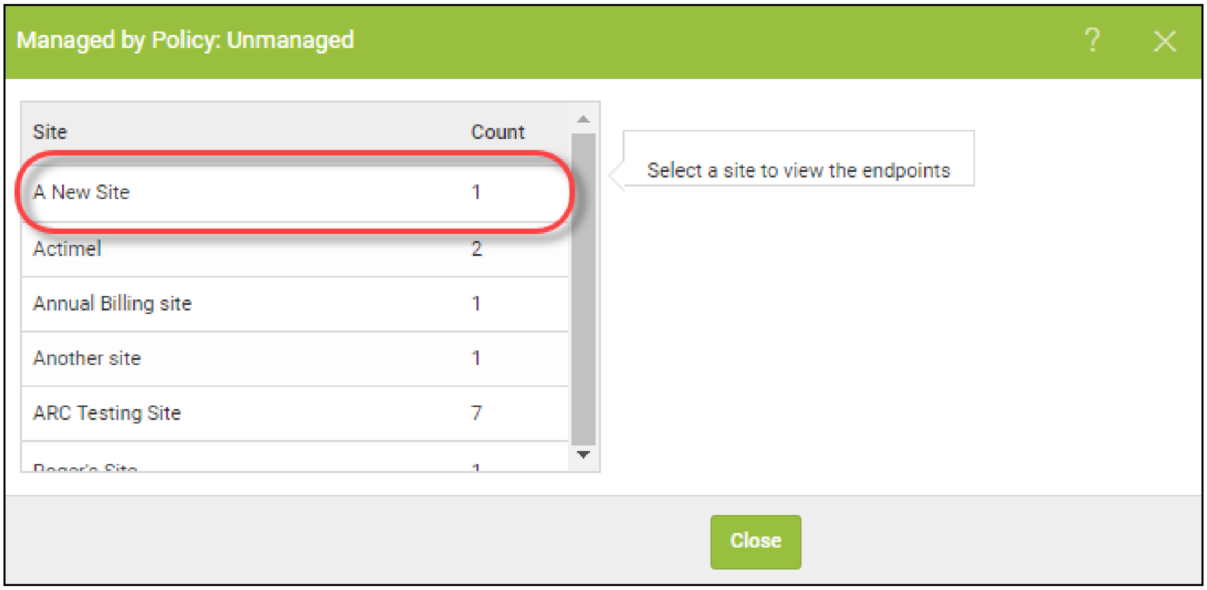
The system displays additional about the sites.



| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 2 |
| Annual Billing site | 1 |
| Another site | 1 |
| ARC Testing Site | 7 |
| Roger's Site | 1 |

Select a site to view the endpoints

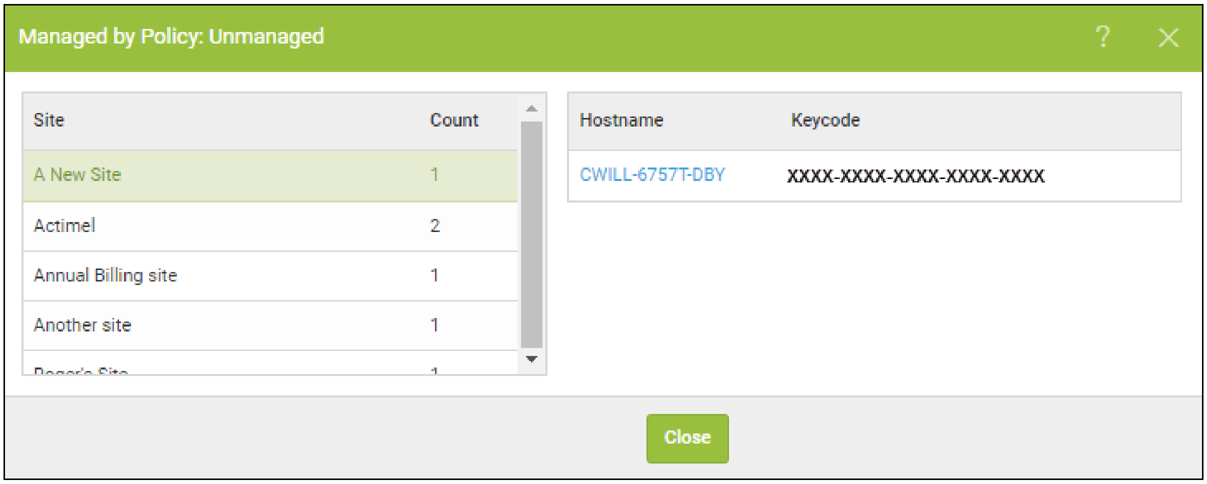
10. For additional information, click the name of the site.



| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 2 |
| Annual Billing site | 1 |
| Another site | 1 |
| ARC Testing Site | 7 |
| Roger's Site | 1 |

Select a site to view the endpoints

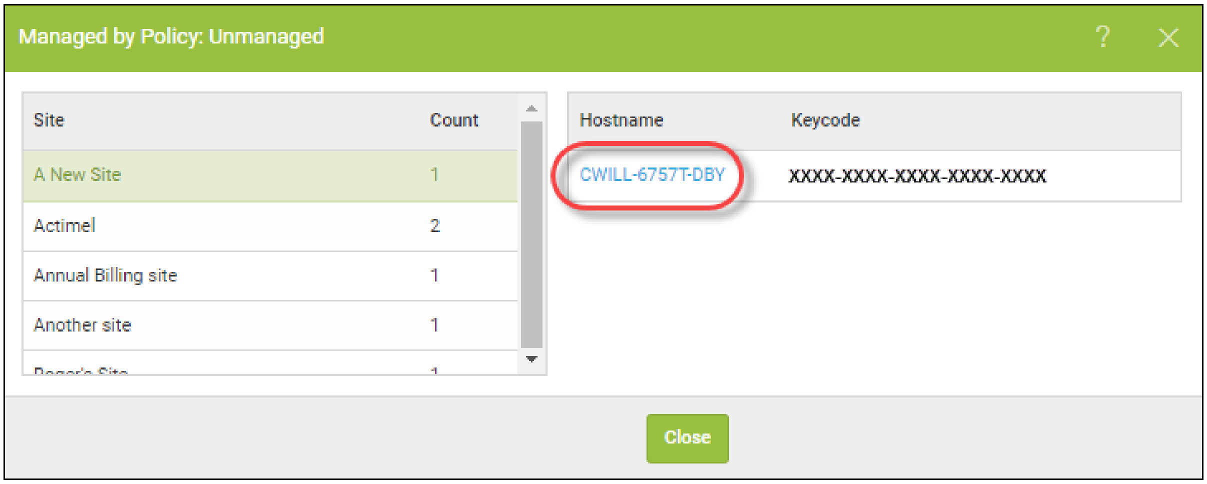
The Hostname and Keycode information display.



| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 2 |
| Annual Billing site | 1 |
| Another site | 1 |
| Roger's Site | 1 |

| Hostname | Keycode |
|---|---|
| CWILL-6757T-DBY | XXXX-XXXX-XXXX-XXXX-XXXX |

11. In the Hostname column, click the link to drill further down.

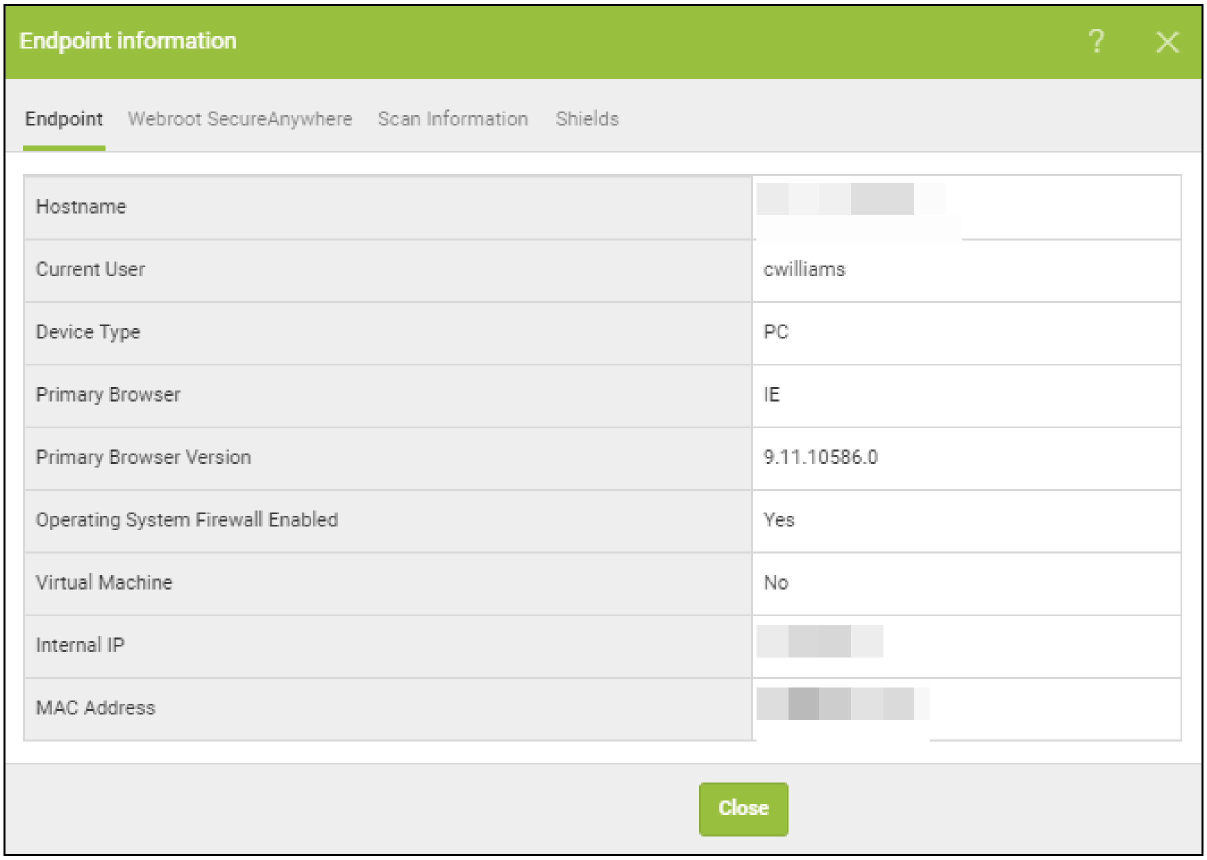


| Site | Count |
|---|---|
| A New Site | 1 |
| Actimel | 2 |
| Annual Billing site | 1 |
| Another site | 1 |
| Roger's Site | 1 |

| Hostname | Keycode |
|---|---|
| CWILL-6757T-DBY | XXXX-XXXX-XXXX-XXXX-XXXX |

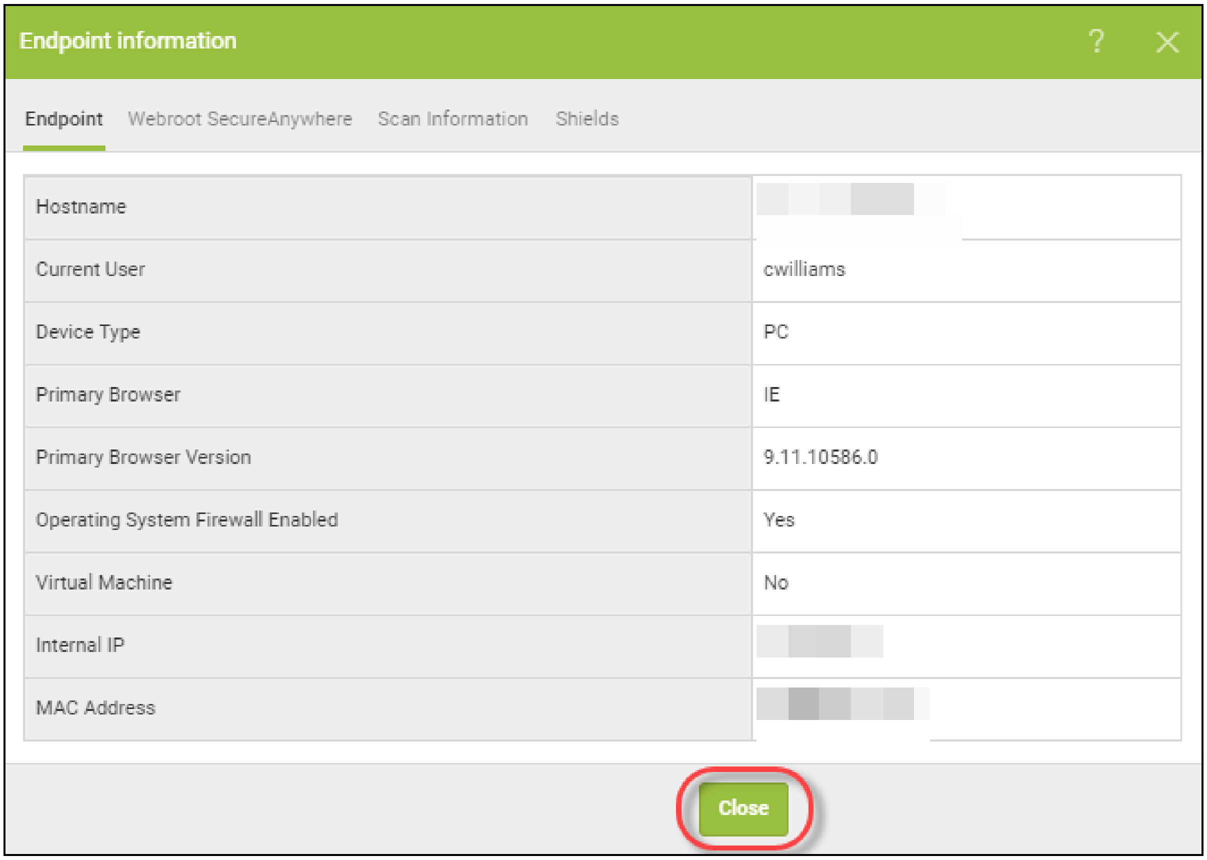
The Endpoint Information window displays with the following tabs:

- **Endpoint** — Includes information about the Hostname, the Current User, Device Type, Internal IP, and MAC Address.
- **Webroot SecureAnywhere** — Includes information about the Keycode, the Version, Expiration Date, Days Remaining.
- **Scan Information** — Includes information about the Last Scan, Total Number of Scans, Scheduled Scan Time.
- **Shields** — Includes information about which shields have been activated.



| | |
|---|---|
| Hostname | [redacted] |
| Current User | cwilliams |
| Device Type | PC |
| Primary Browser | IE |
| Primary Browser Version | 9.11.10586.0 |
| Operating System Firewall Enabled | Yes |
| Virtual Machine | No |
| Internal IP | [redacted] |
| MAC Address | [redacted] |

12. When you're done, click the **Close** button.



| | |
|---|---|
| Hostname | [redacted] |
| Current User | cwilliams |
| Device Type | PC |
| Primary Browser | IE |
| Primary Browser Version | 9.11.10586.0 |
| Operating System Firewall Enabled | Yes |
| Virtual Machine | No |
| Internal IP | [redacted] |
| MAC Address | [redacted] |

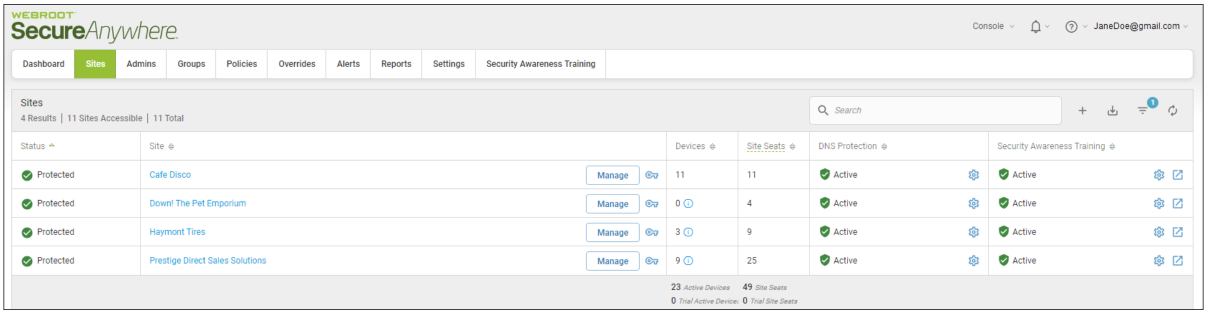
# Suspending and Resuming Site Protection

You can suspend site protection for any site, and then resume site protection at any time.

**To suspend and resume site protection:**

1. Log in to the management console.

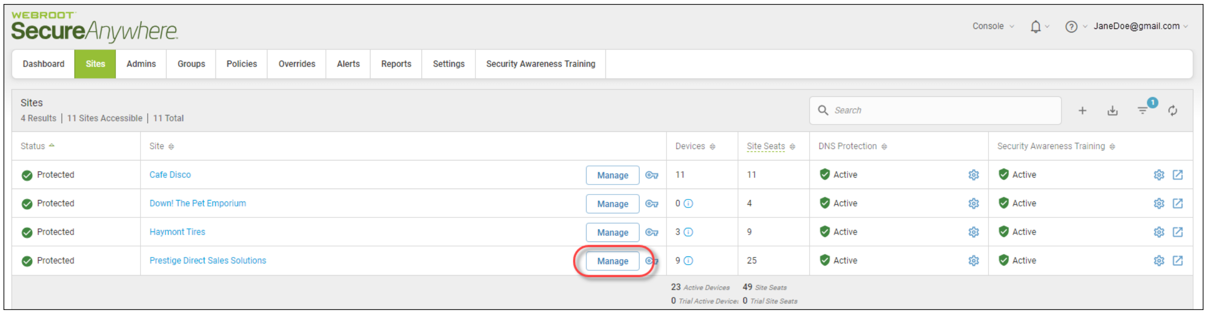
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

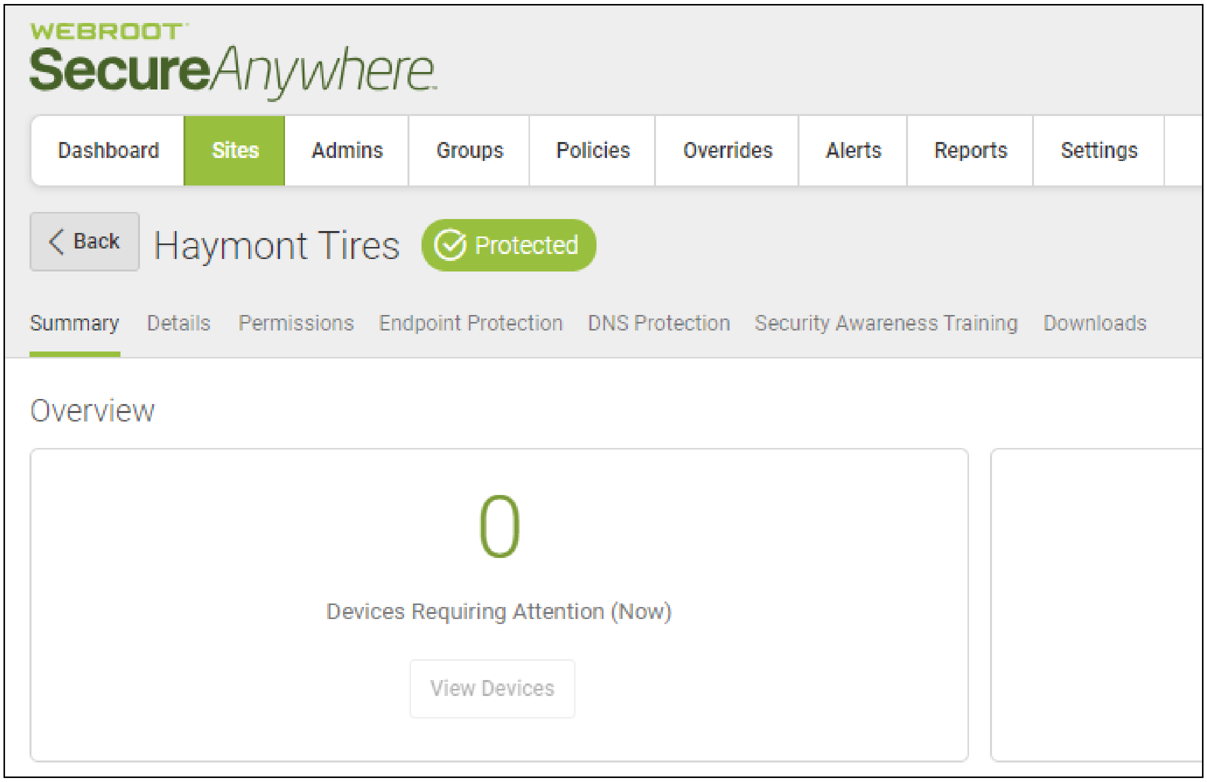
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

2. For the site that you want to suspend, click the **Manage** button.


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

The Manage Sites panel displays, with the Summary tab active.



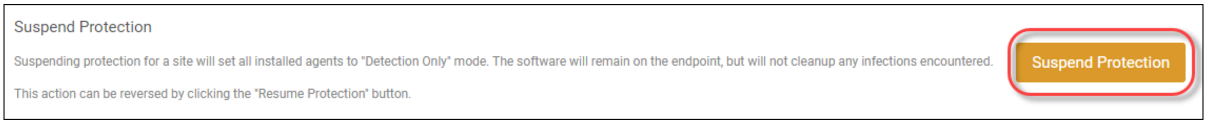
Haymont Tires

Overview

0

Devices Requiring Attention (Now)

3. Scroll down the page and click the **Suspend Protection** button to suspend protection for that site.

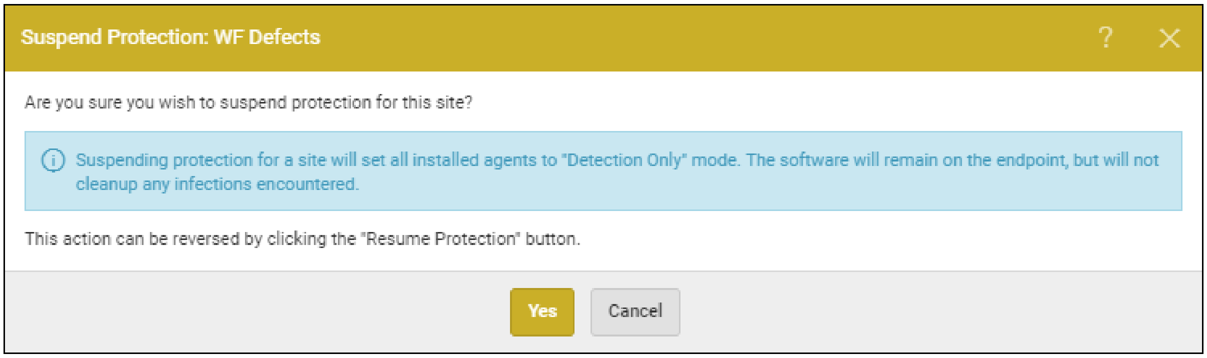


Suspend Protection

Suspending protection for a site will set all installed agents to "Detection Only" mode. The software will remain on the endpoint, but will not cleanup any infections encountered.

This action can be reversed by clicking the "Resume Protection" button.

The system displays a Suspend Protection warning message.



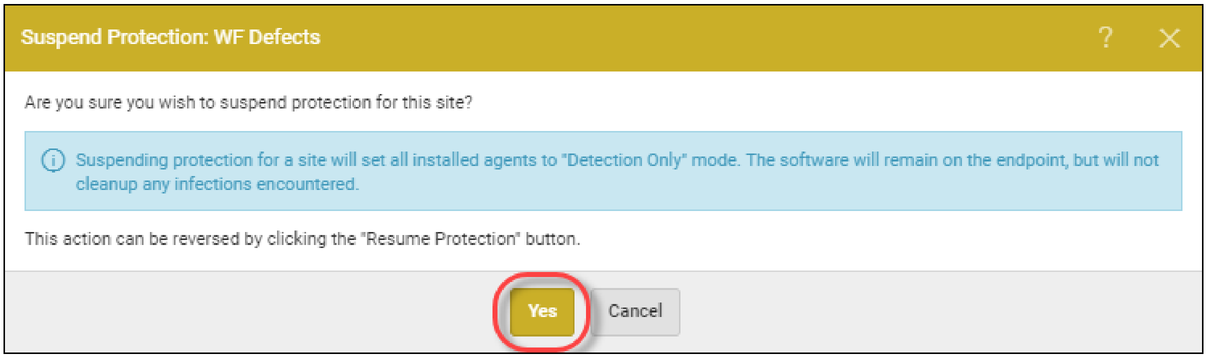
Suspend Protection: WF Defects

Are you sure you wish to suspend protection for this site?

Suspending protection for a site will set all installed agents to "Detection Only" mode. The software will remain on the endpoint, but will not cleanup any infections encountered.

This action can be reversed by clicking the "Resume Protection" button.

4. Click the **Yes** button to continue with suspending protection.



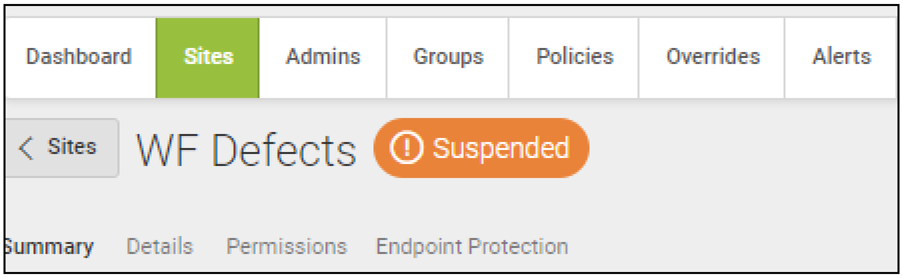
Suspend Protection: WF Defects

Are you sure you wish to suspend protection for this site?

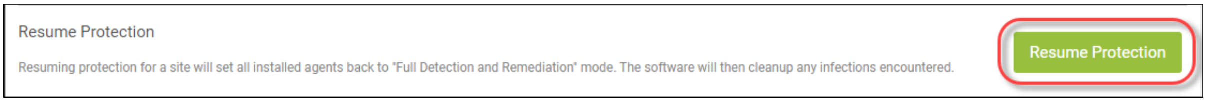
Suspending protection for a site will set all installed agents to "Detection Only" mode. The software will remain on the endpoint, but will not cleanup any infections encountered.

This action can be reversed by clicking the "Resume Protection" button.

The system suspends the site, and indicates this by displaying a Suspended icon in the upper left corner.



Also, the Suspend Protection button becomes the Resume Protection button



Resume Protection

Resuming protection for a site will set all installed agents back to "Full Detection and Remediation" mode. The software will then cleanup any infections encountered.

5. To resume protection for that site, click the **Resume Protection** button.

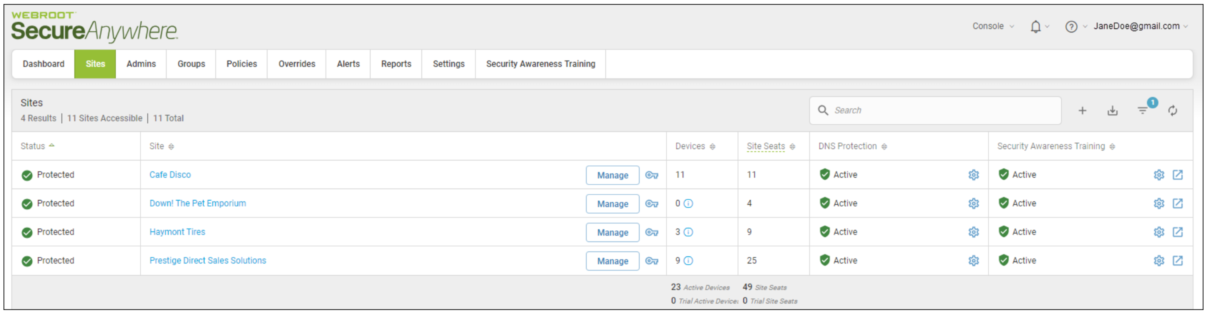
# Deactivating Site Protection

Follow this procedure to deactivate protection for a site.

**To deactivate site protection:**

1. Log in to the management console.

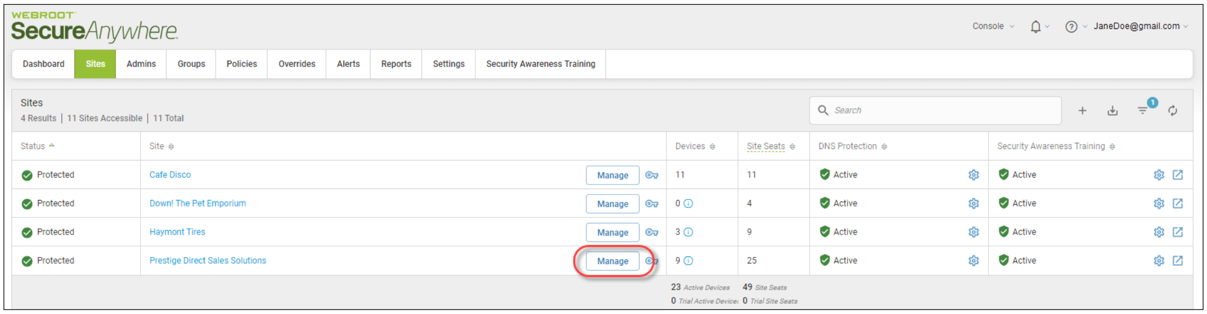
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

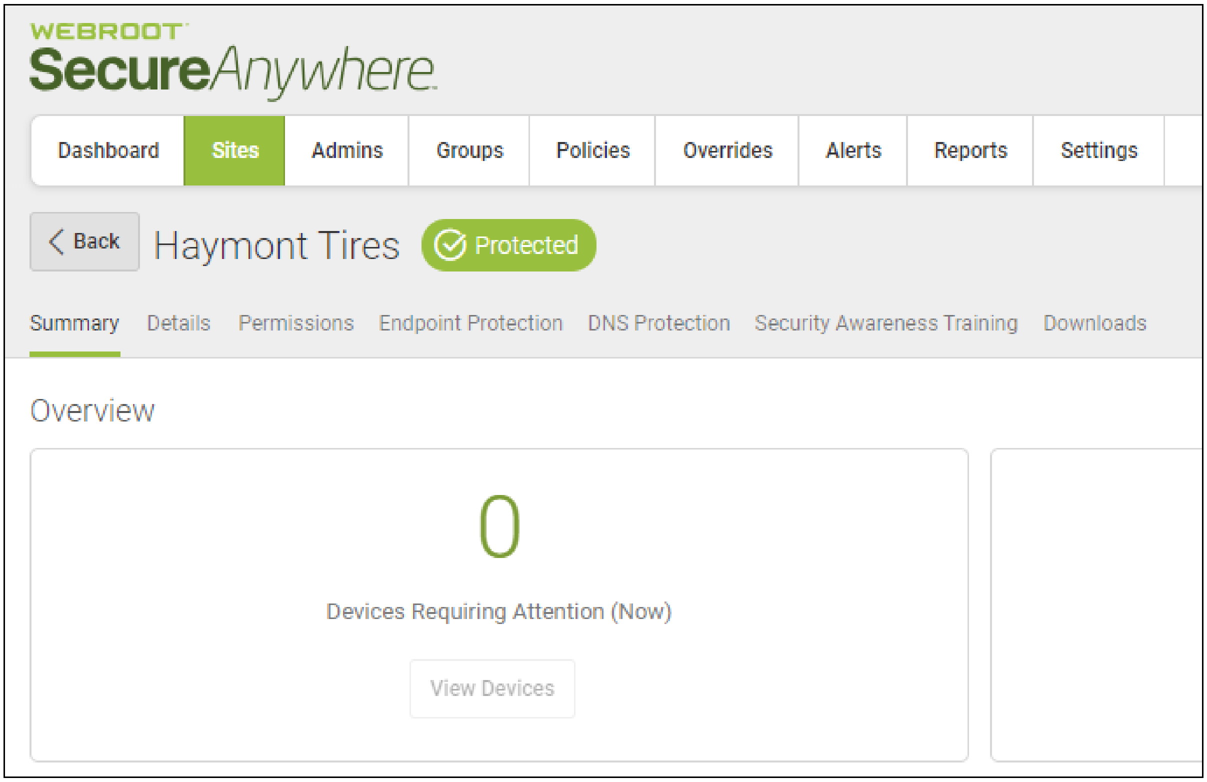
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

2. For the site that you would like to suspend, click the **Manage** button.

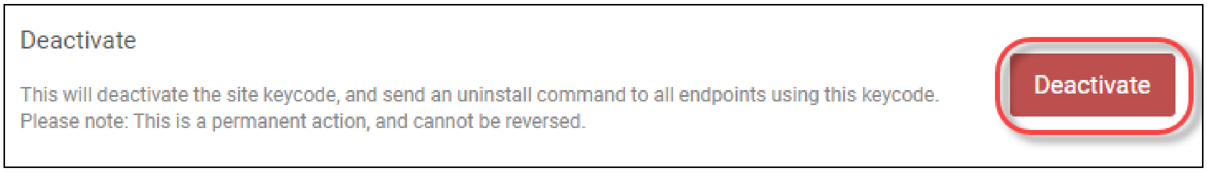

Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

The Manage Sites panel displays, with the Summary tab active.



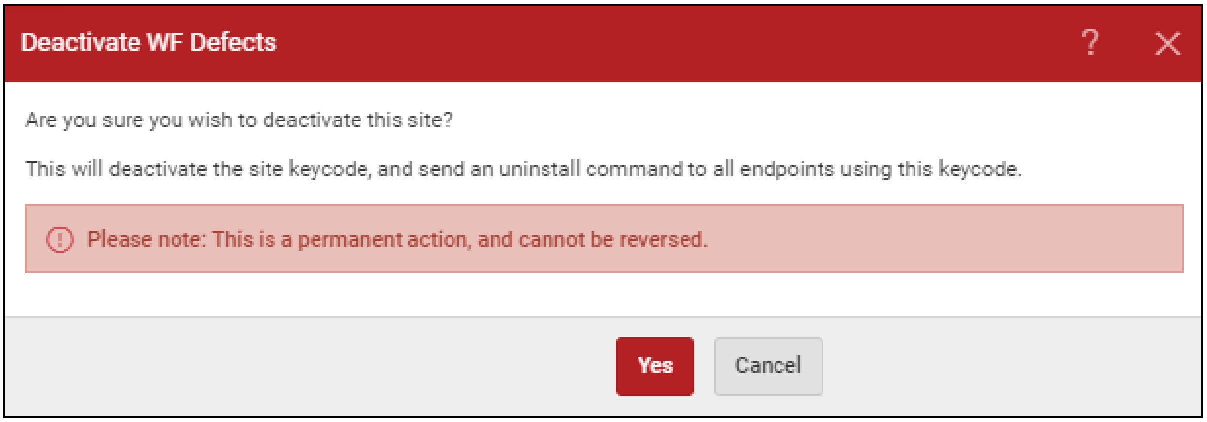
3. Scroll down and click the **Deactivate** button.



Deactivate

This will deactivate the site keycode, and send an uninstall command to all endpoints using this keycode. Please note: This is a permanent action, and cannot be reversed.

The system deactivates the site, and displays a Deactivate warning message.



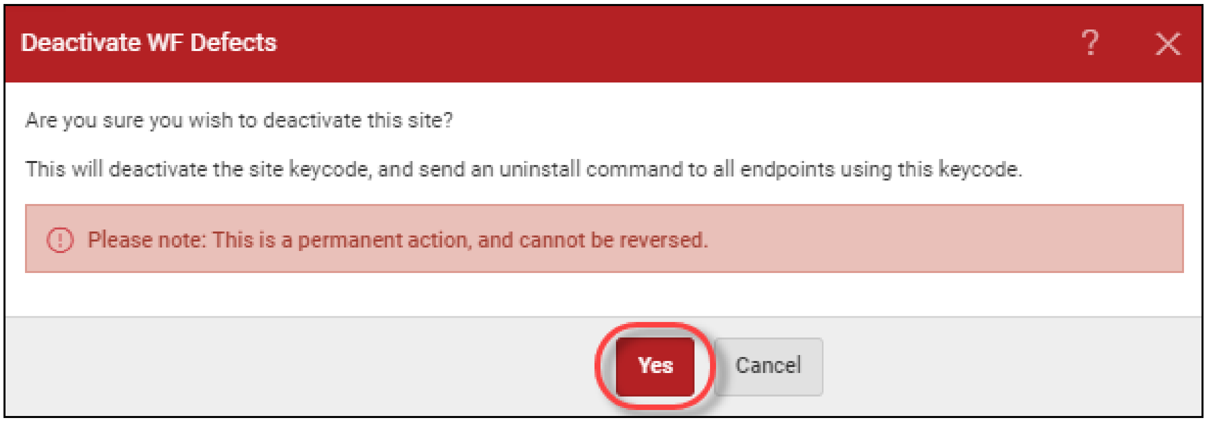
Deactivate WF Defects

Are you sure you wish to deactivate this site?

This will deactivate the site keycode, and send an uninstall command to all endpoints using this keycode.

Please note: This is a permanent action, and cannot be reversed.

4. Click the **Yes** button to continue.



Deactivate WF Defects

Are you sure you wish to deactivate this site?

This will deactivate the site keycode, and send an uninstall command to all endpoints using this keycode.

Please note: This is a permanent action, and cannot be reversed.

The system deactivates the site, which expires the site keycode and uninstalls Webroot SecureAnywhere from all endpoints.

5. To view sites that have been deactivated, click the **Sites Back Arrow**, click the **Filters** button, and select the **Deactivated** button. For more information, see *Filtering Sites on page 81* .

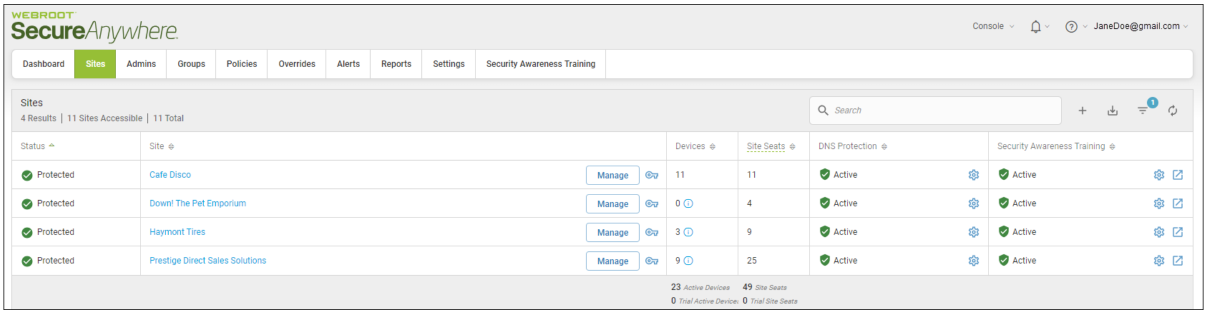
# Editing Site Details

Follow this procedure to edit site details, such as site or company name, number of seats, and to add information about the site.

**To edit a site's details:**

1. Log in to the management console.

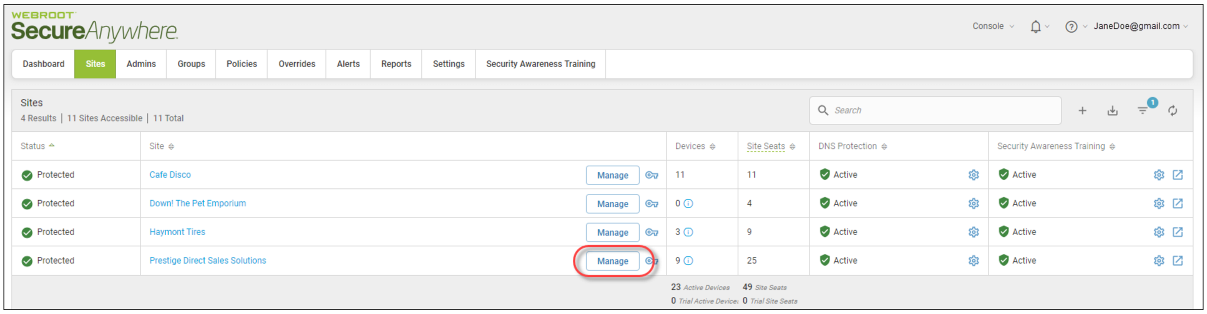
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

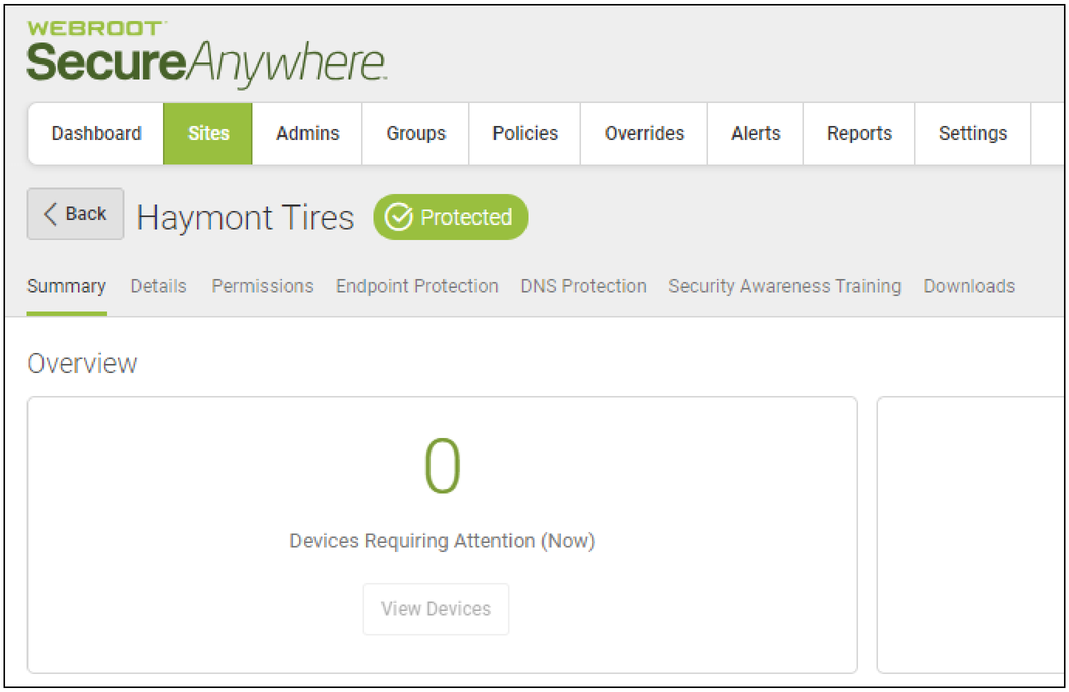
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

2. Click the **Manage** button.

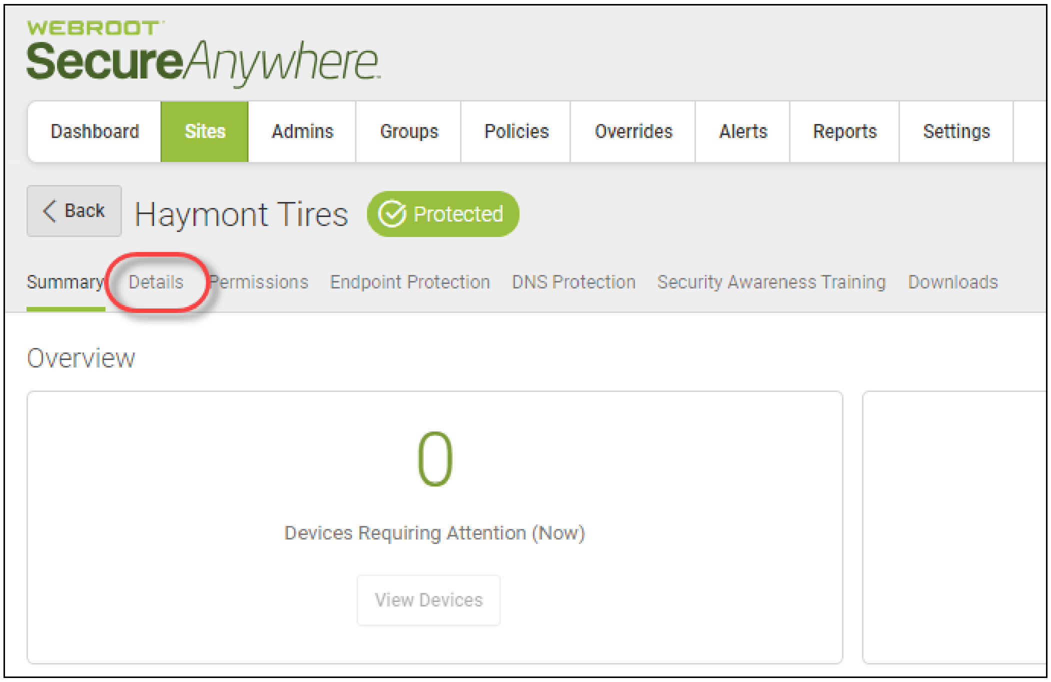

Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

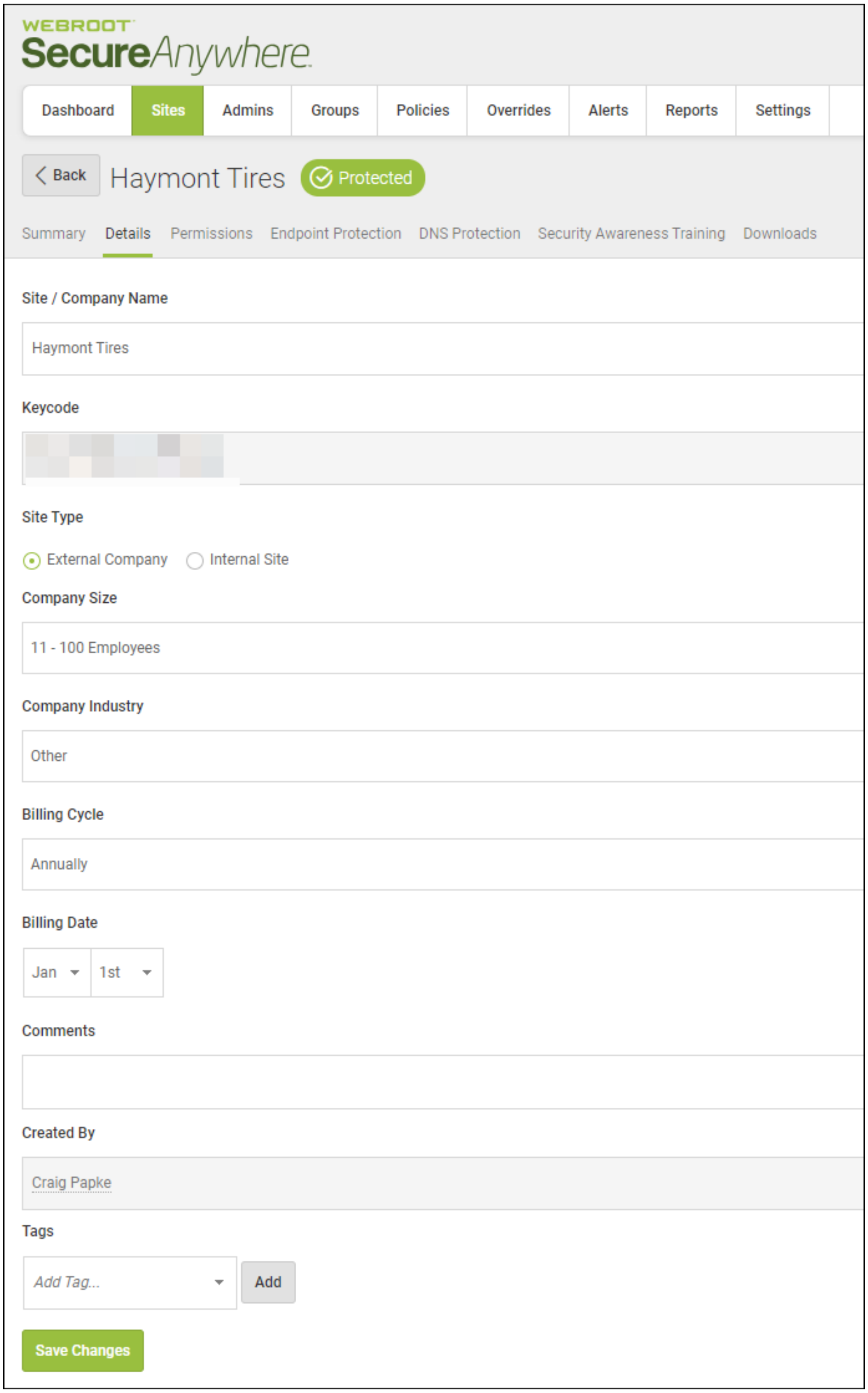
   The Manage Sites panel displays, with the Summary tab active.



3. Click the **Details** tab.



The Details tab displays.



Haymont Tires Protected

Site / Company Name

Haymont Tires

Keycode

[redacted]

Site Type

● External Company ○ Internal Site

Company Size

11 - 100 Employees

Company Industry

Other

Billing Cycle

Annually

Billing Date

Jan 1st

Comments

Created By

Craig Papke

Tags

Add Tag...

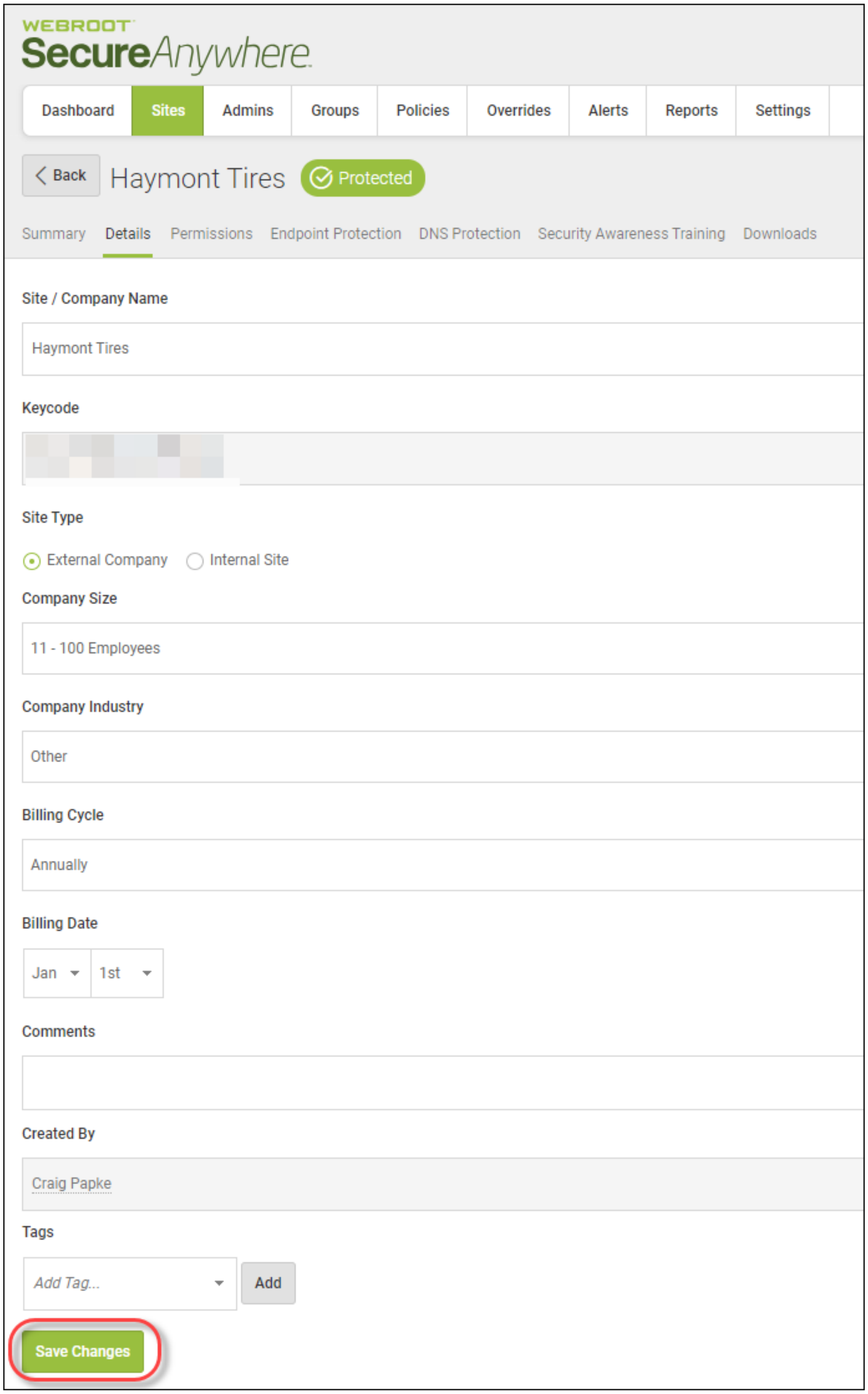
4. In the Site/Site Company field, update the site or company name, as needed.
5. In the Site Type area, select one of the following radio buttons:
   - **External Company**
   - **Internal Site**

   > **Note:** If you selected the Internal Site radio button, the Company Size, Company Industry, Billing Cycle, and Billing Date fields do not display, and you do not have to populate them.

6. In the Company Size field, from the drop-down menu, select the range that best represents the size of your company.
7. In the Company Industry field, from the drop-down menu, select the industry that best represents your company.
8. In the Billing Cycle field, from the drop-down menu, select one of the following billing cycles:
   - **Annually**
   - **Quarterly**
   - **Monthly**
   - **Weekly**
9. In the Billing Date field, use the drop-down menus to select both the month and the date for billing.
10. In the Comments field, enter any comments or notes as needed. This is a free-form field.
11. In the Created By field, update the person who created the site, as needed.
12. From the Tags drop-down menu, enter as many tags as needed. You can create tags based on any or all of the following:
    - The type of company, such as medical, construction, or transportation.
    - The time zone, geographic location, country, or language.
    - The account manager's name, the IT person's name, or the name of your main contact.

    For more information, see *Tagging Sites on page 122*.

13. When you're done, click the **Save Changes** button, which is located at the bottom of the tab.



Haymont Tires

Site / Company Name: Haymont Tires

Keycode: [redacted]

Site Type

● External Company ○ Internal Site

Company Size: 11 - 100 Employees

Company Industry: Other

Billing Cycle: Annually

Billing Date: Jan 1st

Comments:

Created By: Craig Papke

Tags: Add Tag...

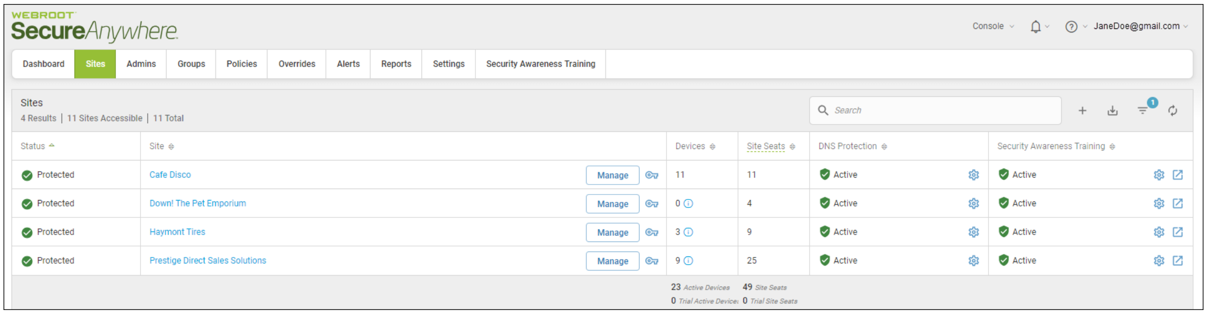
# Tagging Sites

The tag function allows admins to group sites together based on a shared attribute, called a tag. Tags are assigned to each site.

**To tag a site:**

1. Log in to the management console.

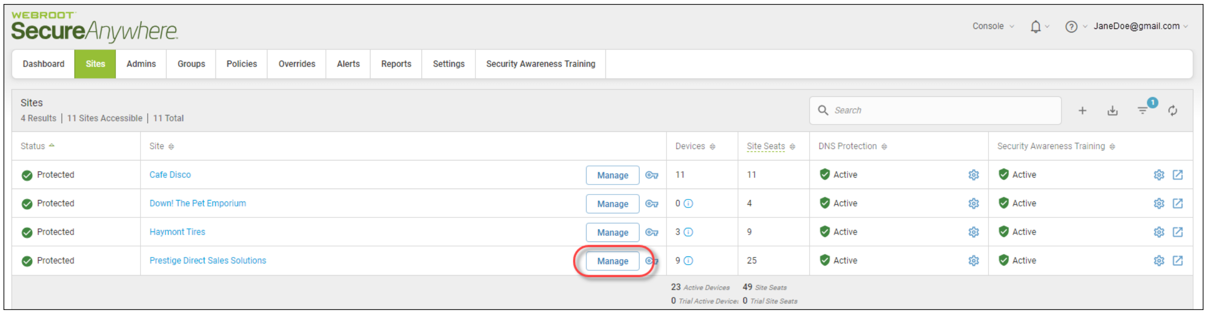
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

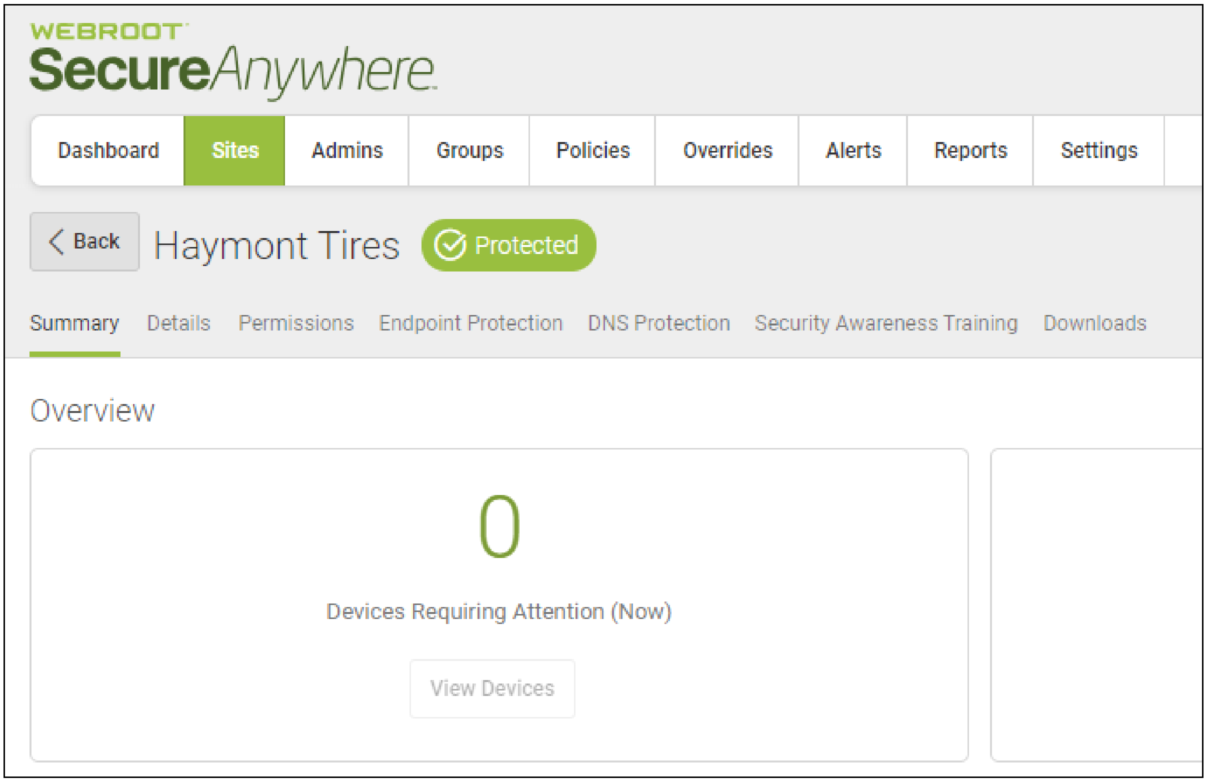
2. Select the site where you want to add tags, and click the **Manage** button.



Sites
4 Results | 11 Sites Accessible | 11 Total

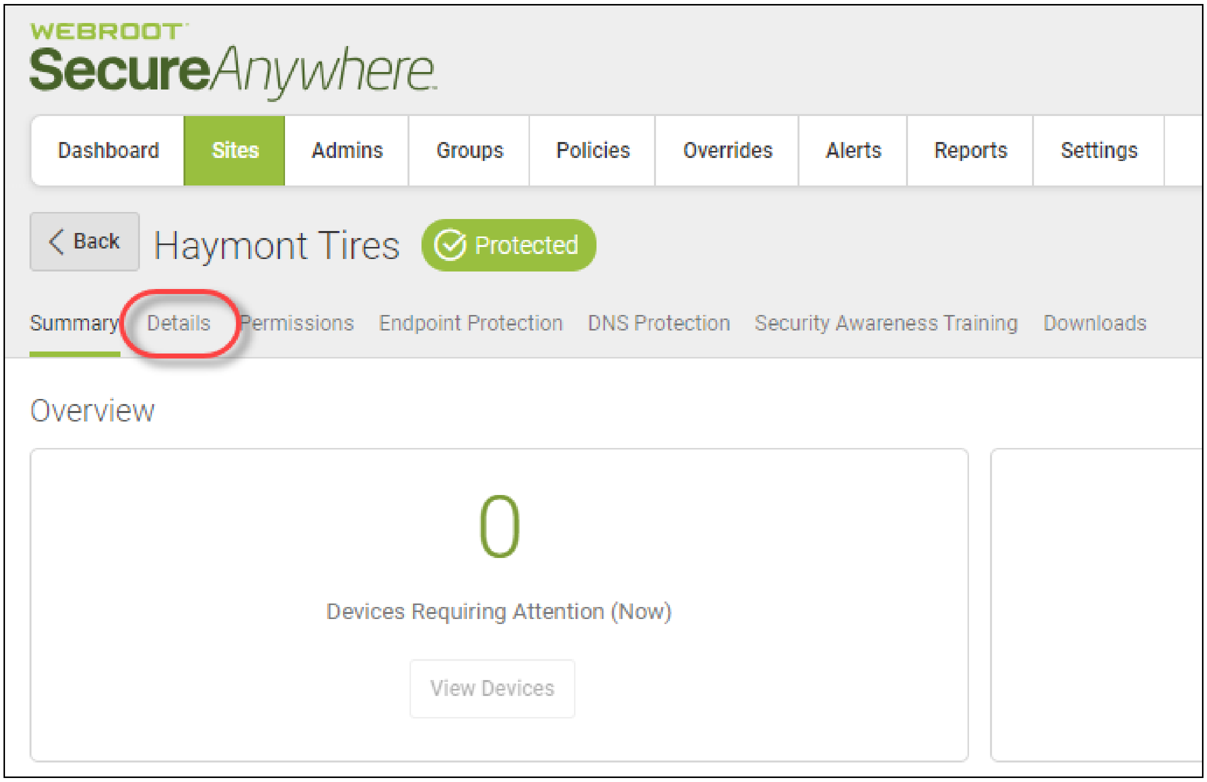
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Manage Sites panel displays with the Summary tab active.

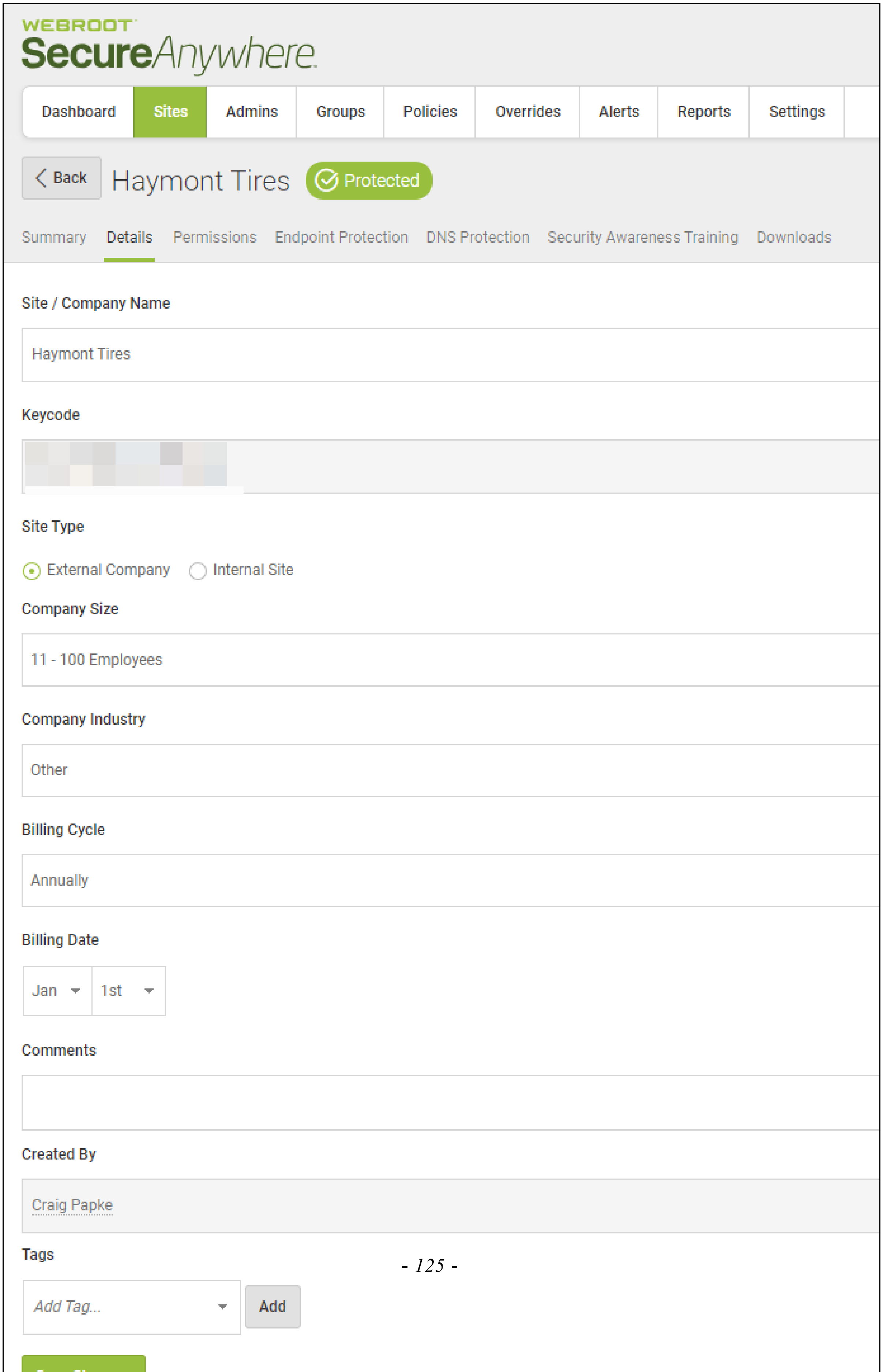


WEBROOT
SecureAnywhere
Dashboard
Sites
Admins
Groups
Policies
Overrides
Alerts
Reports
Settings
Back
Haymont Tires
Protected
Summary
Details
Permissions
Endpoint Protection
DNS Protection
Security Awareness Training
Downloads
Overview
0
Devices Requiring Attention (Now)
View Devices

3. Click the **Details** tab.



The Details tab displays.



Site / Company Name

Haymont Tires

Keycode

[redacted]

Site Type

● External Company ○ Internal Site

Company Size

11 - 100 Employees

Company Industry

Other

Billing Cycle

Annually

Billing Date

Jan 1st

Comments

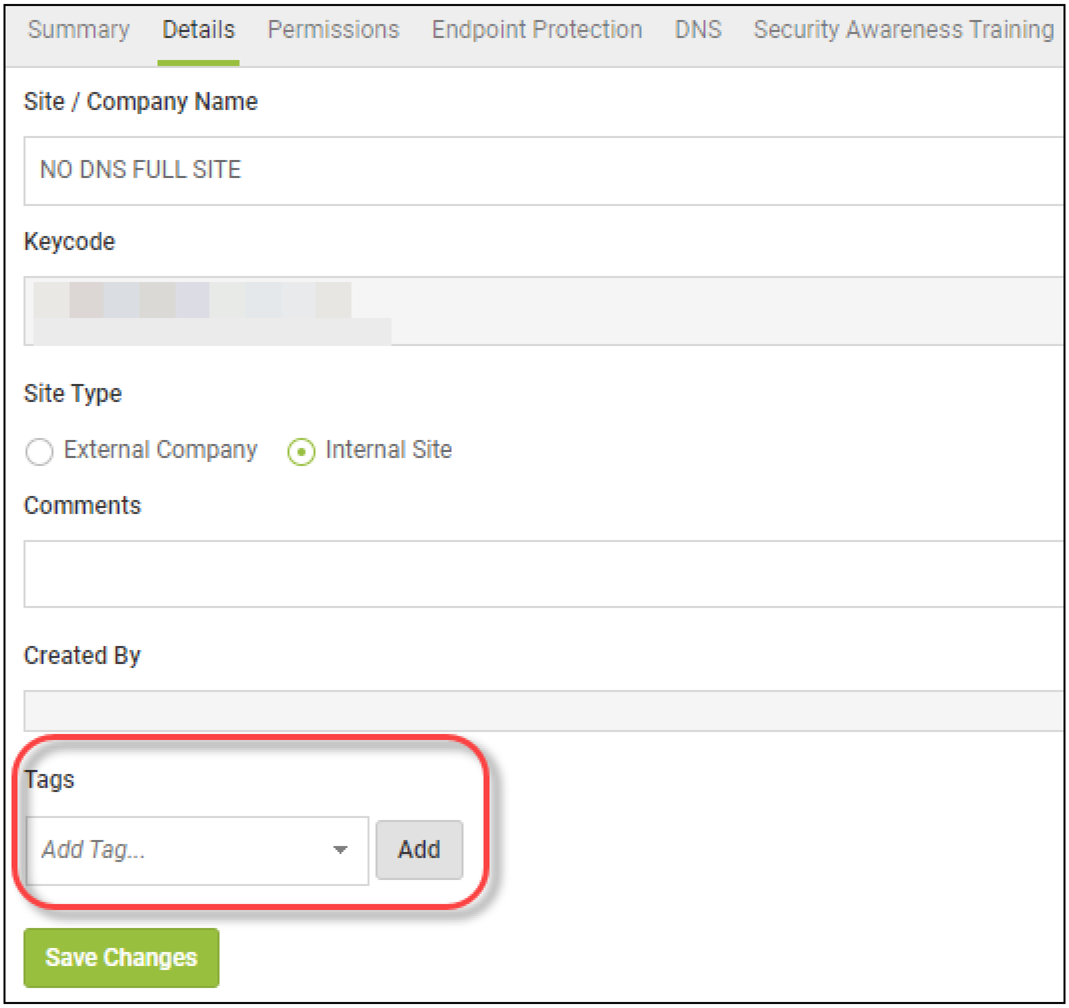
Created By

Craig Papke

Tags

*Add Tag...*

4. In the Tags field, enter as many tags as needed.



Site / Company Name

NO DNS FULL SITE

Keycode

[redacted]

Site Type

○ External Company ● Internal Site

Comments

Created By

Tags

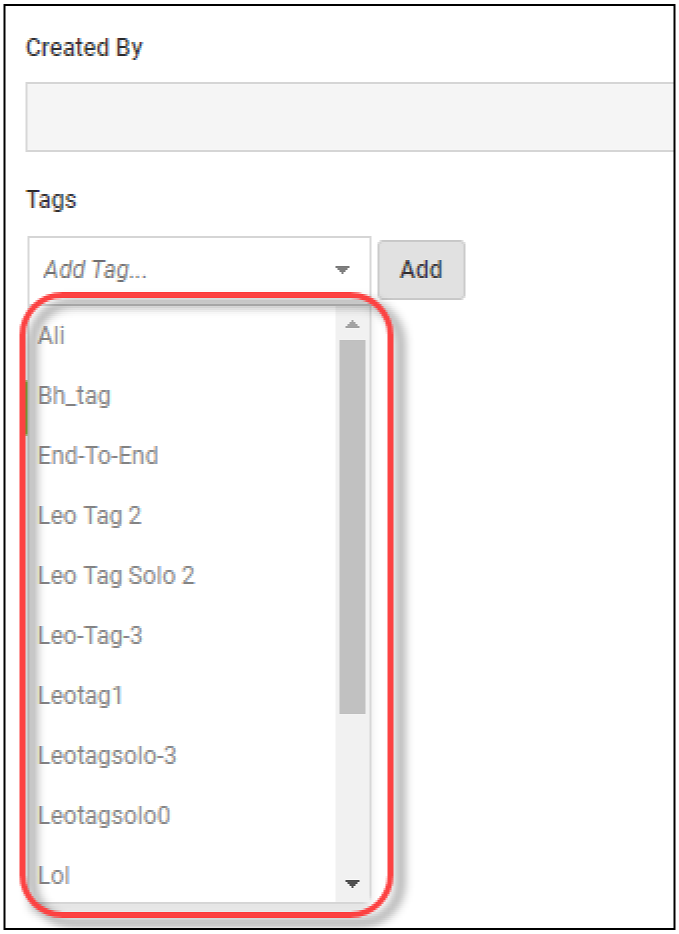
Add Tag...

You can create tags based on any or all of the following:

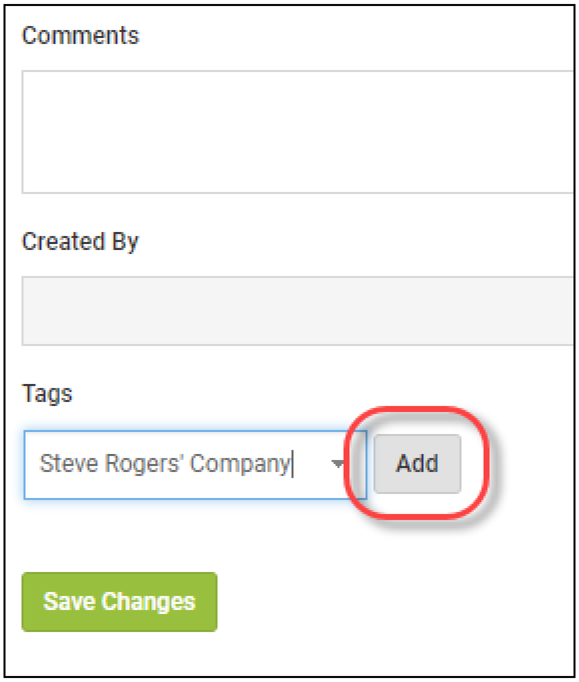
- The type of company, such as medical, construction, or transportation.
- The time zone, geographic location, country, or language.
- The account manager's name, the IT person's name, or the name of your main contact.

**Note:** You can tag a site as many ways as needed, however, you can only filter based on a single tag.

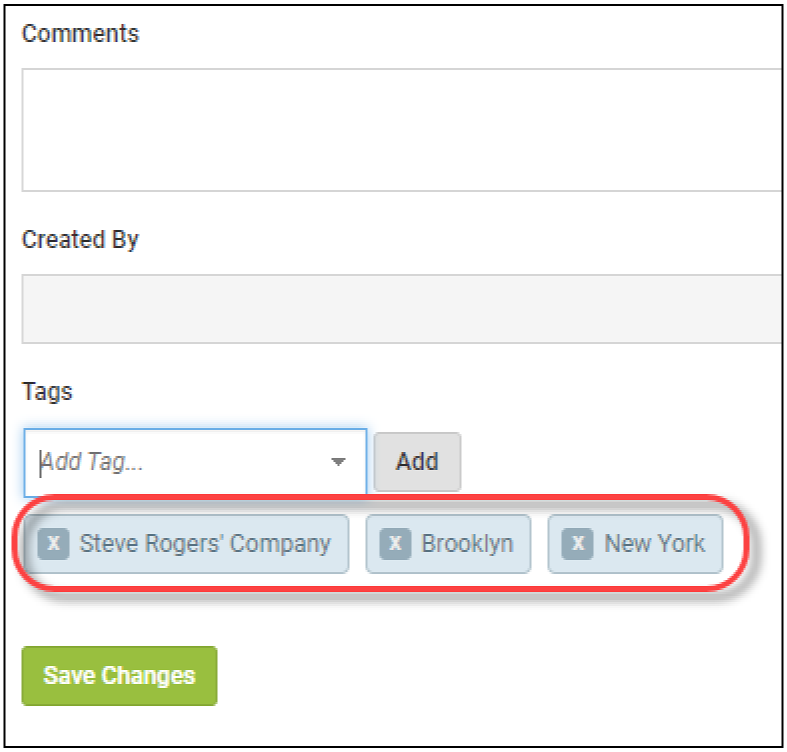
As needed, you can click the arrow to display the Tags drop-down menu, which displays tags that you have previously used.



5. After you add each tag, click the **Add** button.



The added tags display below the Tags field.

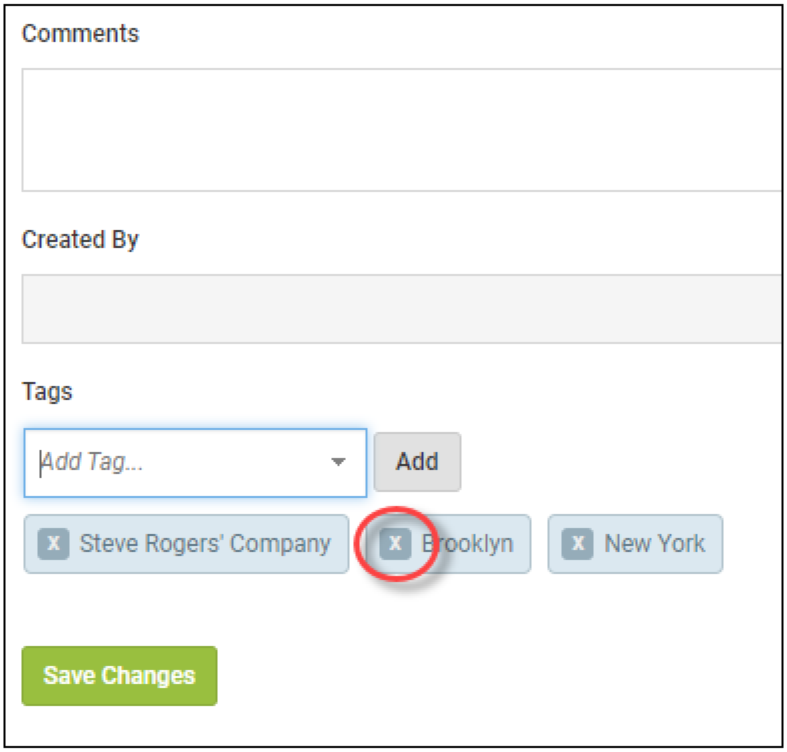


Comments

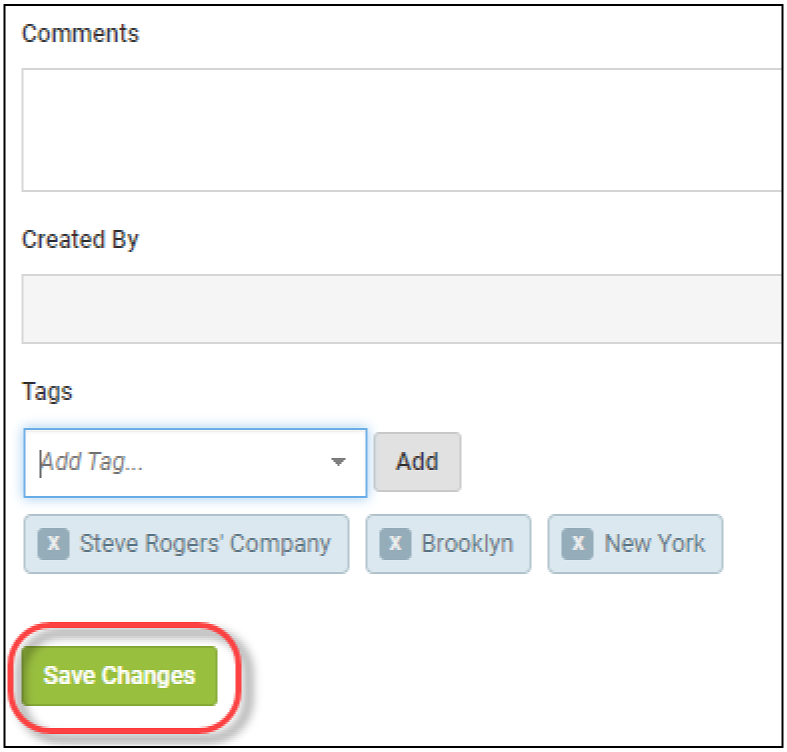
Created By

Tags

6. To remove a tag, click the **X** to the left of each tag.



7. When you're done, click the **Save Changes** button.



Comments

Created By

Tags

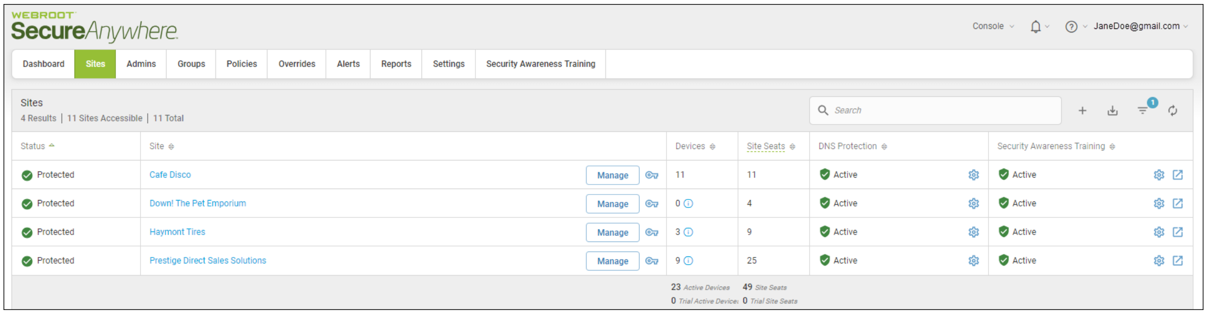
After you have tagged a site, you can use this information to filter on sites. For more information, see *Filtering Sites on page 81*.

# Updating Site Admin Permissions

**To update site admin permissions:**

1. Log in to the management console.

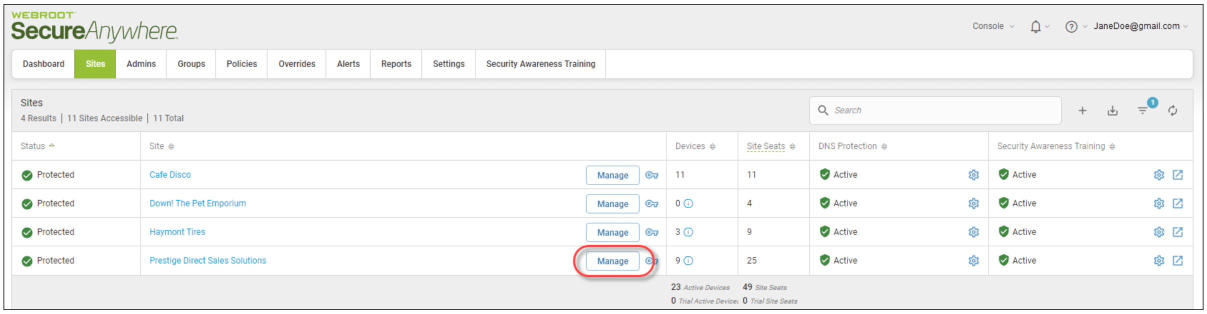
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

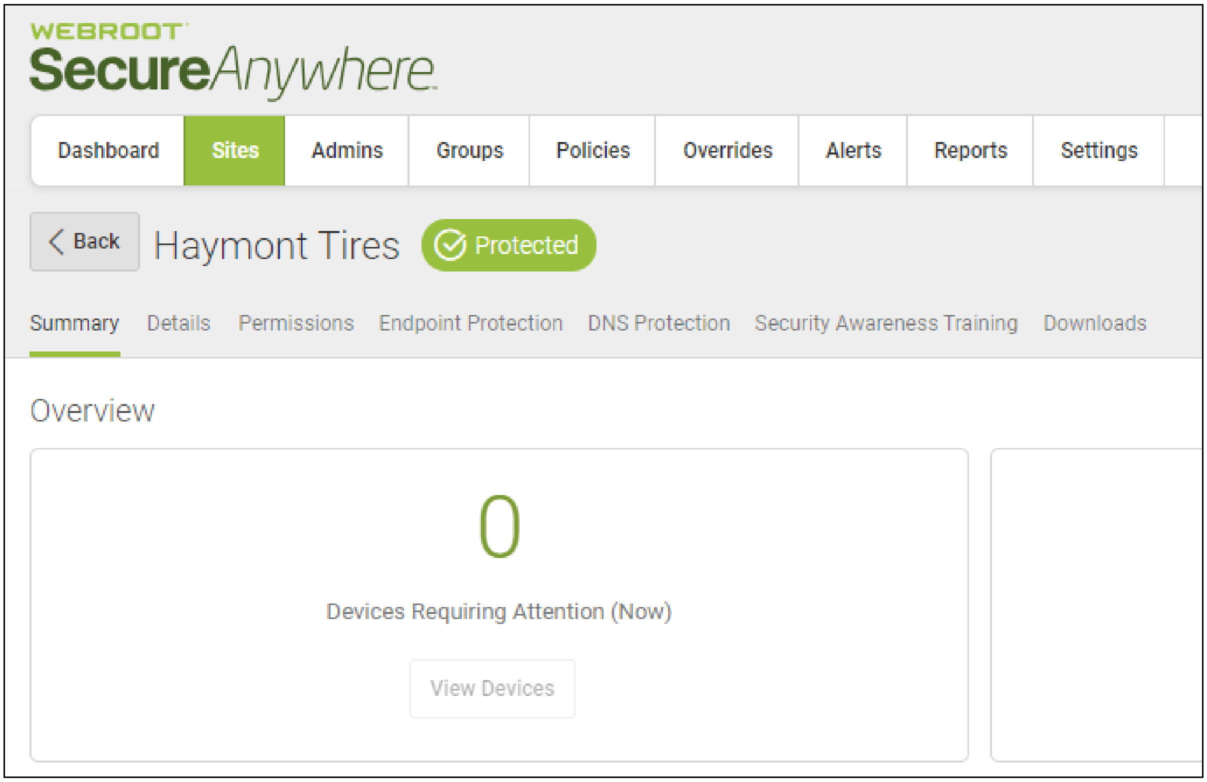
2. Click the **Manage** button.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

The Manage Sites panel displays, with the Summary tab active.



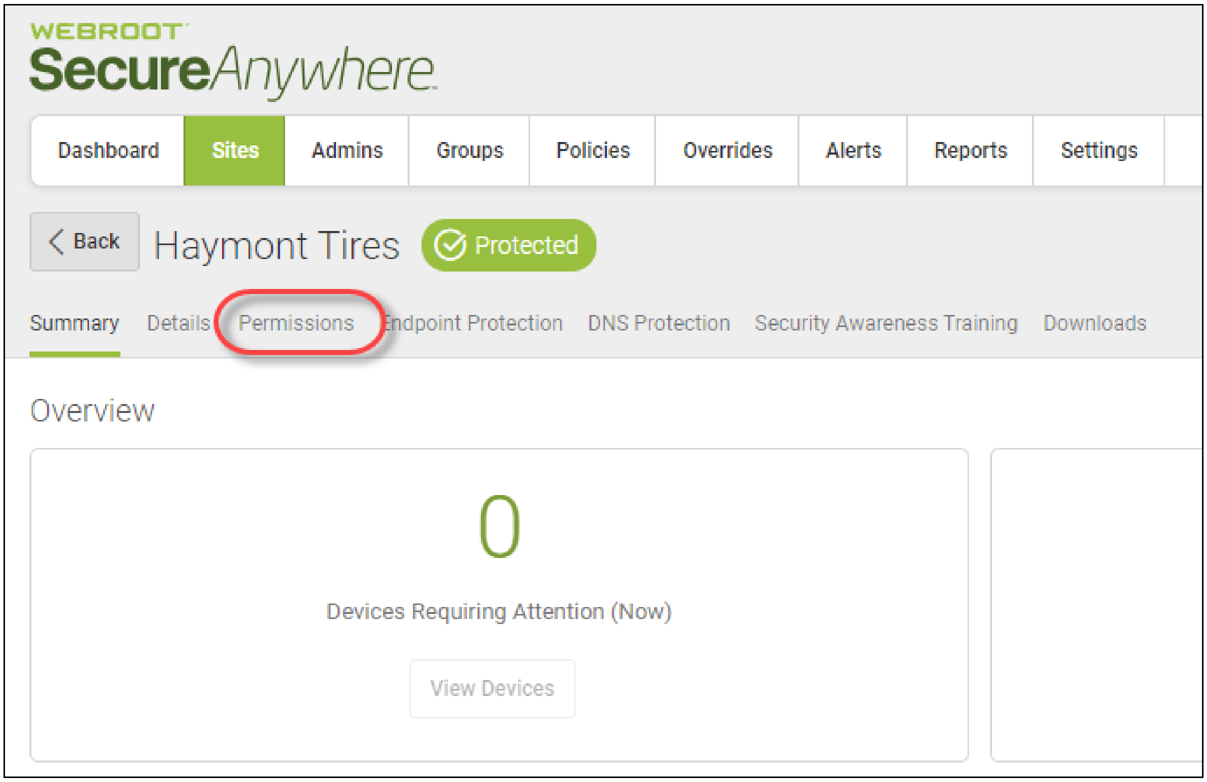
Haymont Tires

Overview

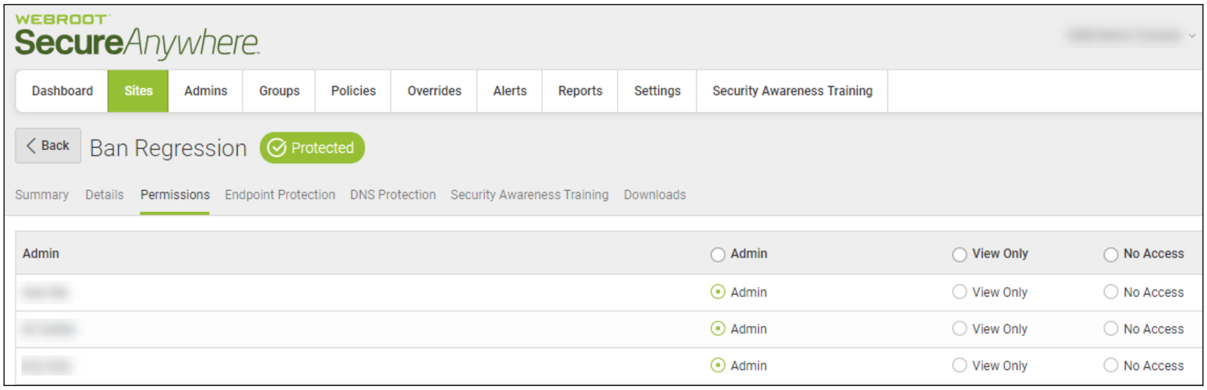
0

Devices Requiring Attention (Now)

3. Click the **Permissions** tab.



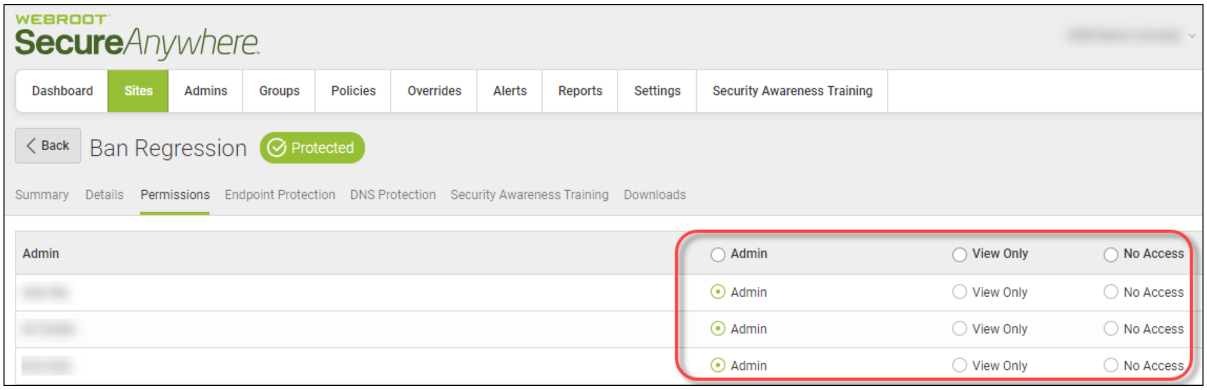
The Permissions tab displays.



| Admin | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| [redacted] | ● Admin | ○ View Only | ○ No Access |
| [redacted] | ● Admin | ○ View Only | ○ No Access |
| [redacted] | ● Admin | ○ View Only | ○ No Access |

4. For each admin, select one of the following radio buttons:
    - **Admin** — Can access all sites, and add, remove, and edit admins.
    - **View Only** — Can only view management console sites.

- **No Access** — Can view the site to which they've been given view permissions.



| Admin | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| [redacted] | ● Admin | ○ View Only | ○ No Access |
| [redacted] | ● Admin | ○ View Only | ○ No Access |
| [redacted] | ● Admin | ○ View Only | ○ No Access |

5. When you're done, click the **Save Changes** button.

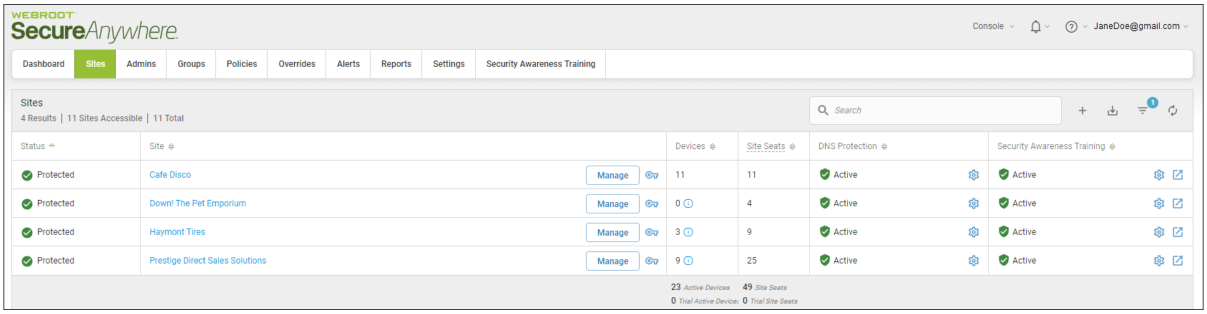
# Editing Site Settings

Follow this procedure to edit information about a site, such as global policies or overrides, report distribution information, and filters.

**To edit a site:**

1. Log in to the management console.

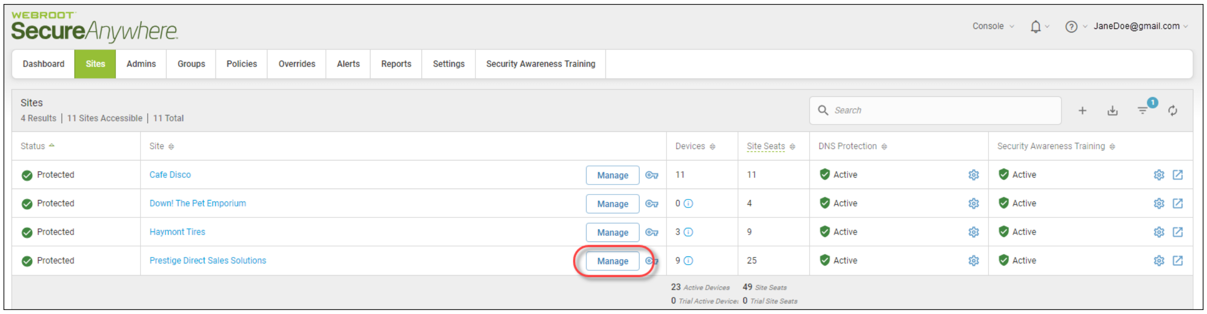
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

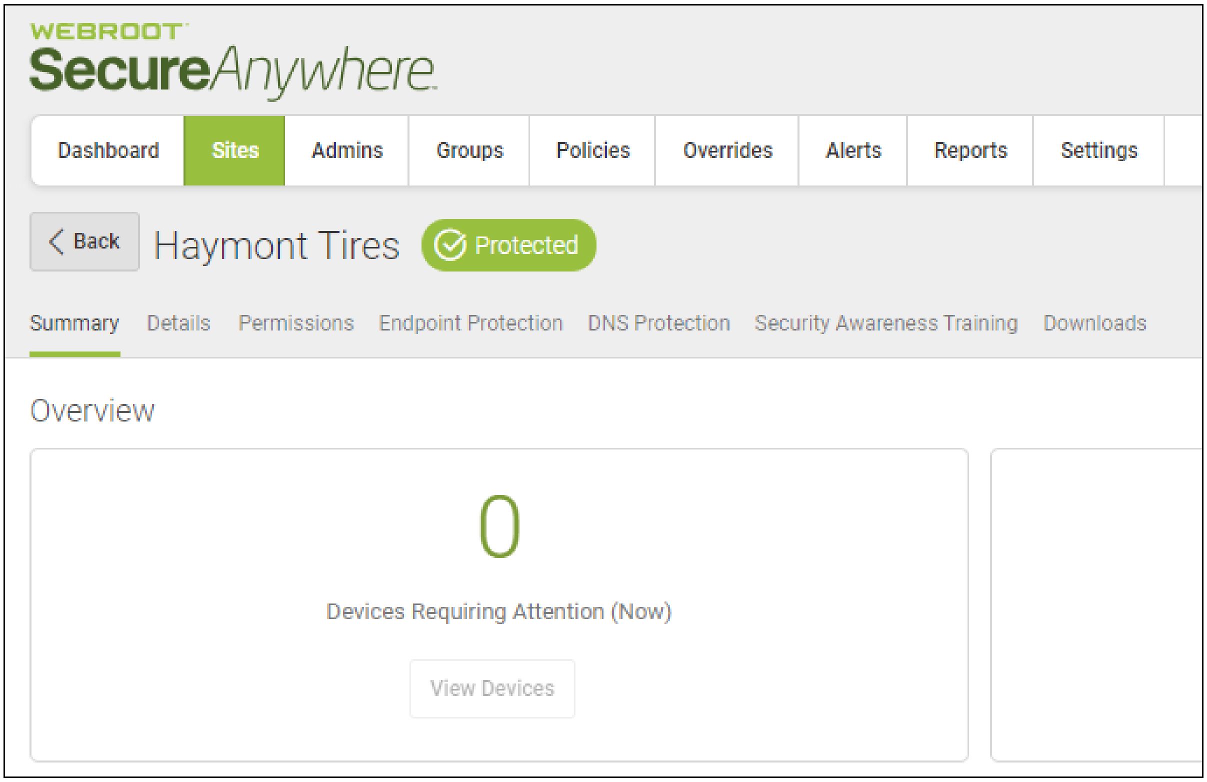
2. Click the **Manage** button.



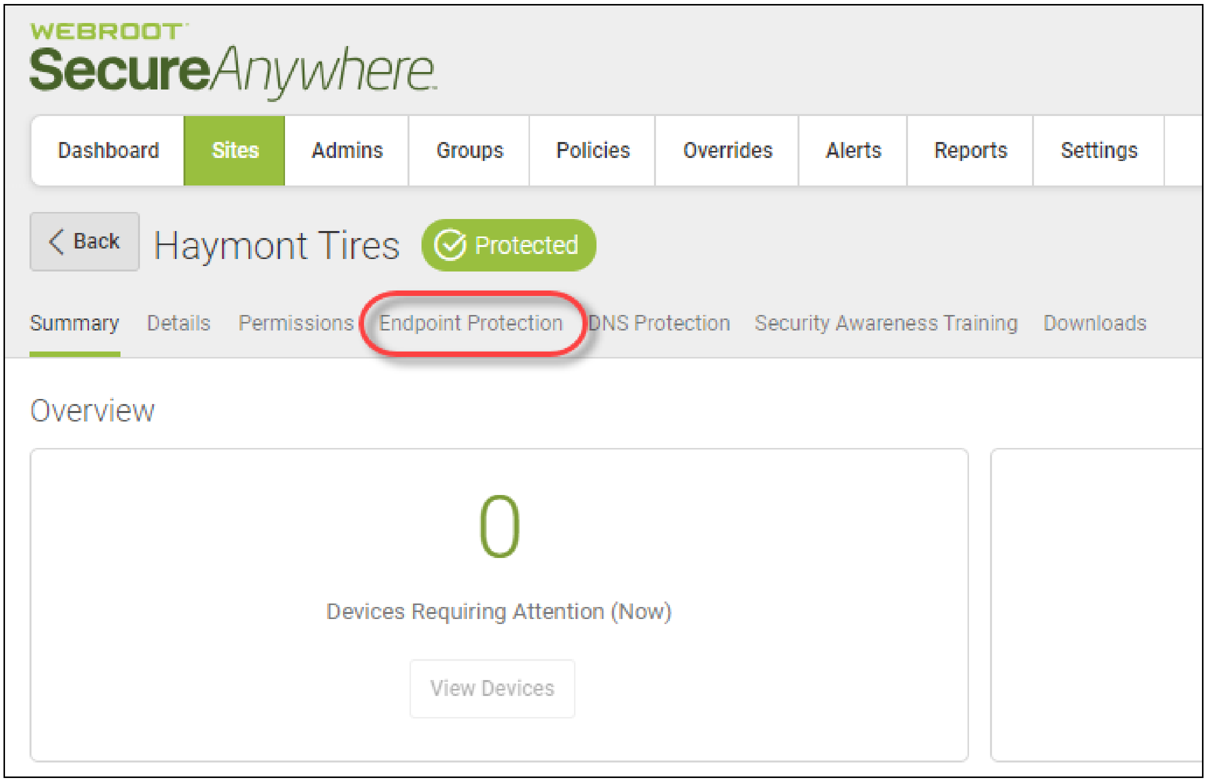
Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

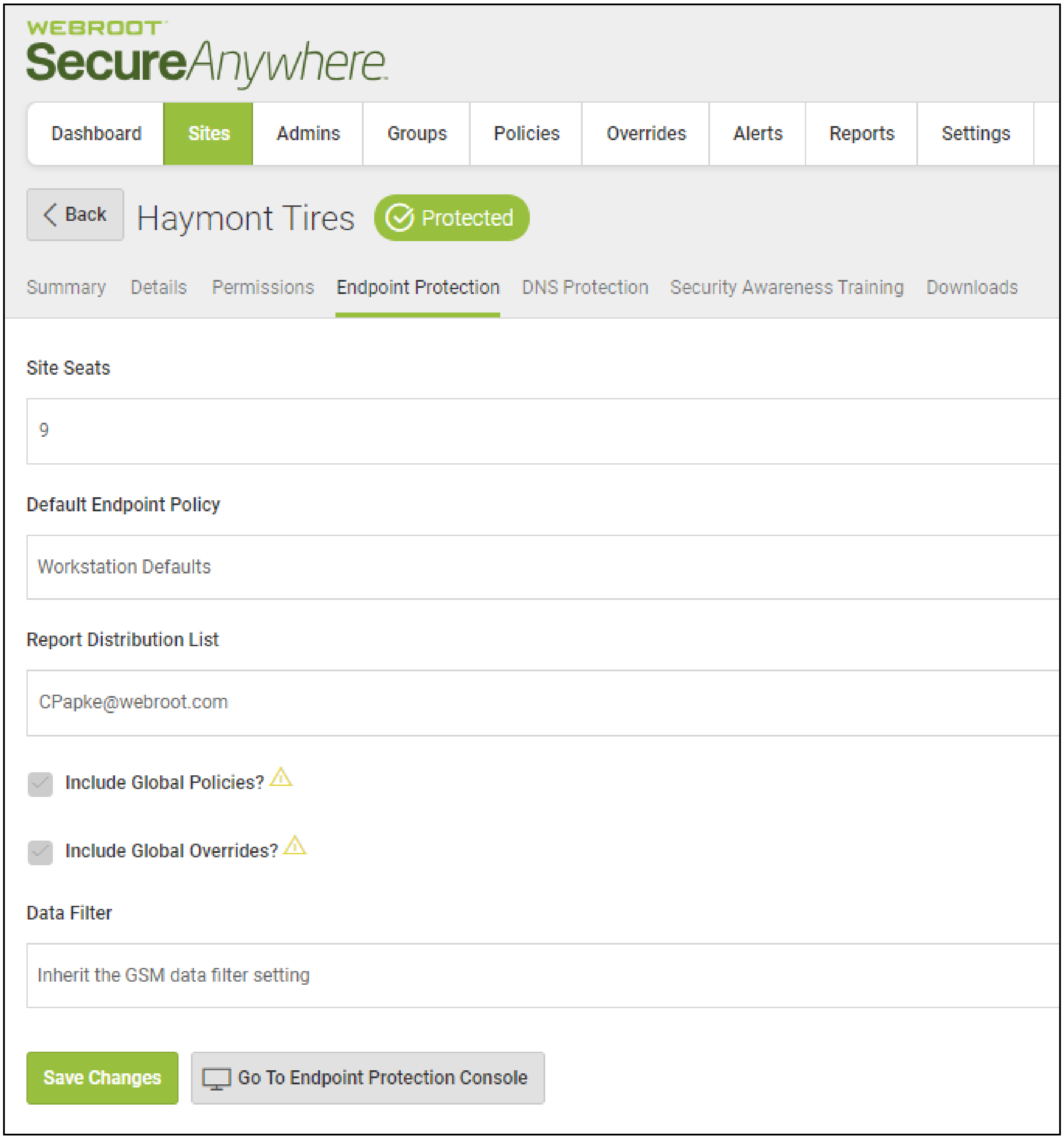
The Manage Sites panel displays, with the Summary tab active.


WEBROOT SecureAnywhere
Dashboard
Sites
Admins
Groups
Policies
Overrides
Alerts
Reports
Settings
Back
Haymont Tires
Protected
Summary
Details
Permissions
Endpoint Protection
DNS Protection
Security Awareness Training
Downloads
Overview
0
Devices Requiring Attention (Now)
View Devices

3. Click the **Endpoint Protection** tab.



The Endpoint Protection tab displays.



Site Seats

9

Default Endpoint Policy

Workstation Defaults

Report Distribution List

CPapke@webroot.com

☑ Include Global Policies? ⚠

☑ Include Global Overrides? ⚠

Data Filter

Inherit the GSM data filter setting

4. In the Site Seats field, enter the number of site seats, as needed. This is an optional step.
5. From the Default Endpoint Policy drop-down menu, select any policy that you would like to set as the default. This is an optional step.

6. For the Include Global Policies checkbox, do one of the following:
   - To include all global policies created at the console level, select the checkbox.
   - To disinclude all global polices created at the console level, deselect the checkbox.

   **Note:** Once selected, including Global Policies cannot be reversed.

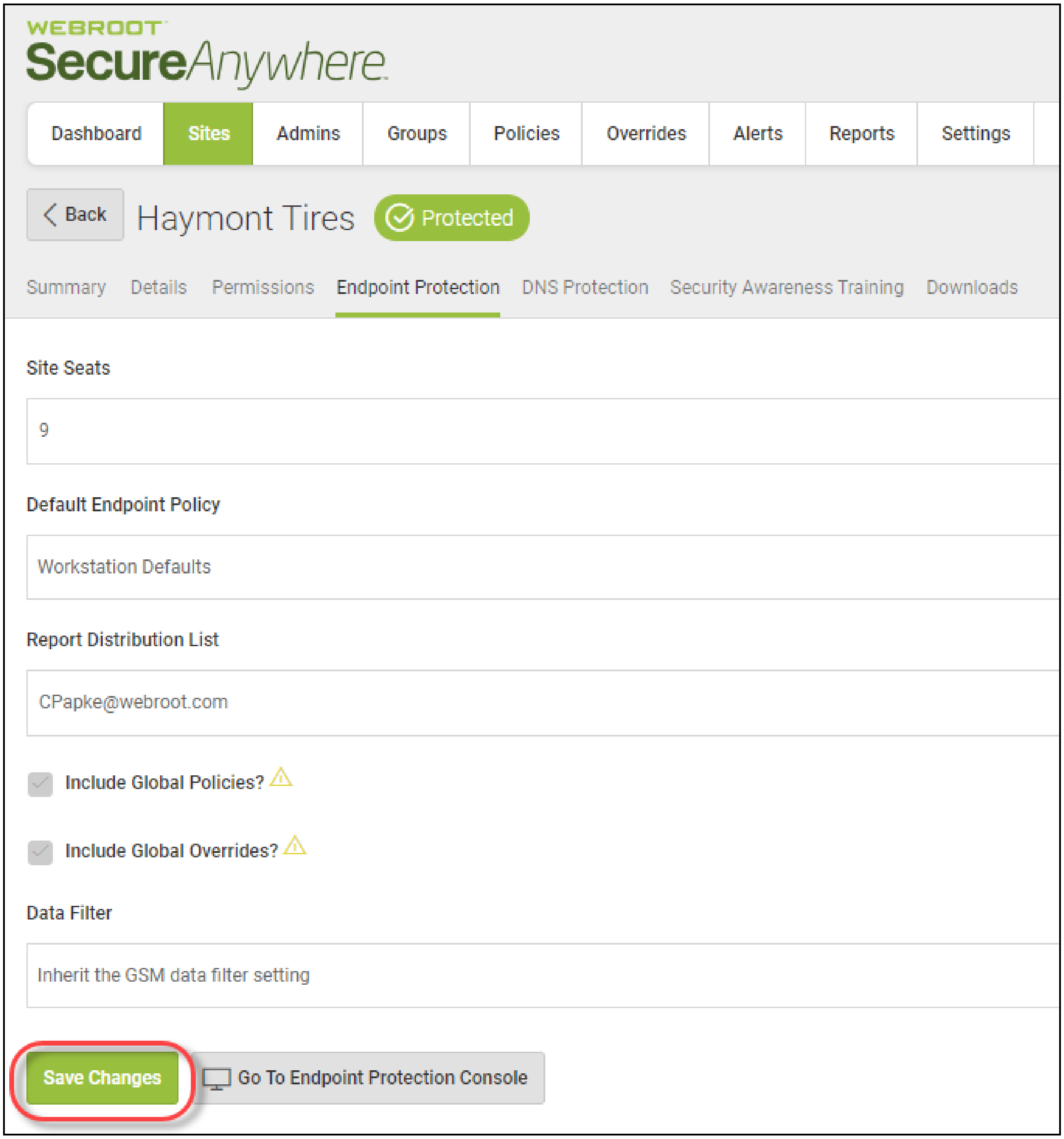
7. For the Include Global Overrides checkbox, do one of the following:
   - To include all global overrides created at the console level, select the checkbox.
   - To disinclude all global overrides created at the console level, deselect the checkbox.

   **Note:** Once selected, including Global Overrides cannot be reversed.

8. In the Report Distribution List field, enter the email address of the person to whom report results should be sent. For more information about reports, see *Global Site Manager Reports Overview on page 441*.
9. From the Data Filter drop-down menu, select setting that you want to filter field, enter the data that you would like to filter sites on.

   For more information, see *Setting Site-Level Data Filters on page 142* and *Filtering Sites on page 81*.

10. When you're done, click the **Save Changes** button.



Site Seats

9

Default Endpoint Policy

Workstation Defaults

Report Distribution List

CPapke@webroot.com

☑ Include Global Policies? ⚠

☑ Include Global Overrides? ⚠

Data Filter

Inherit the GSM data filter setting

# Setting Site-Level Data Filters

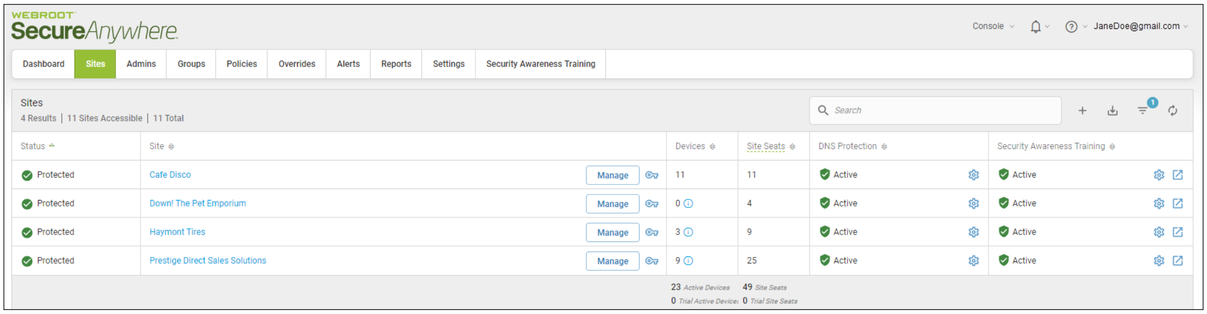
Use the site-level data filter to create data filters at the site level. You can select the same time period options available under the master setting with the additional option to force a particular site to follow the master setting.

For more information on editing site settings, see *Editing Site Settings on page 136*.

**To set a site-level data filter:**

1. Log in to the management console.

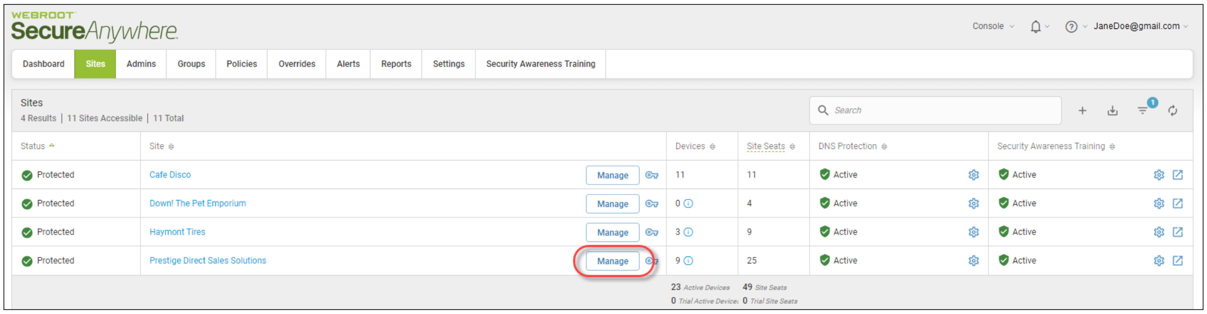
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

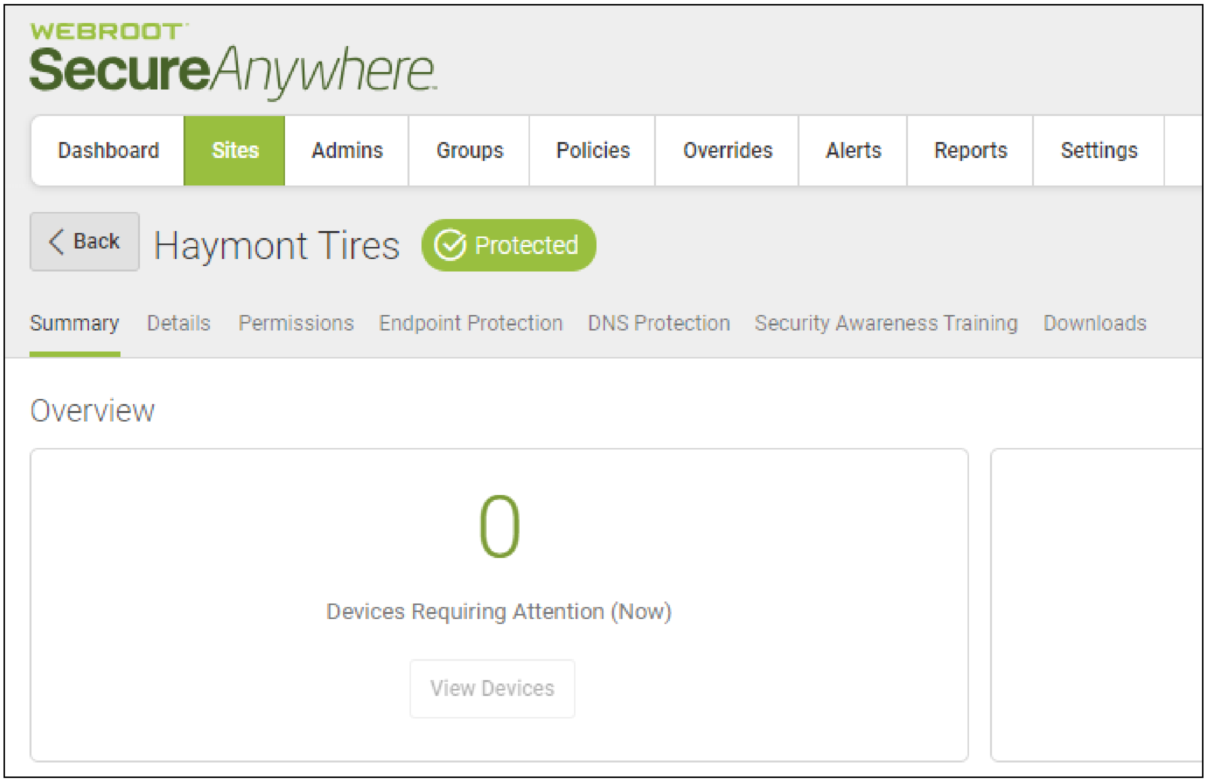
2. Within the site list, for the site that you want to set data filters for, click the **Manage** button.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Manage Sites panel displays, with the Summary tab active.



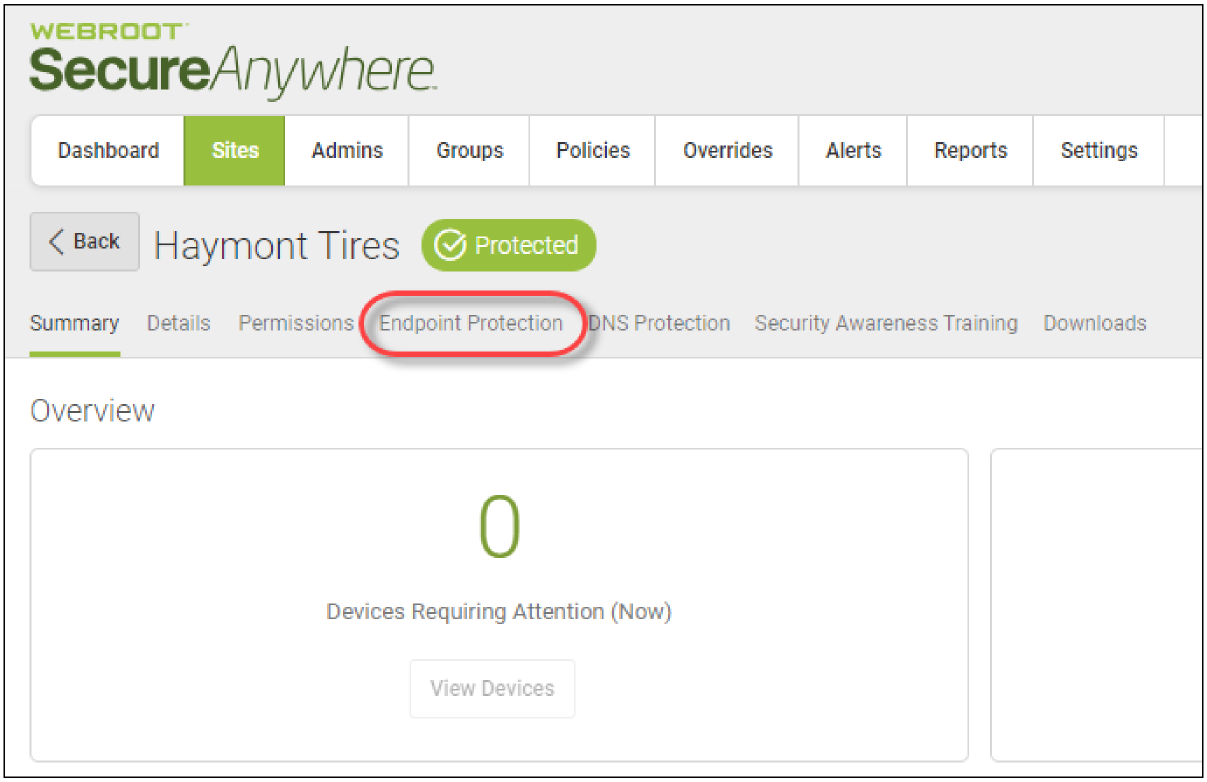
Haymont Tires

Overview

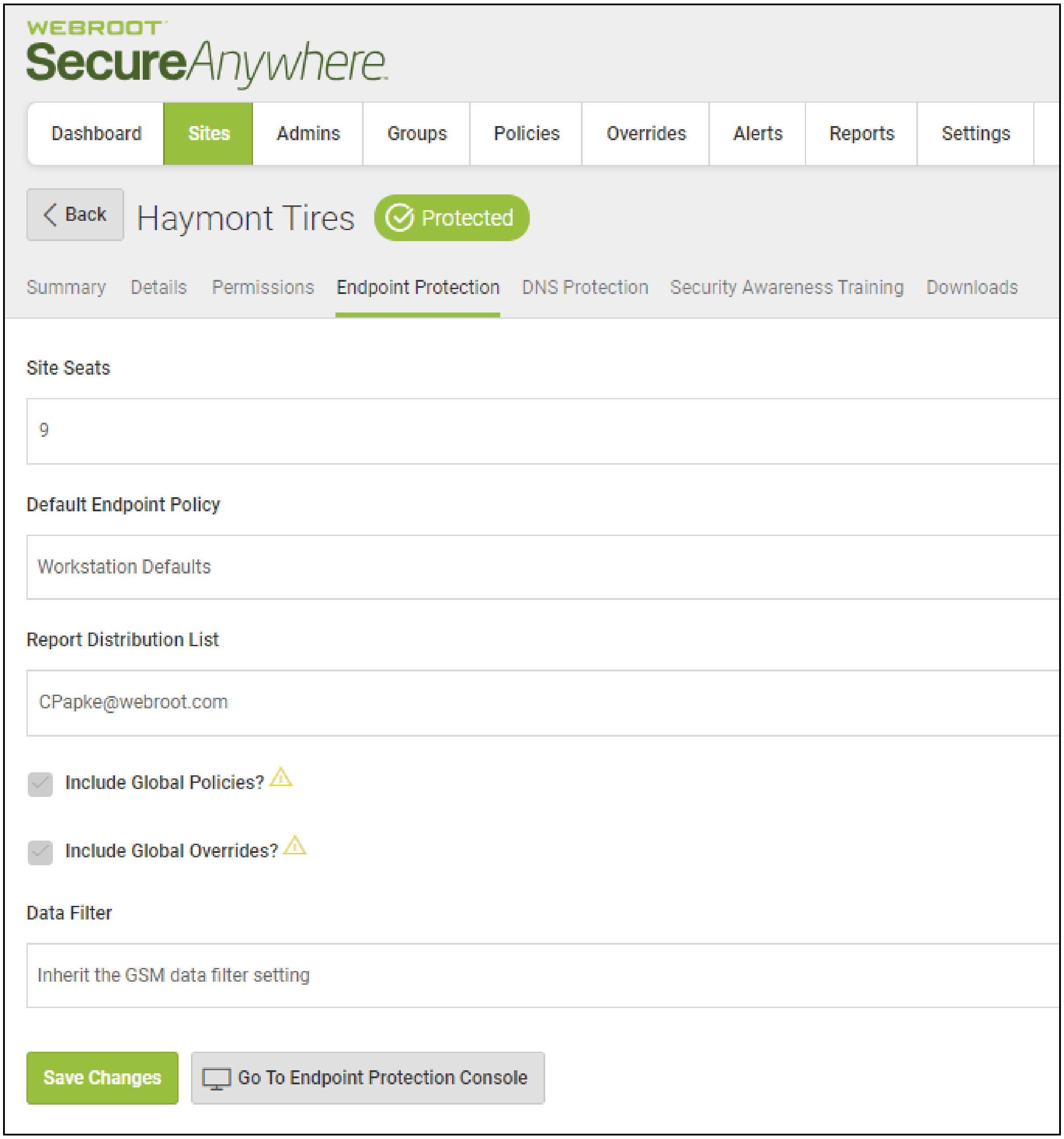
0

Devices Requiring Attention (Now)

3. Click the **Endpoint Protection** tab.



The Endpoint Protection tab displays.



Site Seats

9

Default Endpoint Policy

Workstation Defaults

Report Distribution List

CPapke@webroot.com

☑ Include Global Policies? ⚠

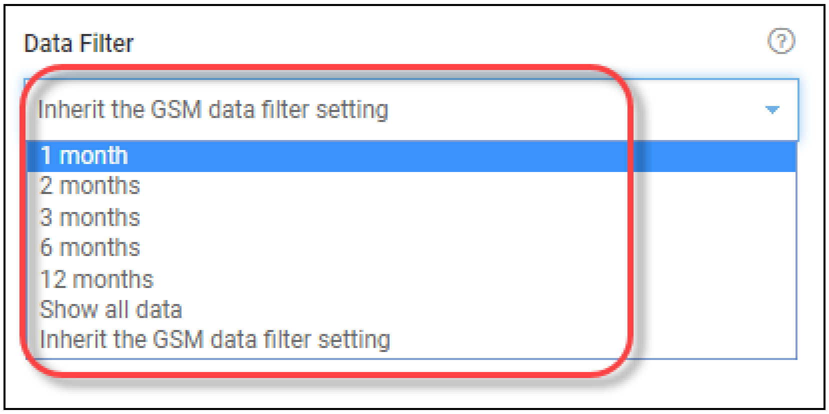
☑ Include Global Overrides? ⚠

Data Filter

Inherit the GSM data filter setting

4. From the Data Filter drop-down menu, select one of the following:
    - **Inherit the GSM data filter setting**
    - **Show all data; this is the default setting**

- **Hide all data for endpoints not seen for 1 month**
- **Hide all data for endpoints not seen for 2 months**
- **Hide all data for endpoints not seen for 3 months**
- **Hide all data for endpoints not seen for 6 months**
- **Hide all data for endpoints not seen for 12 months**



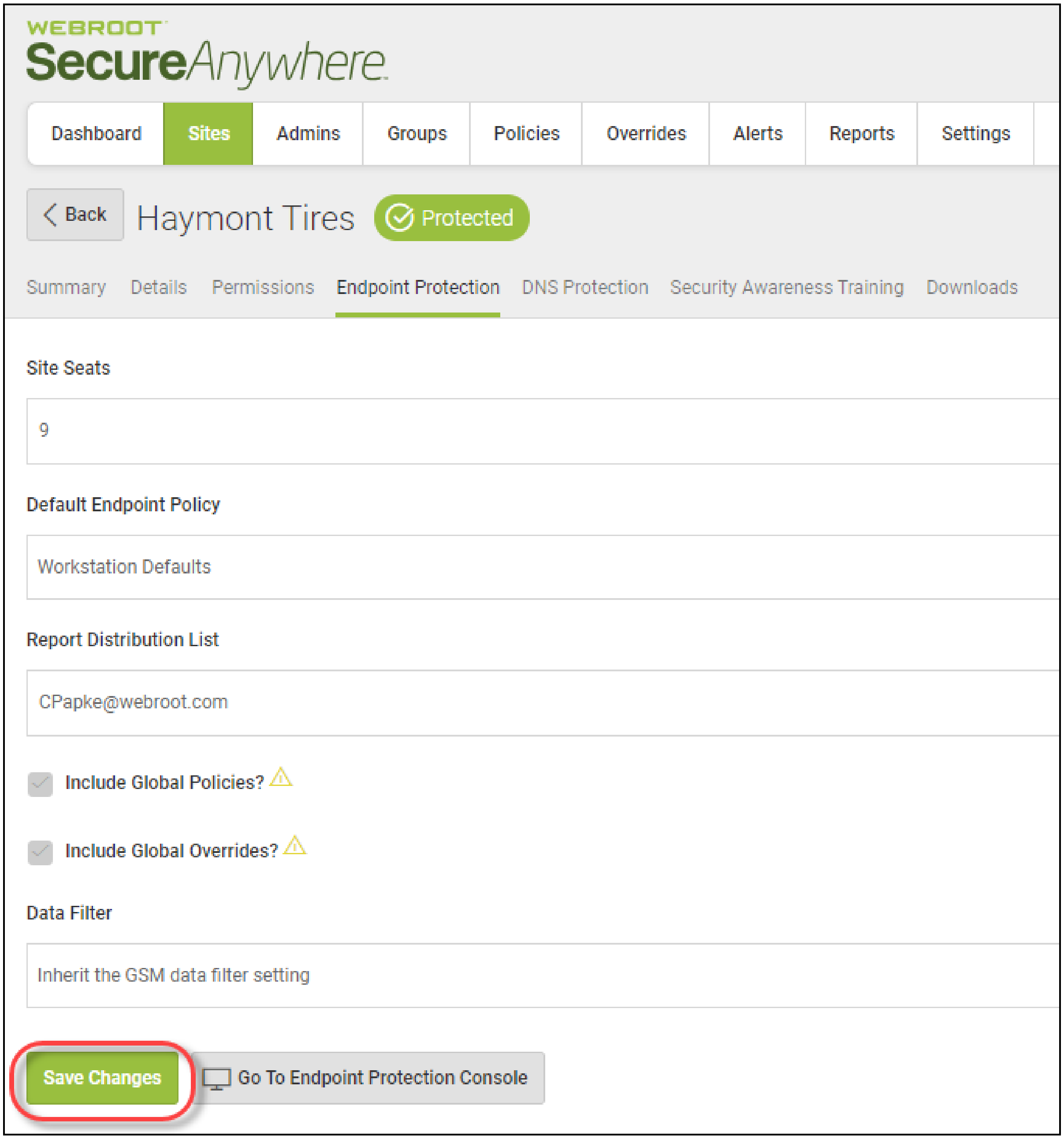
Data Filter

Inherit the GSM data filter setting

1 month
2 months
3 months
6 months
12 months
Show all data
Inherit the GSM data filter setting

**Note**: Limited admin permissions have been updated to grant access to the settings tab when editing a site. From here you may change the default site policy, data filter setting and report distribution list.

5. When you're done, click the **Save Changes** button.



Site Seats

9

Default Endpoint Policy

Workstation Defaults

Report Distribution List

CPapke@webroot.com

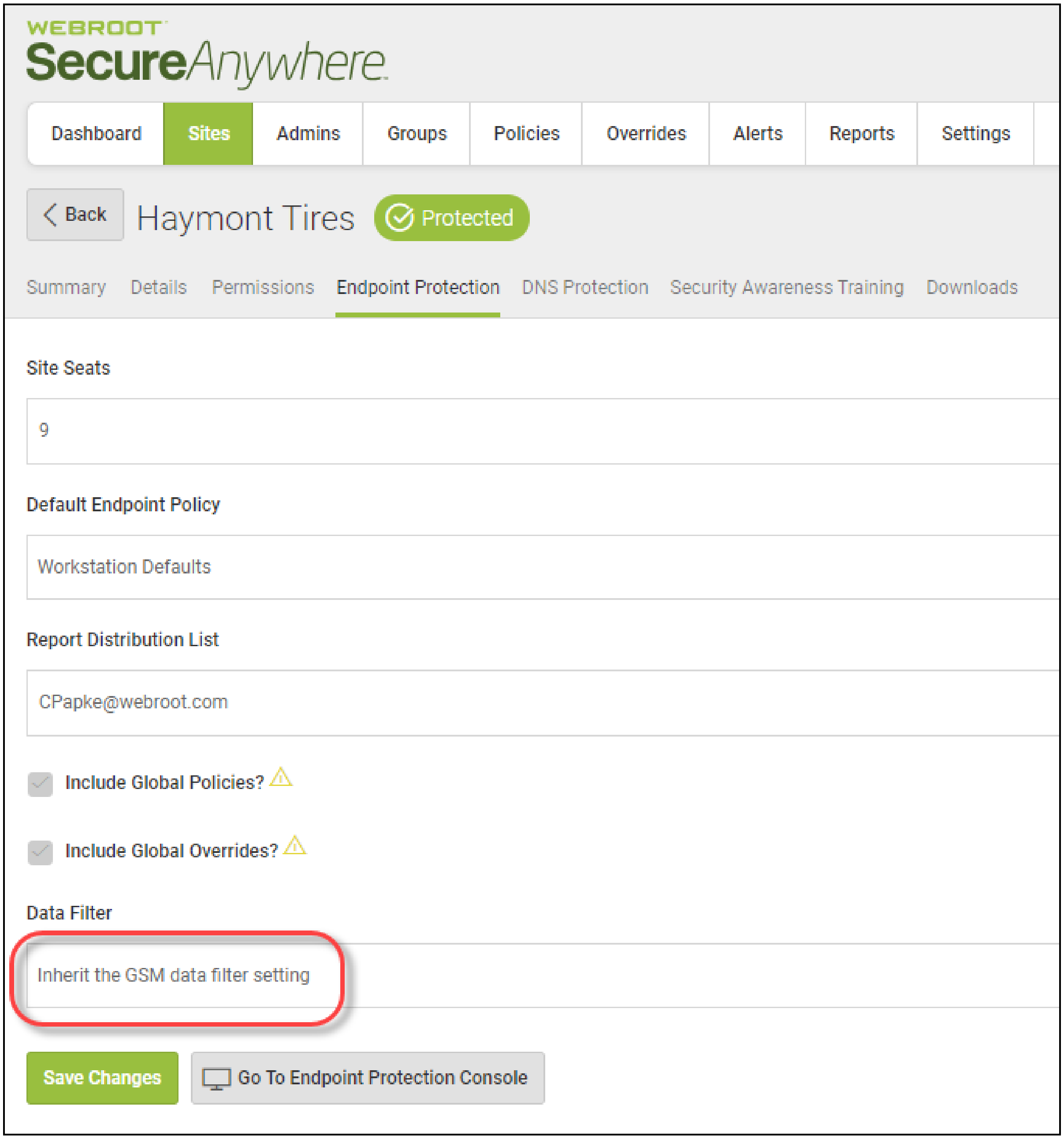
☑ Include Global Policies? ⚠

☑ Include Global Overrides? ⚠

Data Filter

Inherit the GSM data filter setting

The system updates the setting.



Site Seats

9

Default Endpoint Policy

Workstation Defaults

Report Distribution List

CPapke@webroot.com

☑ Include Global Policies? ⚠

☑ Include Global Overrides? ⚠

Data Filter

Inherit the GSM data filter setting

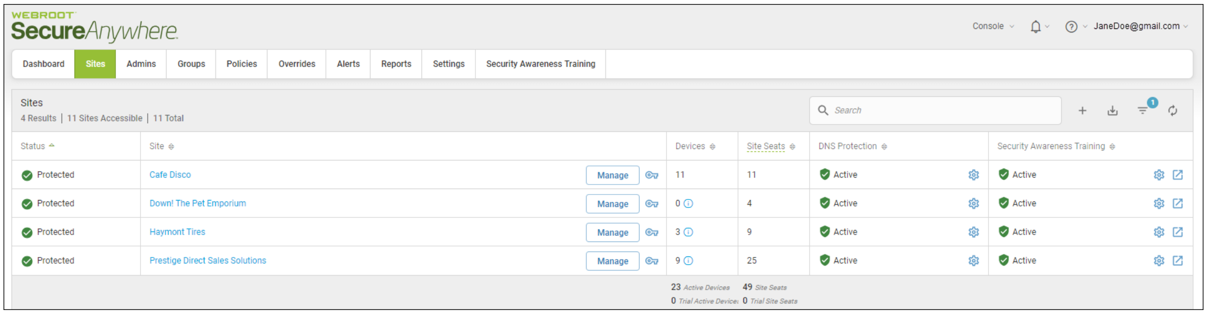
# Downloading Webroot

For quick and easy deployment of the Webroot SecureAnywhere software to select devices, follow this procedure.

**To download Webroot:**

1. Log in to the management console.

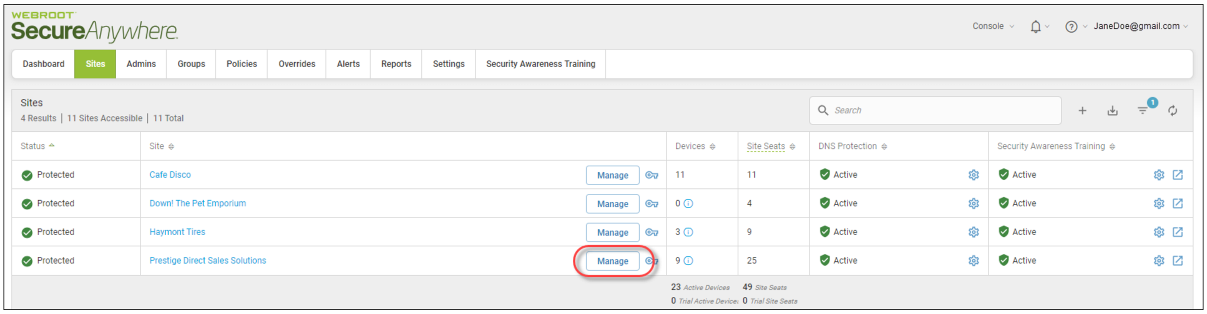
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

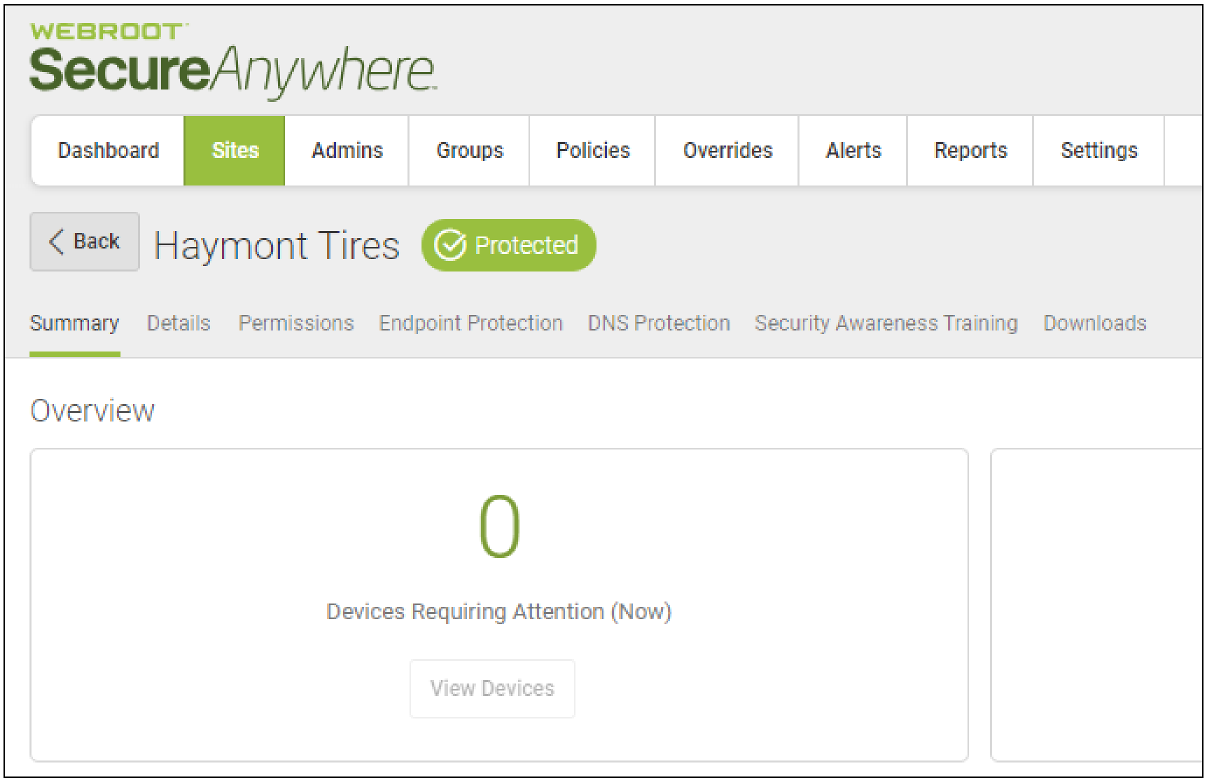
2. Click the **Manage** button.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

The Manage Sites panel displays, with the Summary tab active.



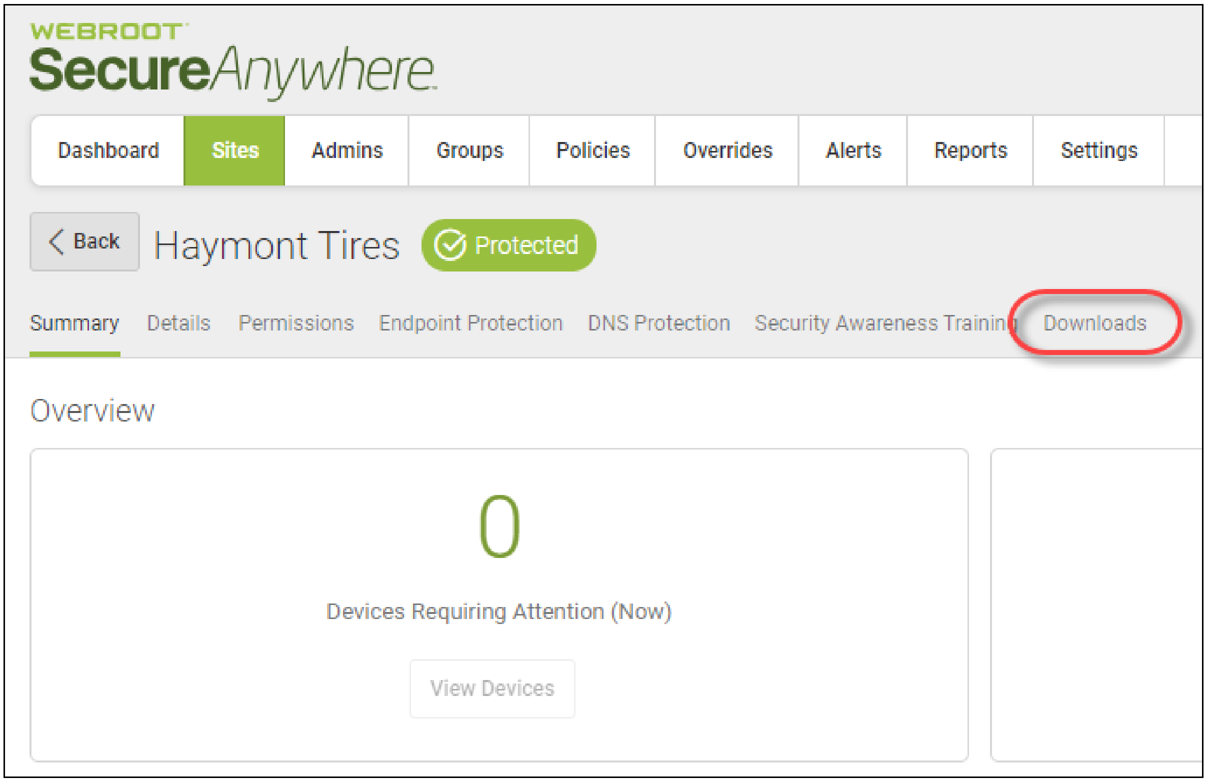
Haymont Tires

Overview

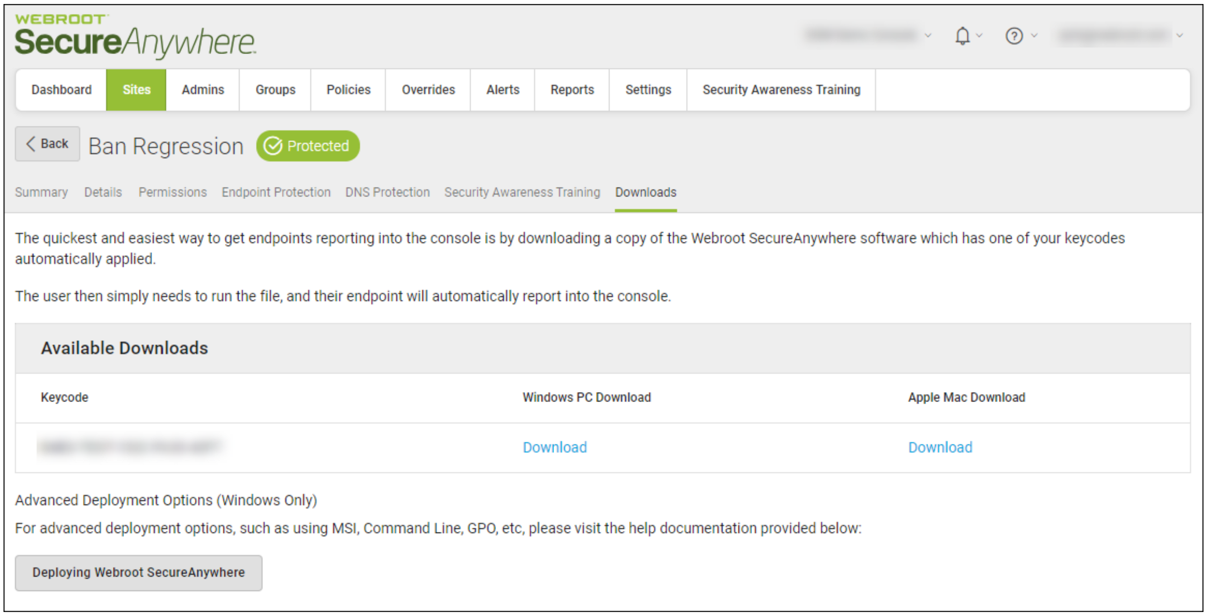
0

Devices Requiring Attention (Now)

3. Click the **Downloads** button.



The Downloads tab displays.



The quickest and easiest way to get endpoints reporting into the console is by downloading a copy of the Webroot SecureAnywhere software which has one of your keycodes automatically applied.

The user then simply needs to run the file, and their endpoint will automatically report into the console.

**Available Downloads**

| Keycode | Windows PC Download | Apple Mac Download |
|---|---|---|
| [redacted] | Download | Download |

Advanced Deployment Options (Windows Only)

For advanced deployment options, such as using MSI, Command Line, GPO, etc, please visit the help documentation provided below:

4. Do either of the following:
   - To download Webroot for Windows PC devices, in the Windows PC Download column, click the **Download** link.
   - To download Webroot for Apple Mac devices, in the Apple Mac Download column, click the **Download** link.
5. Run the downloaded file. Endpoints automatically report into the console.

# Chapter 4: Working With Admins

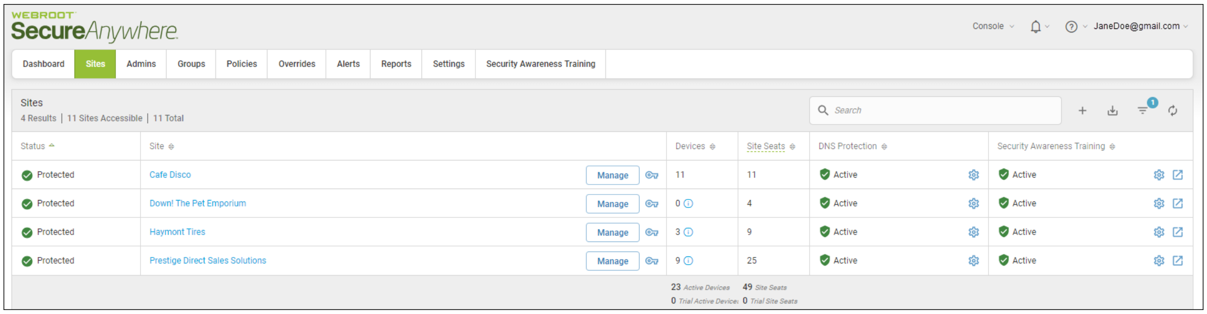
# Adding Admins

You can add additional admins to the different sites.

**To add an admin:**

1. Log in to the management console.

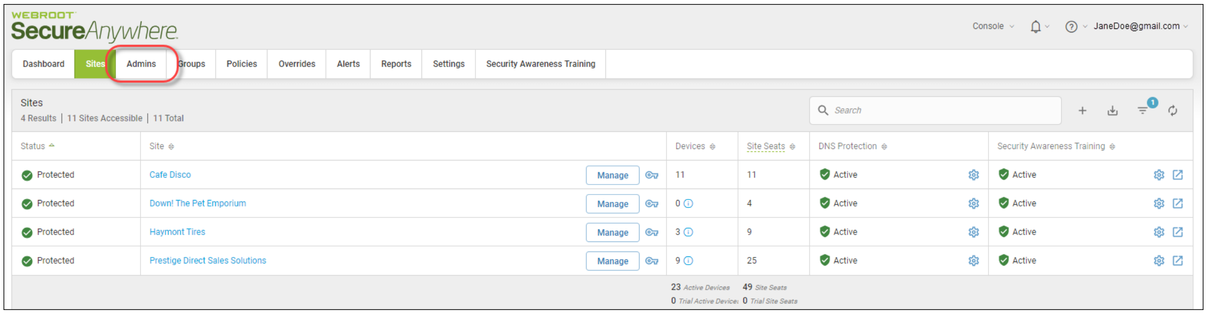
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

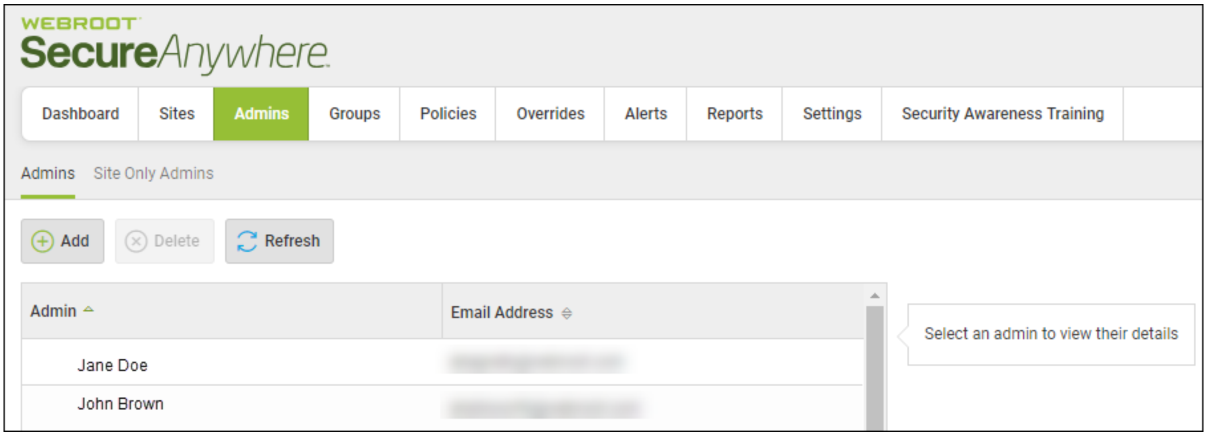
2. Click the **Admins** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

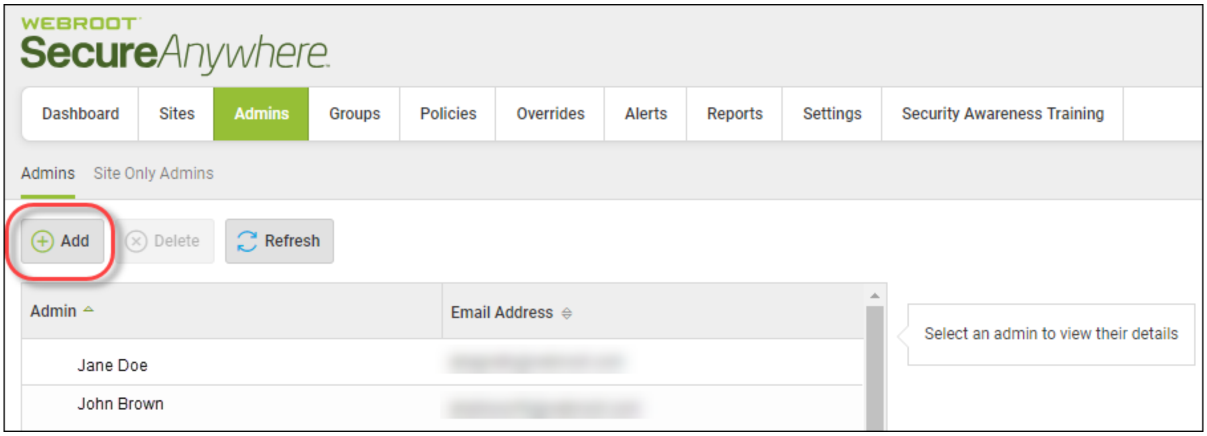
The system displays the Admins tab.



| Admin | Email Address |
|---|---|
| Jane Doe | [redacted] |
| John Brown | [redacted] |

Select an admin to view their details

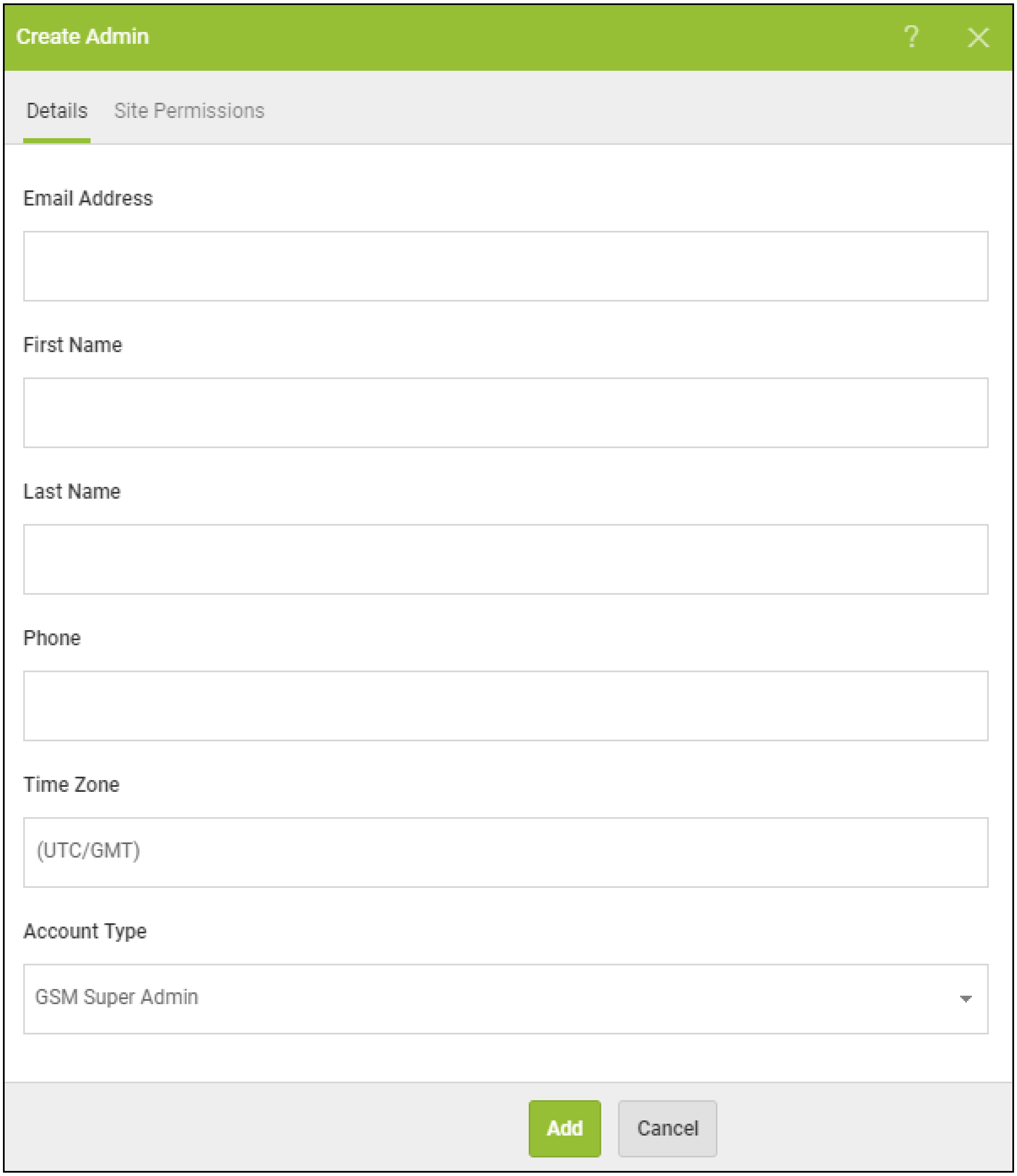
3. Click the **Add** button.



| Admin | Email Address |
|---|---|
| Jane Doe | [redacted] |
| John Brown | [redacted] |

Select an admin to view their details

The system displays the Create Admin window.



Email Address

First Name

Last Name

Phone

Time Zone

(UTC/GMT)

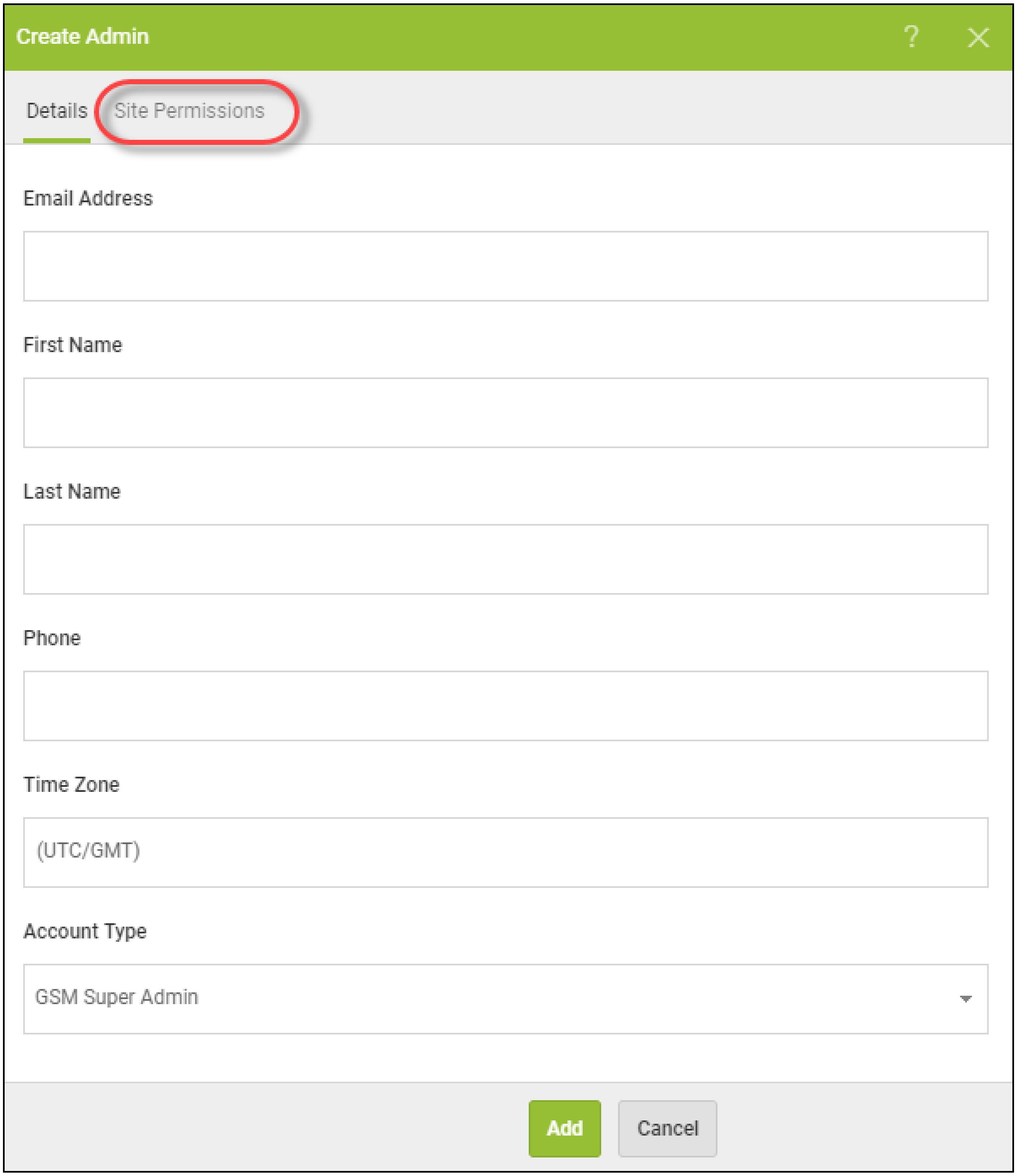
Account Type

GSM Super Admin

4. In the Email field, enter the email of the admin being added.

5. In the First Name field, enter the first name of the admin being added.
6. In the Last Name field, enter the last name of the admin being added.
7. In the Phone field, enter the phone number of the admin being added.
8. In the Time Zone field, click the **Pencil** icon, and enter the country, region, or major city that represents the appropriate time zone of the admin being added.
9. In the Account Type field, from the drop-down menu, select one of the following options:
   - **GSM Super Admin** — Can access all sites, and add, remove, and edit admins.
   - **GSM Limited Admin** — Can only view sites, and cannot add, remove, or edit admins.
   - **Site Admin Only (No GSM Access)** — Can view the site to which they've been given view permissions.

10. Click the **Site Permissions** tab.



Email Address

First Name

Last Name

Phone

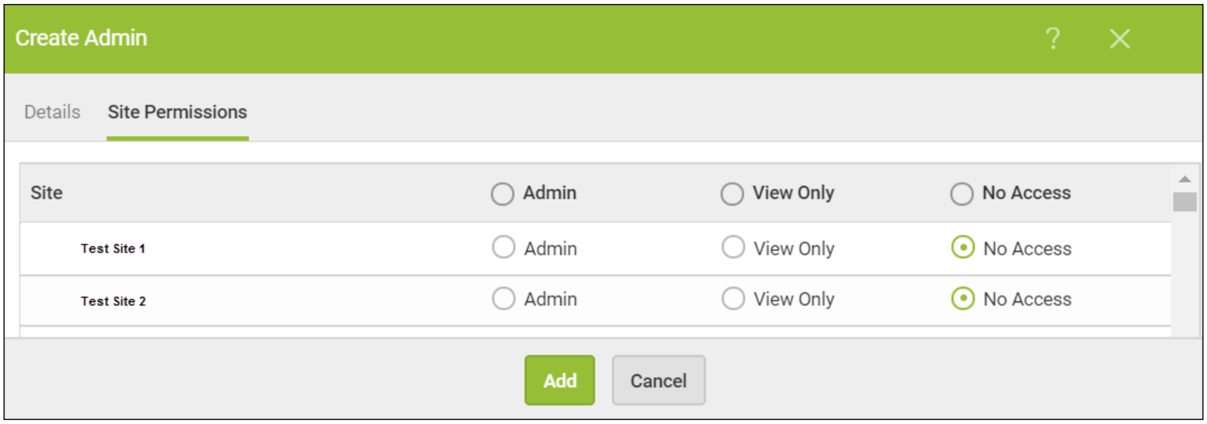
Time Zone

(UTC/GMT)

Account Type

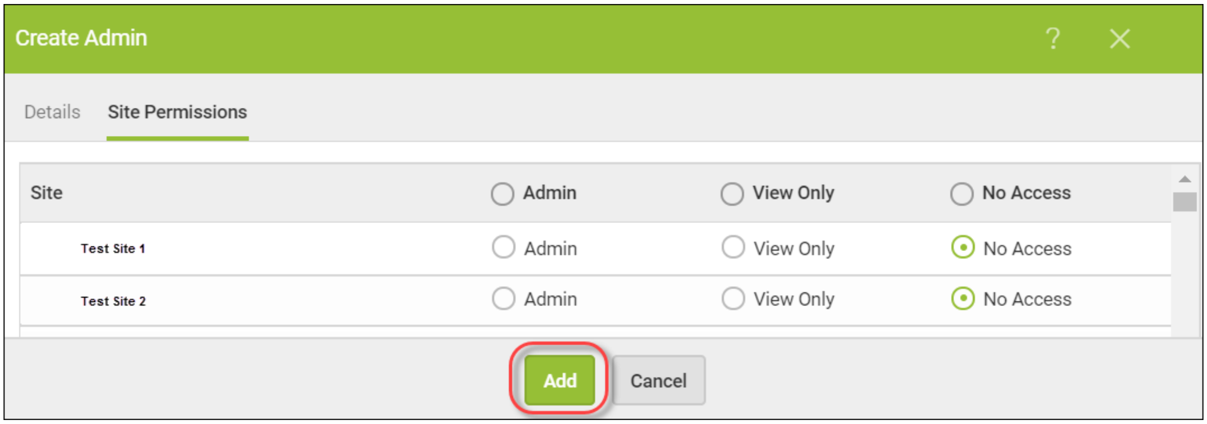
GSM Super Admin

The system displays the Site Permissions tab.



| Site | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| Test Site 1 | ○ Admin | ○ View Only | ● No Access |
| Test Site 2 | ○ Admin | ○ View Only | ● No Access |

11. For each site, select one of the following permission levels:
    - **Admin**
    - **View Only**
    - **No Access**
12. When you're done, click the **Add** button.



| Site | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| Test Site 1 | ○ Admin | ○ View Only | ● No Access |
| Test Site 2 | ○ Admin | ○ View Only | ● No Access |

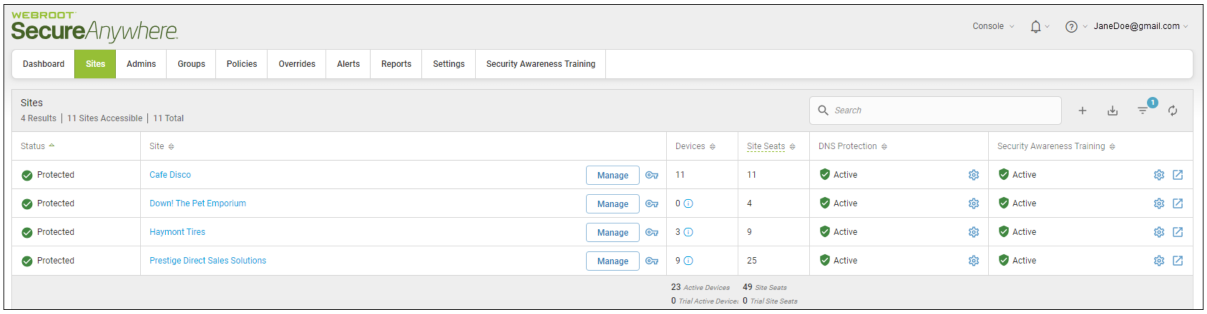
# Updating Admin Information

Follow this procedure to view and update admin information. You can also update admin permissions by following the *Updating Site Admin Permissions on page 132* procedure.

**To work with admins:**

1. Log in to the management console.

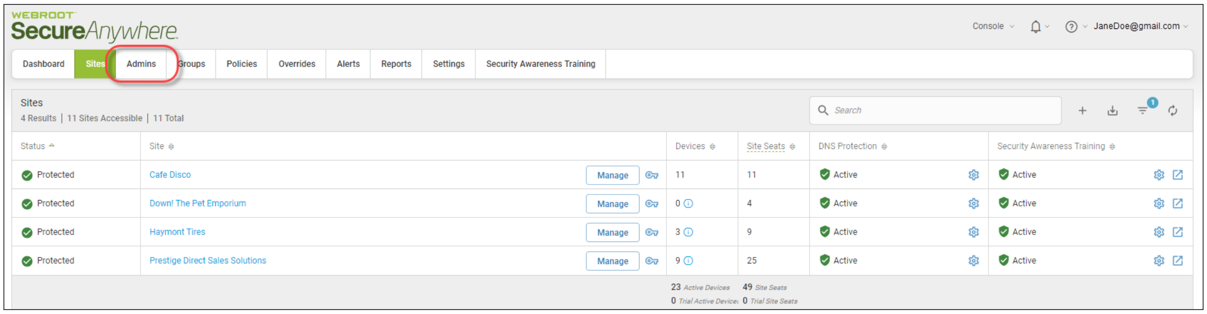
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

2. Click the **Admins** tab.

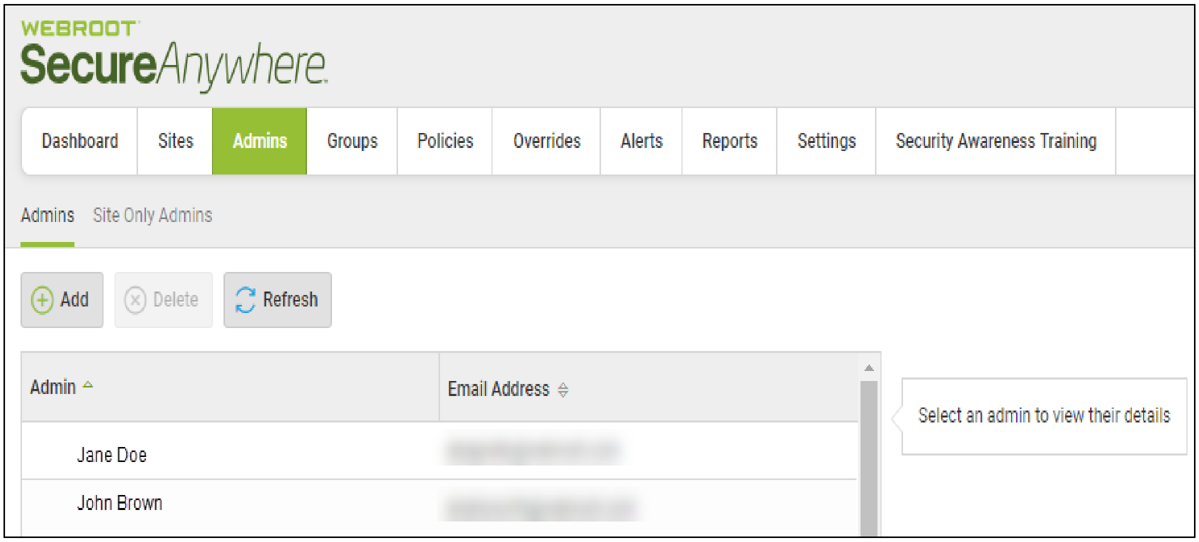


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

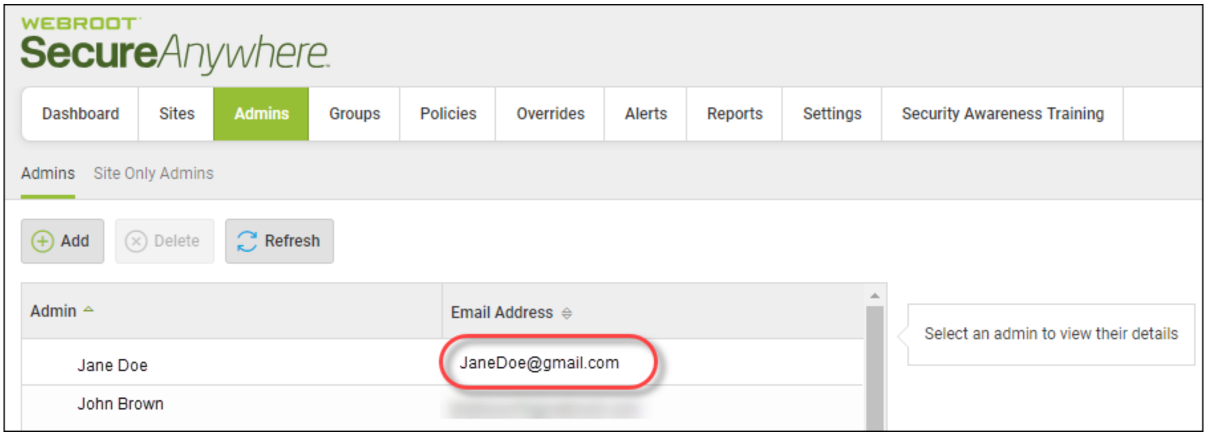
   The system displays the Admins panel with the following information:

- **Name** — The name of the admin.
- **Email** — The email address of the admin.



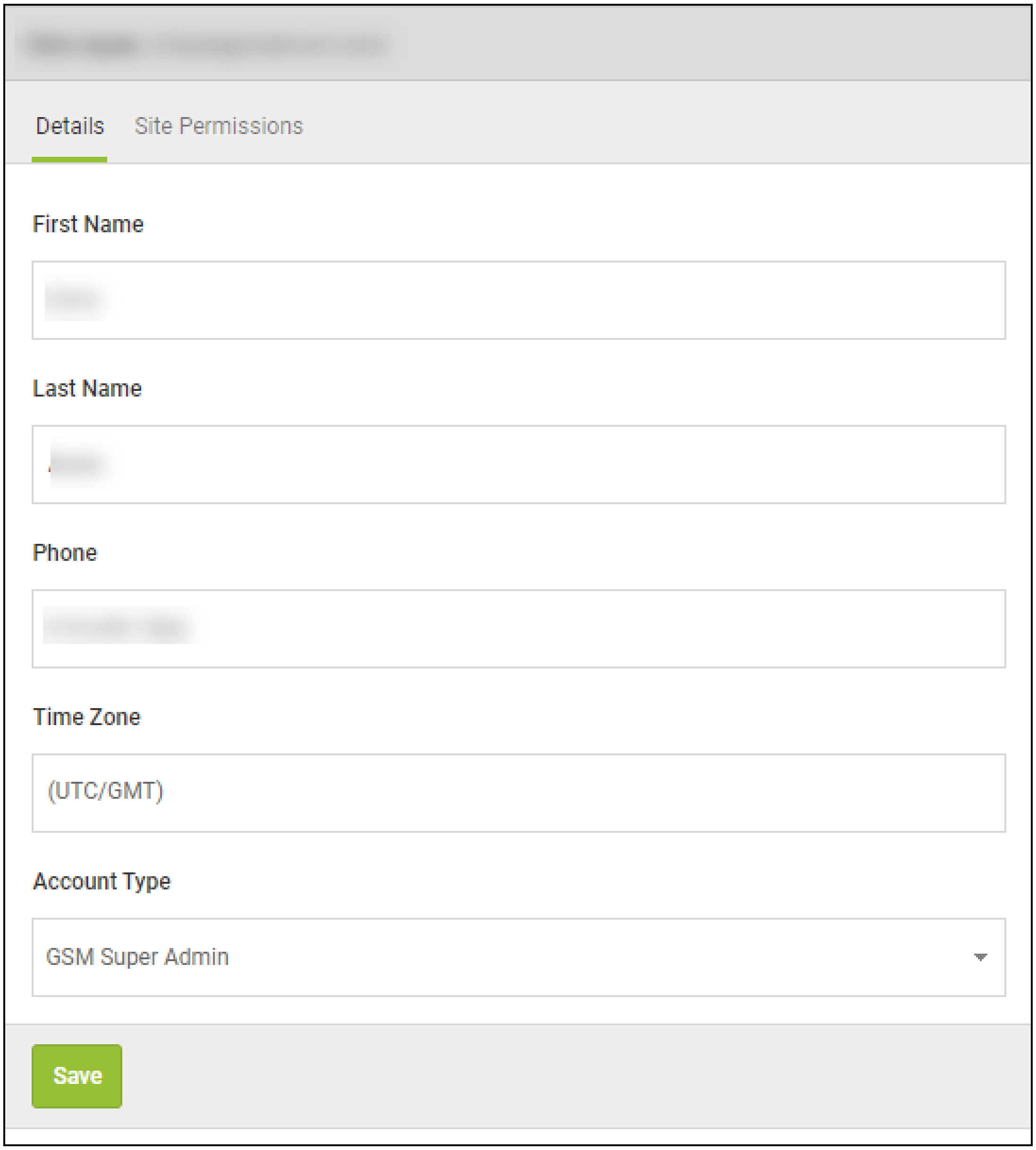
| Admin | Email Address |
|---|---|
| Jane Doe | [redacted] |
| John Brown | [redacted] |

3. Double-click an admin to view additional admin information.



| Admin | Email Address |
|---|---|
| Jane Doe | JaneDoe@gmail.com |
| John Brown | [redacted] |

The system displays admin information with the Details tab active.



[redacted]

First Name

[redacted]

Last Name

[redacted]

Phone

[redacted]

Time Zone

(UTC/GMT)

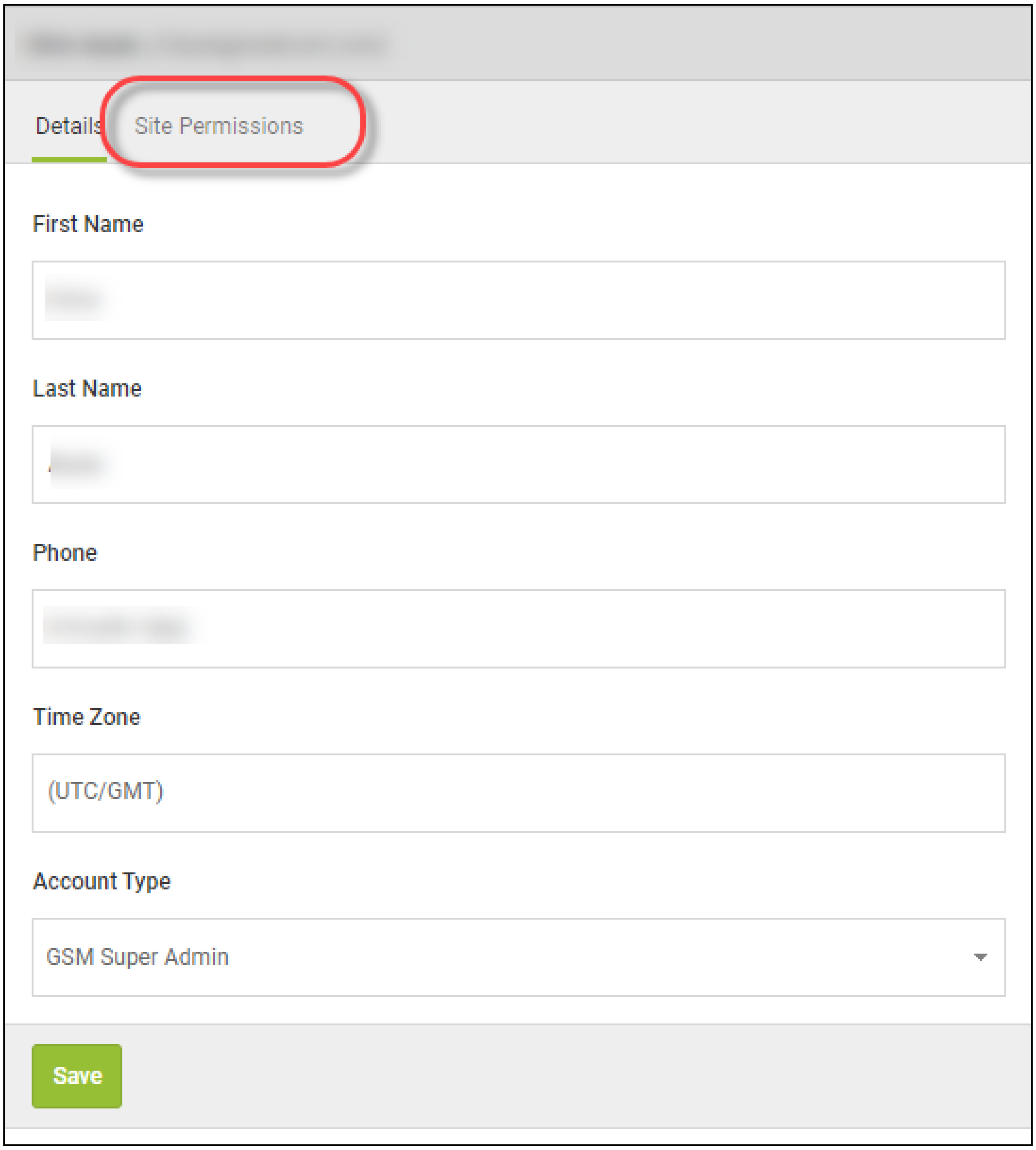
Account Type

GSM Super Admin

4. On the Details panel, you can view and edit the following:
   - **First Name** — The field is editable.
   - **Last Name** — The field is editable.
   - **Phone** — The field is editable.
   - **Time Zone** — Click the pencil icon to edit the information.

- **Account Type** — From the drop-down menu, select one of the following:
  - **GSM Super Admin** — Can access all sites, and add, remove, and edit admins.
  - **GSM Limited Admin** — Can only view sites, but cannot add, remove, or edit admins.
  - **No Access** — Can view the site to which they've been given view permissions.

5. When you are finished viewing and editing information on the Details tab, click the **Site Permissions** tab.



[redacted]

First Name

[redacted]

Last Name

[redacted]

Phone

[redacted]

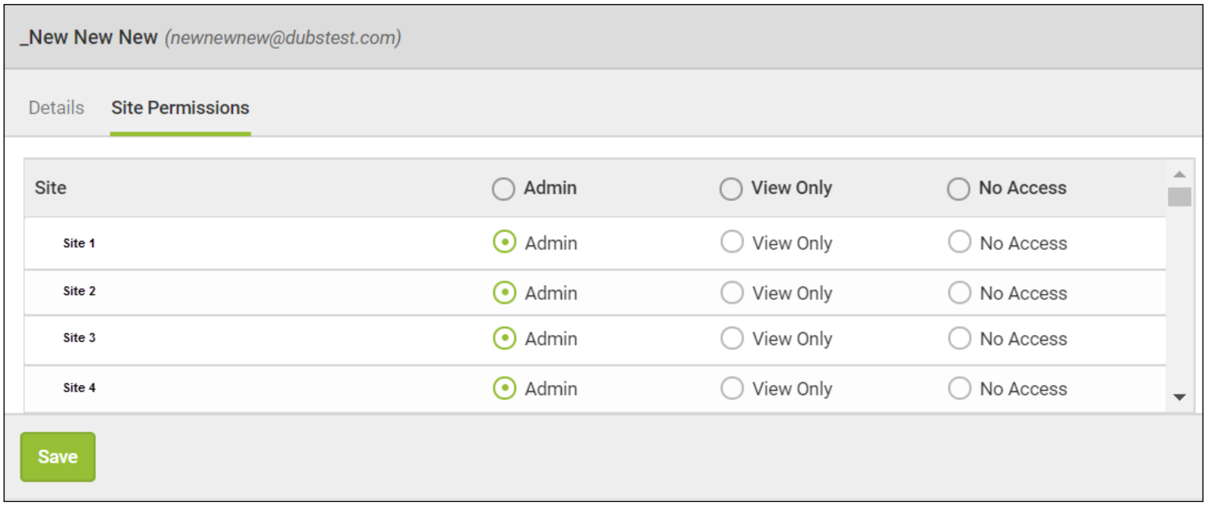
Time Zone

(UTC/GMT)

Account Type

GSM Super Admin

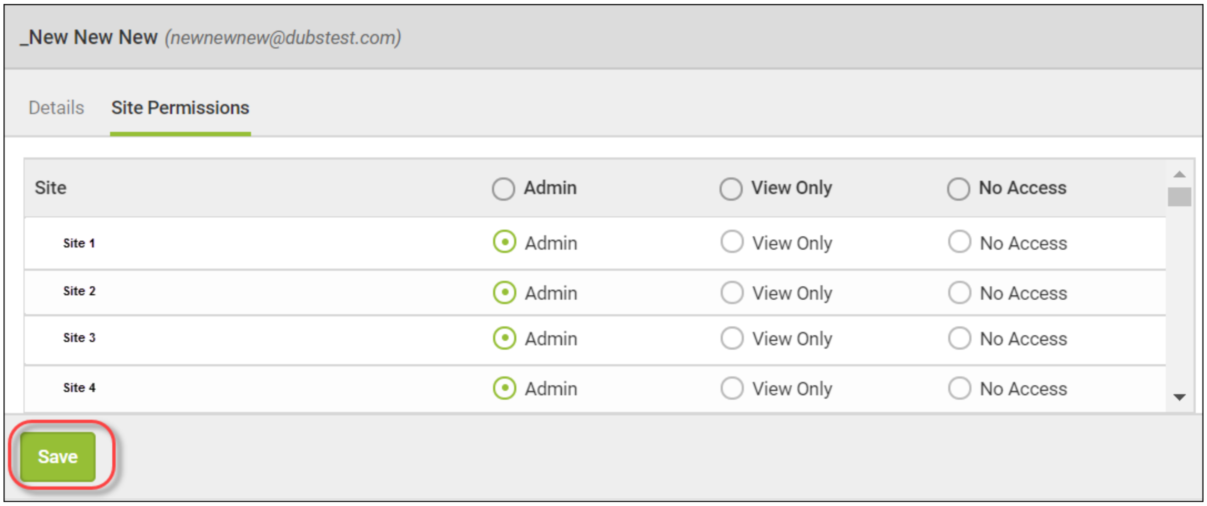
The system displays the Site Permissions tab.



_New New New *(newnewnew@dubstest.com)*

| Site | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| Site 1 | ● Admin | ○ View Only | ○ No Access |
| Site 2 | ● Admin | ○ View Only | ○ No Access |
| Site 3 | ● Admin | ○ View Only | ○ No Access |
| Site 4 | ● Admin | ○ View Only | ○ No Access |

6. For each site, select one of the following permission levels:
   - **Admin**
   - **View Only**
   - **No Access**
7. When you're done, click the **Save** button.



_New New New *(newnewnew@dubstest.com)*

| Site | ○ Admin | ○ View Only | ○ No Access |
|---|---|---|---|
| Site 1 | ● Admin | ○ View Only | ○ No Access |
| Site 2 | ● Admin | ○ View Only | ○ No Access |
| Site 3 | ● Admin | ○ View Only | ○ No Access |
| Site 4 | ● Admin | ○ View Only | ○ No Access |

If you would like more information on changing your account security settings, see *Changing your account security settings on page 166*

# Changing your account security settings

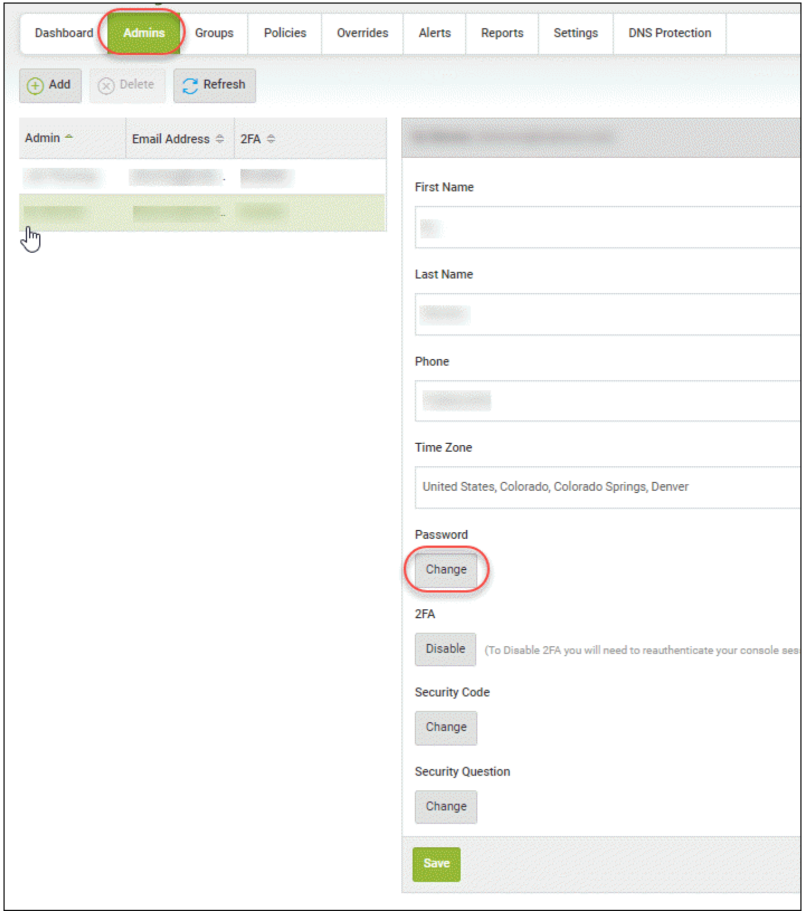
For more help updating general Admin information, see *Updating Admin Information on page 160*.

Refer to the following procedures to learn about changing your account security settings:

- *Changing your password on page 166*
- *Disabling 2-factor authentication (2FA) on page 167*
- *Changing your security code on page 170*
- *Changing your security questions on page 172*

### Changing your password

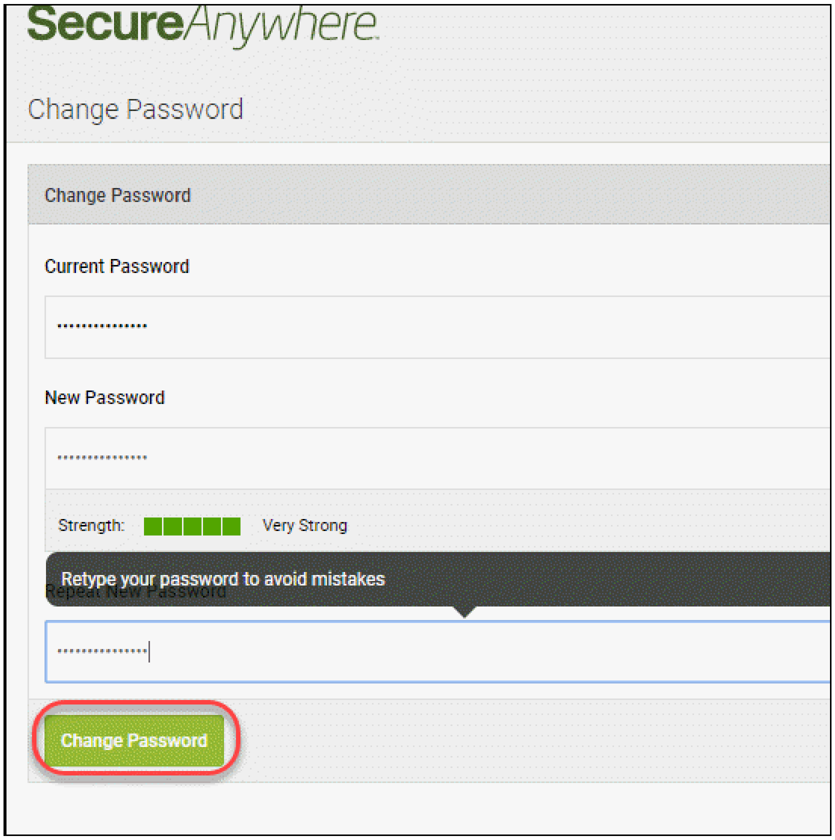
1. Log in to the Management Console, select your Console, and click on the **Admins** tab to view Admin user settings.
2. Click on your user name to display the settings panel, and click **Change** under Password.



Time Zone: United States, Colorado, Colorado Springs, Denver

(To Disable 2FA you will need to reauthenticate your console ses

3. Enter your current password, a new password, and then click **Change Password.**



Current Password

••••••••••••••••

New Password

••••••••••••••••

Strength: 🟩🟩🟩🟩🟩 Very Strong

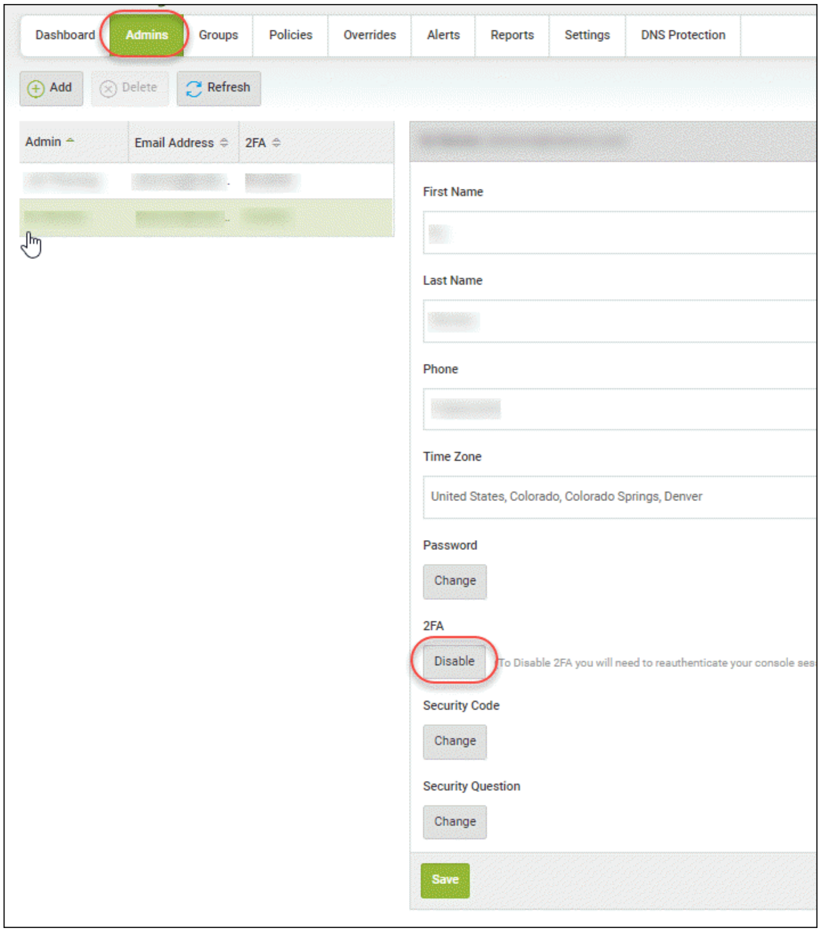
Retype your password to avoid mistakes

Repeat New Password

••••••••••••••••

## Disabling 2-factor authentication (2FA)

1. Log in to the Management Console, and click on the **Admins** tab to view your Admin user settings.
2. Click on your admin account to display the settings panel, and then click **Disable** under 2FA.



First Name [redacted]

Last Name [redacted]

Phone [redacted]

Time Zone: United States, Colorado, Colorado Springs, Denver

Password

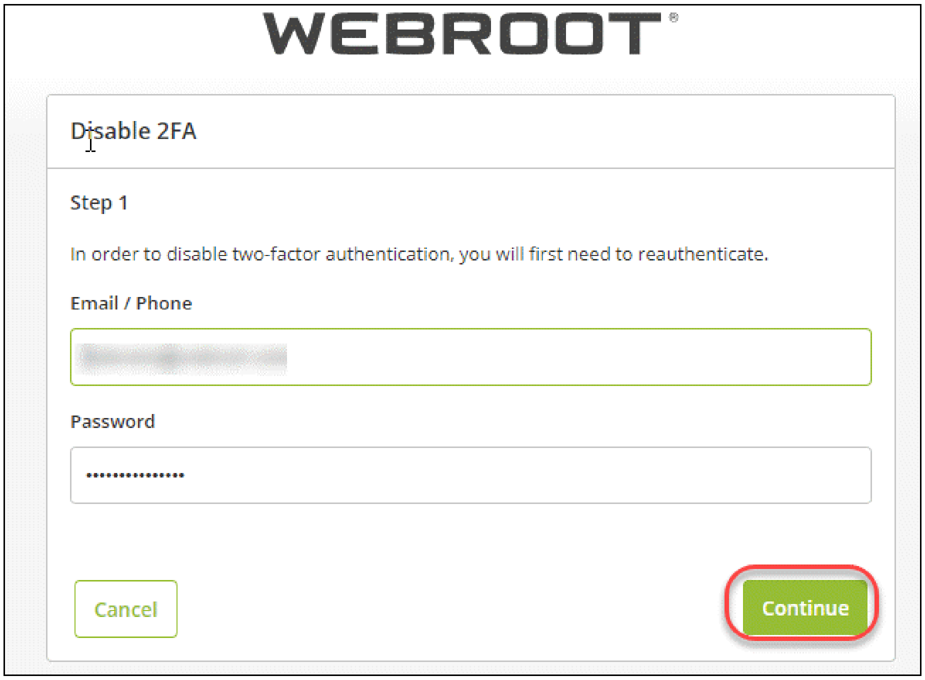
2FA

To Disable 2FA you will need to reauthenticate your console ses

Security Code

Security Question

3. The Disable 2FA screen displays, and you will need to enter your Email / Phone and your Password, and then click **Continue**.



Disable 2FA

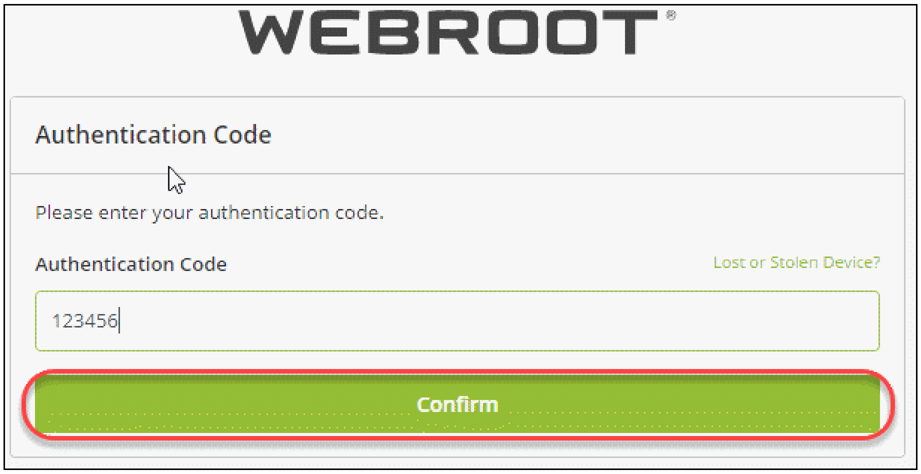
Step 1

In order to disable two-factor authentication, you will first need to reauthenticate.

Email / Phone: [redacted]

Password: •••••••••••••••

4. Open your mobile authenticator app, enter the code displayed there into the Authentication Code box, and then click **Confirm**.

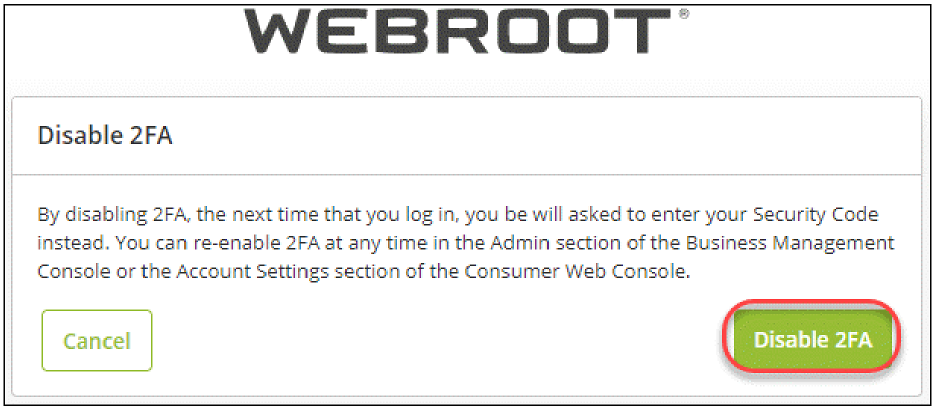


Authentication Code

Please enter your authentication code.

Authentication Code: 123456

5. Click **Disable 2FA**.

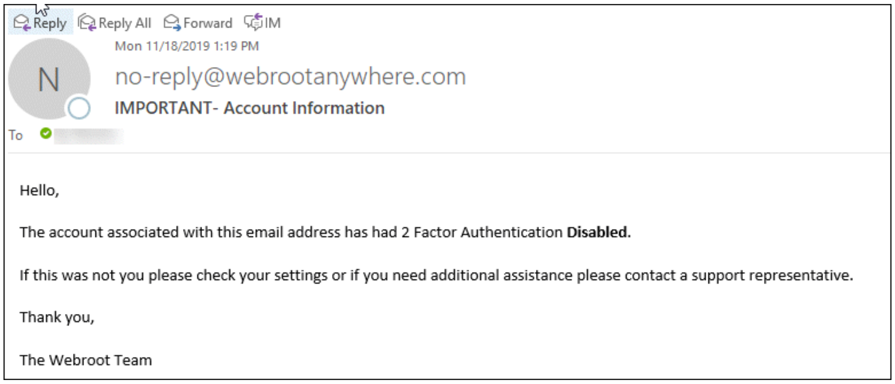


Disable 2FA

By disabling 2FA, the next time that you log in, you be will asked to enter your Security Code instead. You can re-enable 2FA at any time in the Admin section of the Business Management Console or the Account Settings section of the Consumer Web Console.

**Note:** If you disable 2FA, you will be required to enter the Security Code you created when you registered your account. You can re-enable 2FA at any time from the Admins tab of the Console. See *Enabling two-factor authentication (2FA) on page 5* for more information.

6. 2FA is now disabled. You will receive an email confirmation that 2FA has been disabled on your account.



Mon 11/18/2019 1:19 PM

no-reply@webrootanywhere.com

IMPORTANT- Account Information

To [redacted]

Hello,

The account associated with this email address has had 2 Factor Authentication **Disabled.**

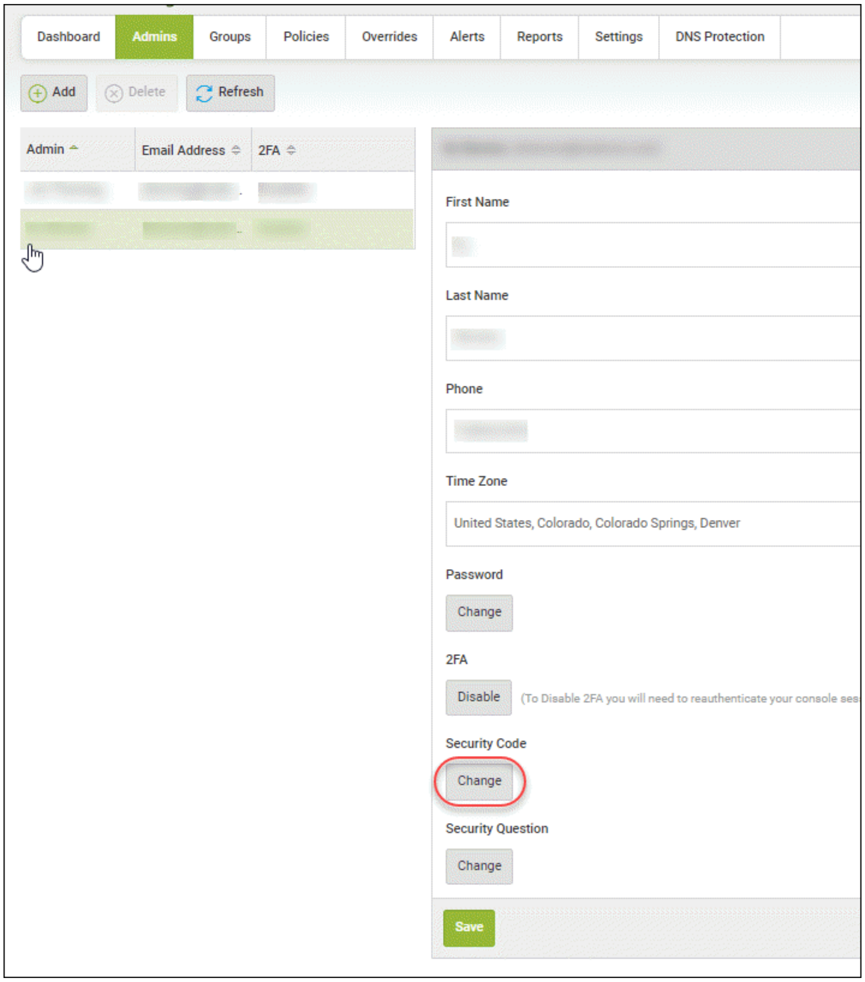
If this was not you please check your settings or if you need additional assistance please contact a support representative.

Thank you,

The Webroot Team

### Changing your security code

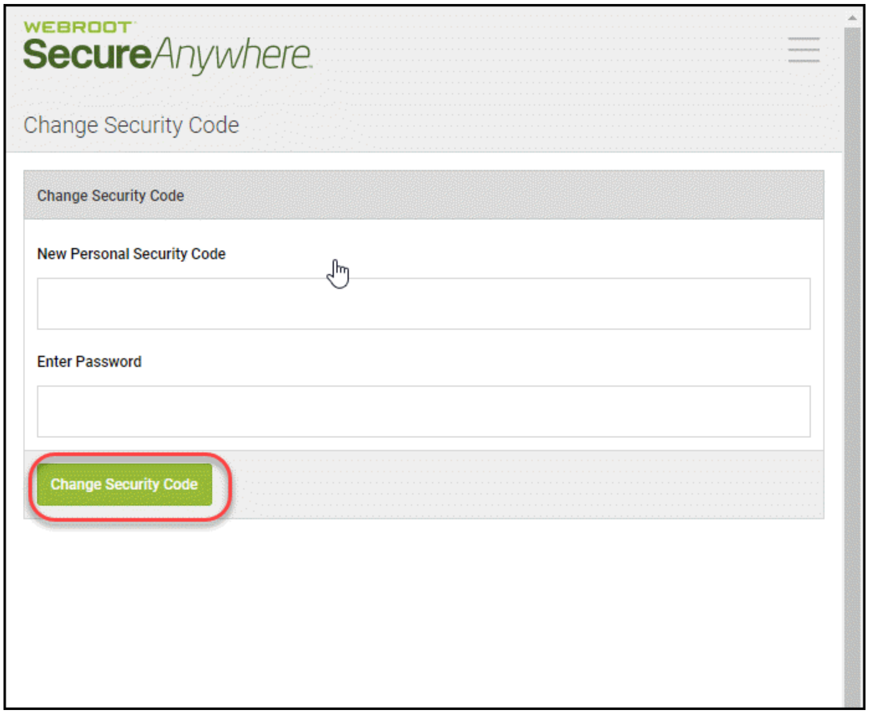
1. Log in to the Management Console, and click on the **Admins** tab.
2. Click on your admin account to display the settings panel, and then click **Change** under Security Code.



Time Zone: United States, Colorado, Colorado Springs, Denver

(To Disable 2FA you will need to reauthenticate your console ses

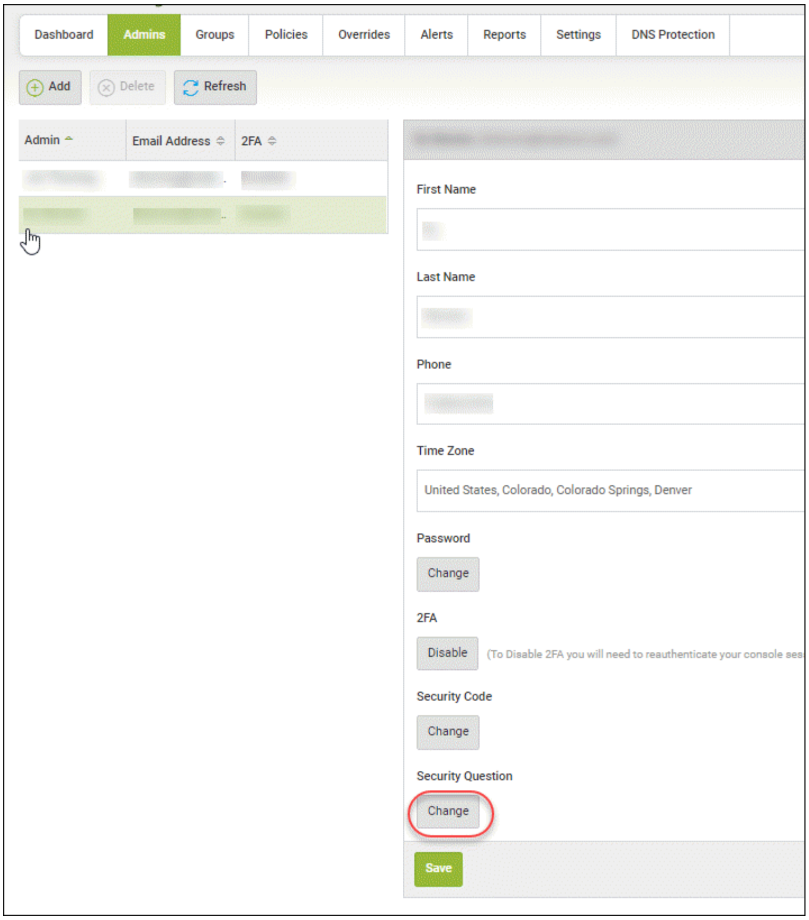
3. Enter a new security code you would like to use as well as your password, and click **Change Security Code**.



### Changing your security questions

1. Log in to the Management Console, and click on the **Admins** tab.

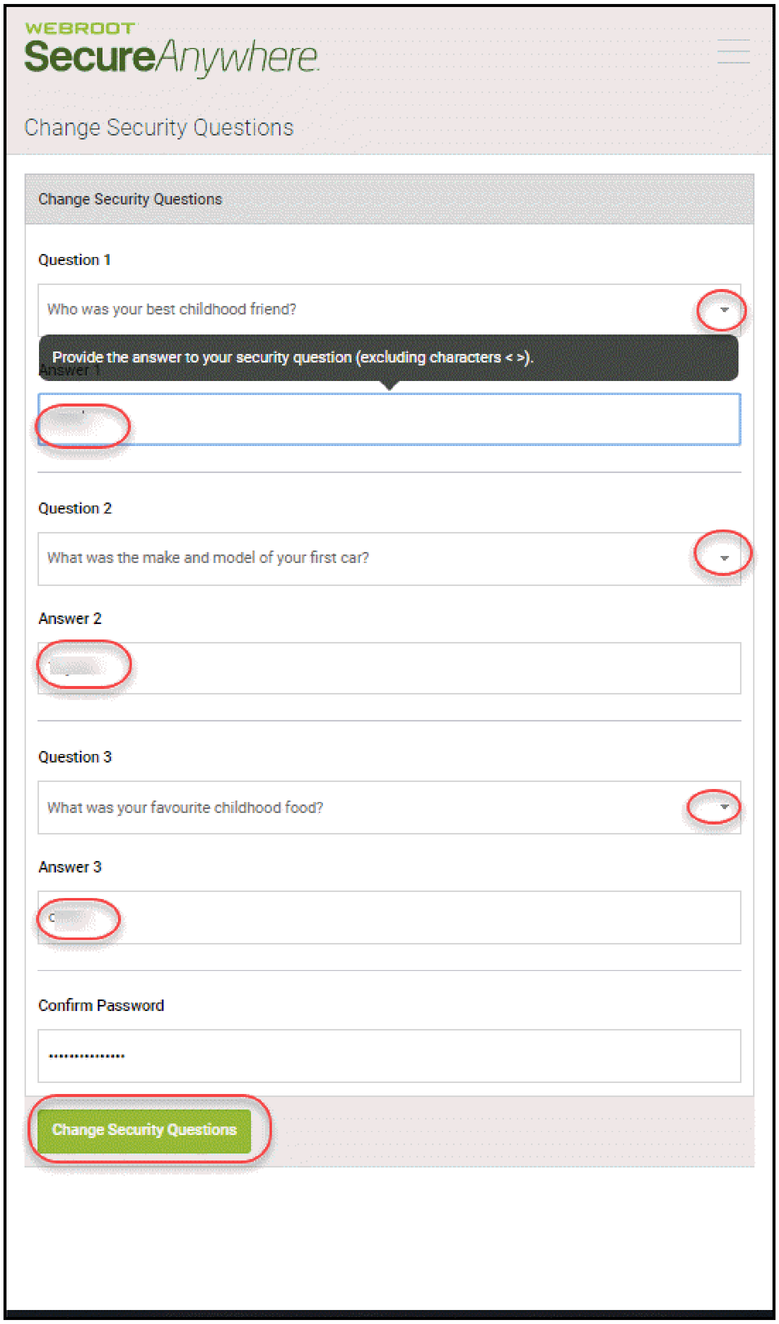
2. Click on your admin account to display the settings panel, and then click **Change** under Security Question.



Time Zone: United States, Colorado, Colorado Springs, Denver

(To Disable 2FA you will need to reauthenticate your console ses

3. Select your desired security questions from each of the drop-down menus and enter your answers in each of the applicable boxes, and then click **Change Security Questions**.



WEBROOT SecureAnywhere

Change Security Questions

Change Security Questions

Question 1

Who was your best childhood friend?

Provide the answer to your security question (excluding characters < >).

Answer 1

Question 2

What was the make and model of your first car?

Answer 2

Question 3

What was your favourite childhood food?

Answer 3

Confirm Password

••••••••••••••••

Change Security Questions

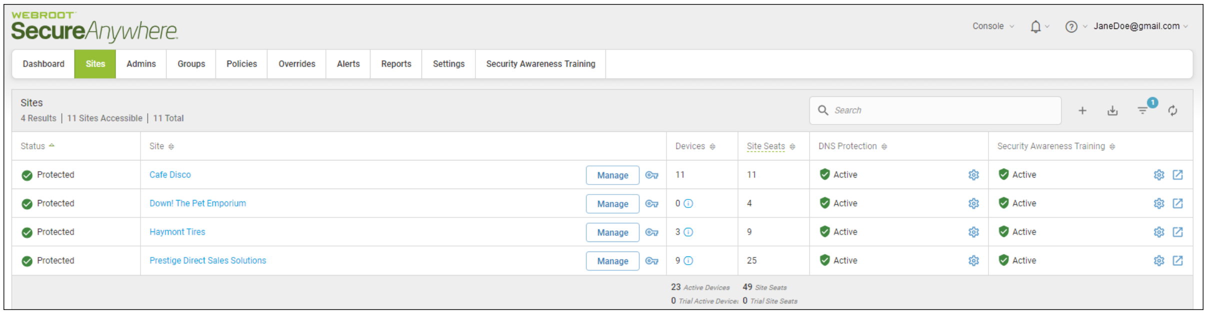
# Deleting Admins

Follow this procedure to delete admins from the system.

**To delete an admin:**

1. Log in to the management console.

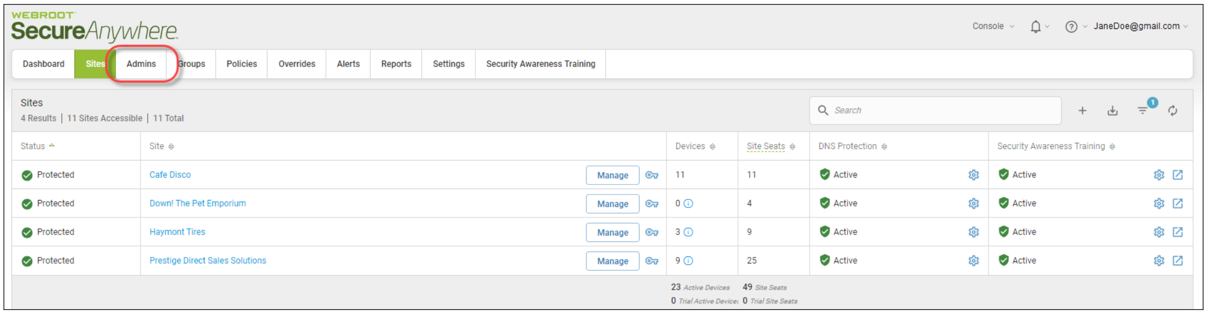
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

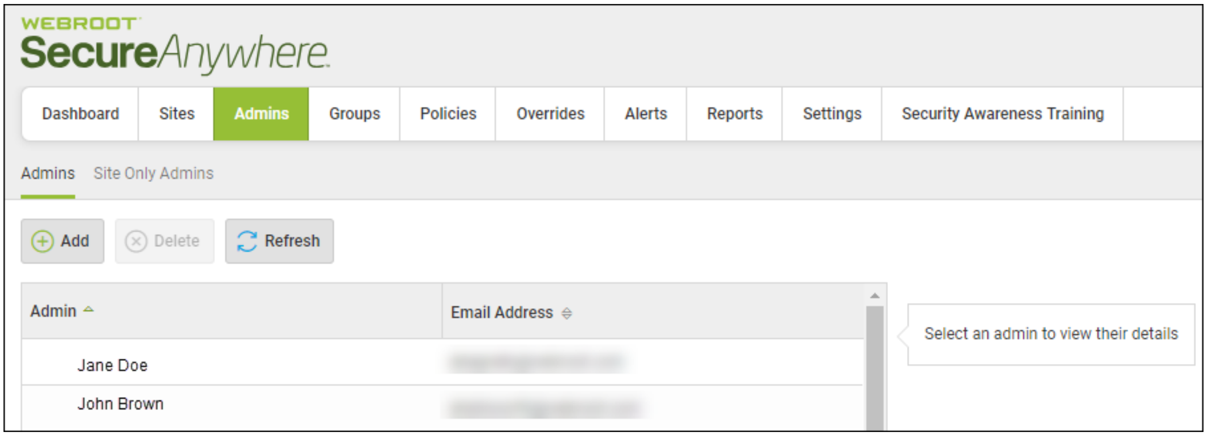
2. Click the **Admins** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

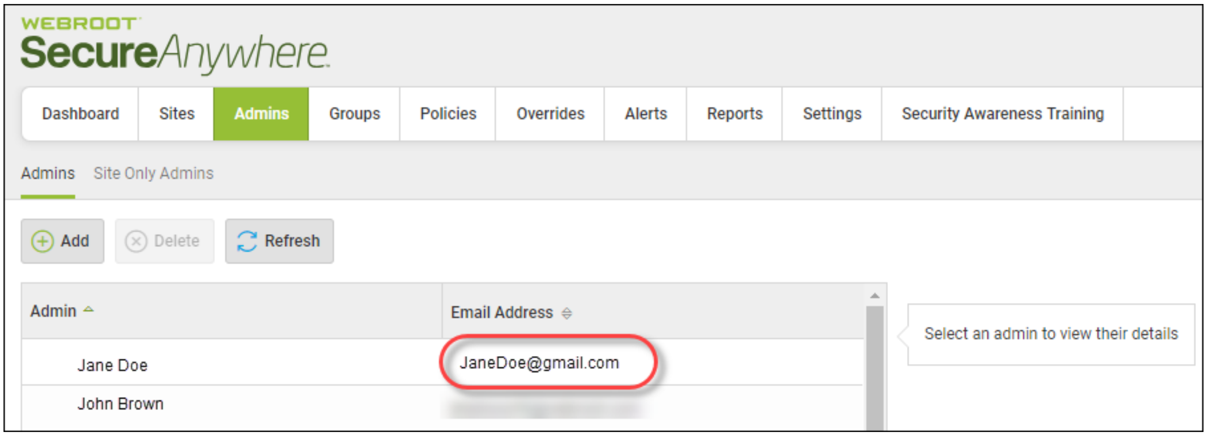
The system displays the Admins tab.



| Admin | Email Address |
|---|---|
| Jane Doe | [redacted] |
| John Brown | [redacted] |

Select an admin to view their details

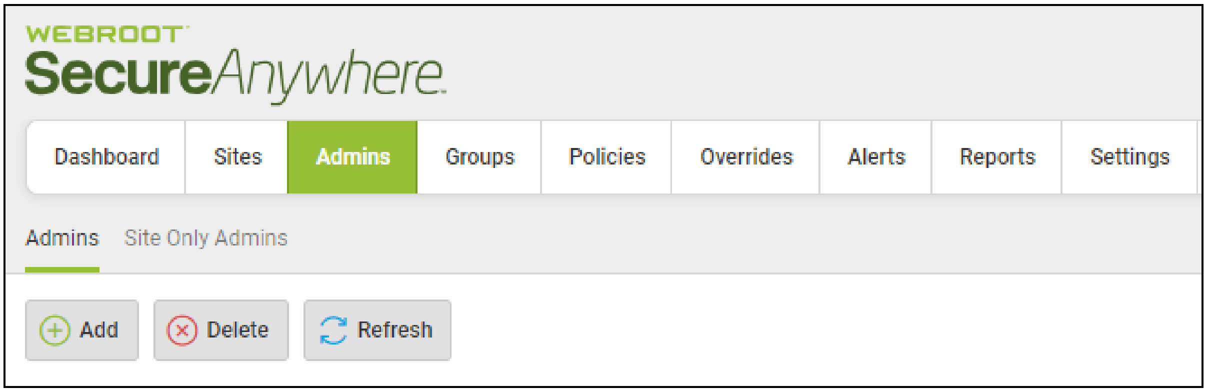
3. Double-click an admin's email address to view their details.



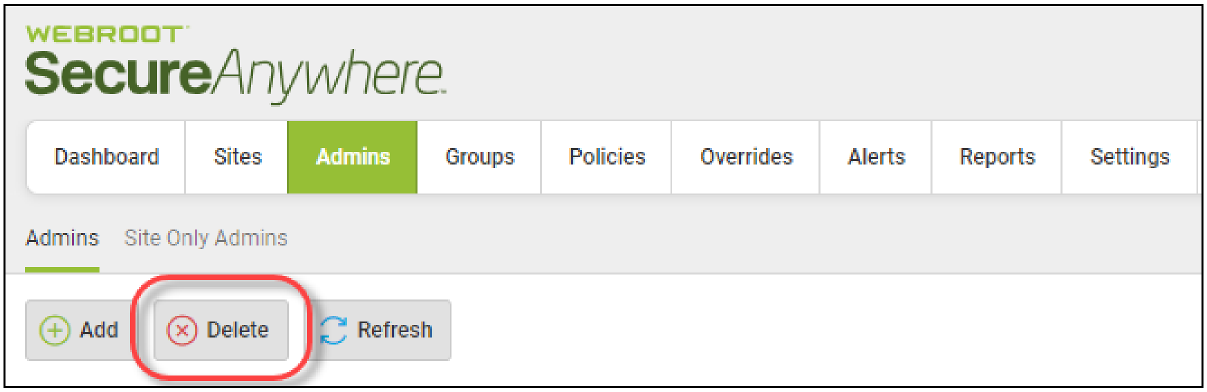
| Admin | Email Address |
|---|---|
| Jane Doe | JaneDoe@gmail.com |
| John Brown | [redacted] |

Select an admin to view their details

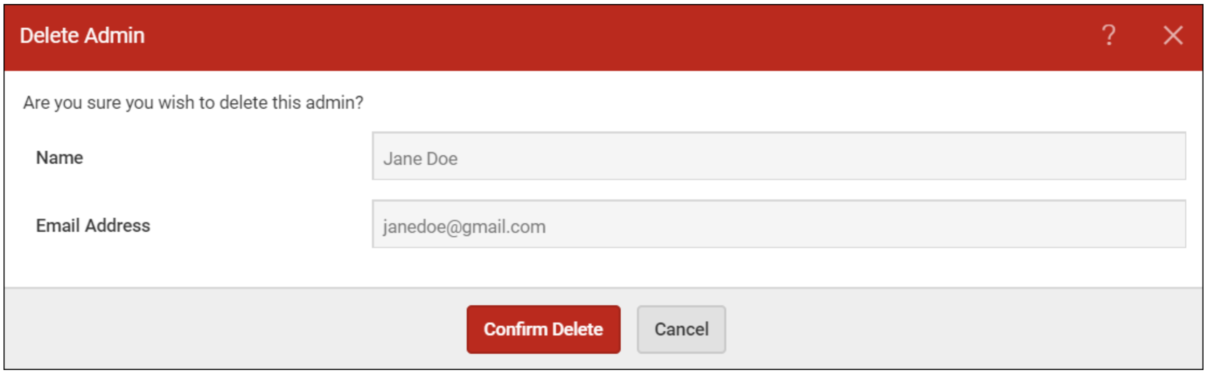
The admin's details display, and the Delete button becomes active.



4. Click the **Delete** button.



The system displays a warning message.



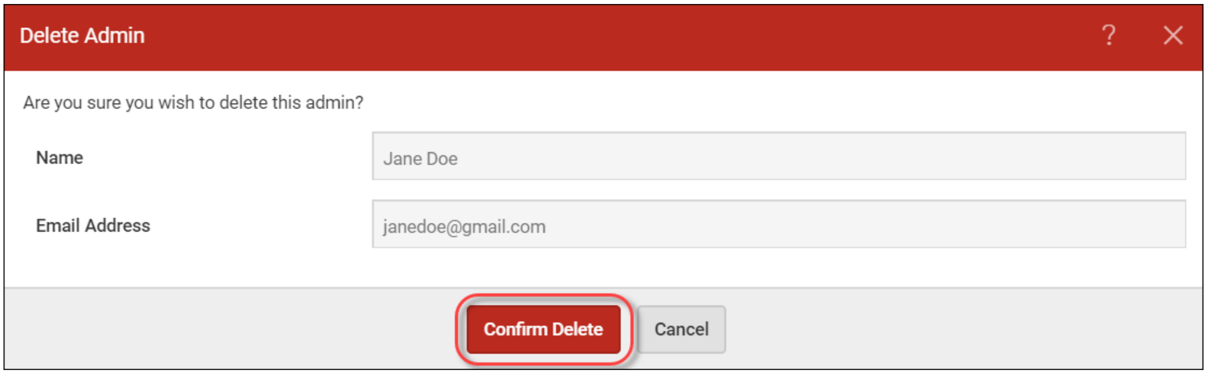
Delete Admin

Are you sure you wish to delete this admin?

Name: Jane Doe

Email Address: janedoe@gmail.com

5. Click the **Confirm Delete** button.



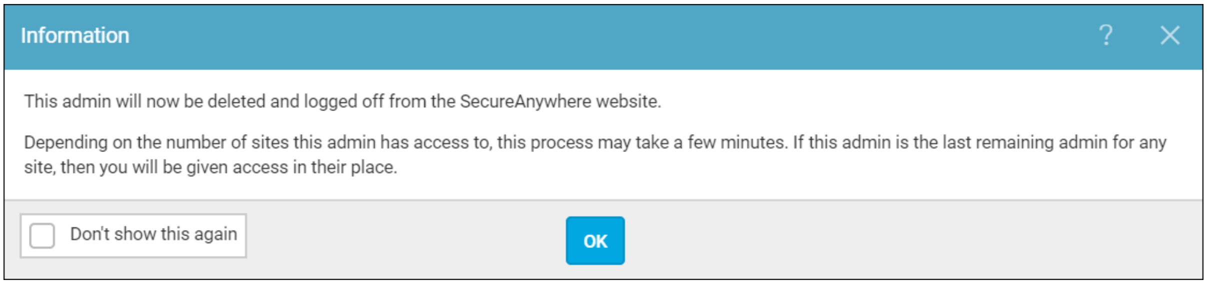
Delete Admin

Are you sure you wish to delete this admin?

Name: Jane Doe

Email Address: janedoe@gmail.com

The system displays an information message.

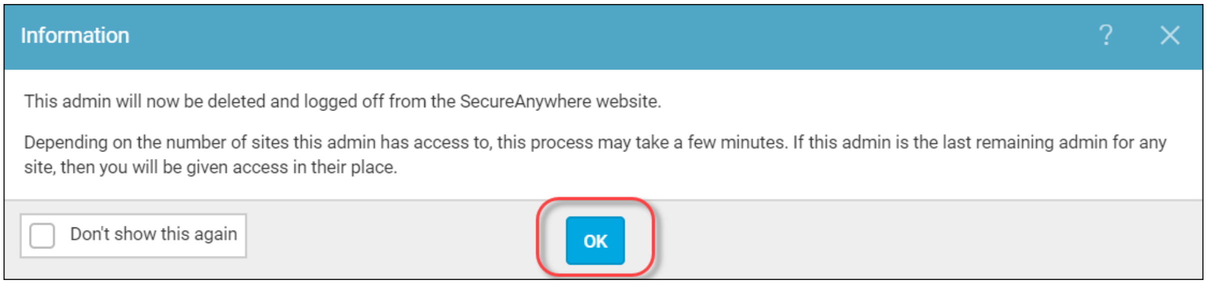


Information

This admin will now be deleted and logged off from the SecureAnywhere website.

Depending on the number of sites this admin has access to, this process may take a few minutes. If this admin is the last remaining admin for any site, then you will be given access in their place.

6. Click the **OK** button.



Information

This admin will now be deleted and logged off from the SecureAnywhere website.

Depending on the number of sites this admin has access to, this process may take a few minutes. If this admin is the last remaining admin for any site, then you will be given access in their place.

The admin is now deleted from the system.

# About Management Console Admin Permissions

The following tables describe various admin permissions for both the management console and the Endpoint Protection consoles.

- Management Console Platform - Management Console Access
- Management Console Platform - Endpoint Protection Console Access
- SecureAnywhere Platform - Admin Level - Endpoint Protection
- SecureAnywhere Platform - Basic Level - Endpoint Protection
- SecureAnywhere Platform - No Access Level - Endpoint Protection

**Note:** Admin permissions marked with an asterisk (*) are configurable.

## Management Console Platform - Management Console Access

| Super Admin | Limited Admin | Site Only |
|---|---|---|
| Dashboard - Yes | Dashboard - Yes | Dashboard - No Access |
| Sites Page - Yes* | Sites Page - Yes* | Sites Page - No Access |
| Admins - Yes | Admins - View Only | Admins - No Access |
| Groups - Yes | Groups - Yes | Groups - No Access |
| Policies - Yes | Policies - No | Policies - No Access |

| **Super Admin** | **Limited Admin** | **Site Only** |
|---|---|---|
| Overrides - Yes | Overrides - No | Overrides - No Access |
| Alerts - Yes | Alerts - No | Alerts - No Access |
| Commands - N/A | Commands - N/A | Commands - No Access |
| Reports - Yes | Reports - Yes | Reports - No Access |
| DNS - Yes | DNS - Yes | DNS - No |
| WSAT - Yes | WSAT - Yes | WSAT - Yes |
| Settings - Yes | Settings - No | Settings - No Access |
| Logs - N/A | Logs - N/A | Logs - No Access |
| Resources - N/A | Resources - N/A | Resources - No Access |
| Downloads - Yes | Downloads - Yes | Downloads - No Access |

## Management Console Platform - Endpoint Protection Console Access

| Super Admin | Limited Admin | Site Only |
|---|---|---|
| Dashboard - Yes | Dashboard - Yes | Dashboard - Yes |
| Sites Page - Yes* | Sites Page - Yes* | Sites Page - N/A |
| Admins - Yes | Admins - Yes | Admins - Yes |
| Groups - Yes* | Groups - Yes* | Groups - Yes* |
| Policies - Yes* | Policies - Yes* | Policies - Yes* |
| Overrides - Yes* | Overrides - Yes* | Overrides - Yes* |
| Alerts - Yes* | Alerts - Yes* | Alerts - Yes* |
| Commands - Yes* | Commands - Yes* | Commands - Yes* |
| Reports - Yes | Reports - Yes | Reports - Yes |
| DNS - No | DNS - No | DNS - No |
| WSAT - Yes | WSAT - Yes | WSAT - Yes |
| Settings - Yes | Settings - Yes | Settings - Yes |

| Super Admin | Limited Admin | Site Only |
|---|---|---|
| Logs - Yes | Logs - Yes | Logs - Yes |
| Resources - Yes | Resources - Yes | Resources - Yes |
| Downloads - Yes | Downloads - Yes | Downloads - Yes |

## SecureAnywhere Platform - Admin Level - Endpoint Protection

| Admin | Basic | No Access |
|---|---|---|
| Status - Yes | Status - Yes | Status - Yes |
| Admins - Yes | Admins - Yes | Admins - Yes |
| Groups - Yes* | Groups - View Only | Groups - No |
| Policies - Yes* | Policies - View Only | Policies - No |
| Overrides - Yes* | Overrides - No | Overrides - No |
| Alerts - Yes* | Alerts - No | Alerts - No |
| Commands - Yes* | Commands - No | Commands - No |
| Reports - Yes | Reports - Yes | Reports - No |

| Admin | Basic | No Access |
|---|---|---|
| DNS - No | DNS - No | DNS - No |
| WSAT - Yes | WSAT - Yes | WSAT - No |
| Settings - Yes | Settings - View Only | Settings - No |
| Logs - Yes | Logs - Yes | Logs - No |
| Resources - Yes | Resources - Yes | Resources - No |
| Downloads - Yes | Downloads - Yes | Downloads - Yes |

## SecureAnywhere Platform - Basic Level - Endpoint Protection

| Admin | Basic | No Access |
|---|---|---|
| Status - Yes | Status | Status - No |
| Admins - No | Admins - No | Admins - No |
| Groups - Yes* | Groups - View Only | Groups - No |
| Policies - Yes* | Policies - View Only | Policies - No |
| Overrides - Yes* | Overrides - No | Overrides - No |

| Admin | Basic | No Access |
|---|---|---|
| Alerts - Yes* | Alerts - No | Alerts - No |
| Commands - Yes* | Commands - No | Commands - No |
| Reports - Yes | Reports - Yes | Reports - No |
| DNS - No | DNS - No | DNS - No |
| WSAT - Yes | WSAT - No | WSAT - No |
| Settings - Yes | Settings - View Only | Settings - No |
| Logs - Yes | Logs - Yes | Logs - No |
| Resources - Yes | Resources - Yes | Resources - No |
| Downloads - Yes | Downloads - Yes | Downloads - No |

## SecureAnywhere Platform - No Access Level - Endpoint Protection

| Admin | Basic | No Access |
|---|---|---|
| Status - No | Status - No | Status - No |
| Admins - No | Admins - No | Admins - No |
| Groups - No | Groups - No | Groups - No |
| Policies - No | Policies - No | Policies - No |
| Overrides - No | Overrides - No | Overrides - No |
| Alerts - No | Alerts - No | Alerts - No |
| Commands - No | Commands - No | Commands - No |
| Reports - No | Reports - No | Reports - No |
| DNS - No | DNS - No | DNS - No |
| WSAT - No | WSAT - No | WSAT - No |
| Settings - No | Settings - No | Settings - No |
| Logs - No | Logs - No | Logs - No |

| Admin | Basic | No Access |
|---|---|---|
| Resources - No | Resources - No | Resources - No |
| Downloads - No | Downloads - No | Downloads - No |

# Chapter 5: Working With Groups

To work with groups, see the following topics:

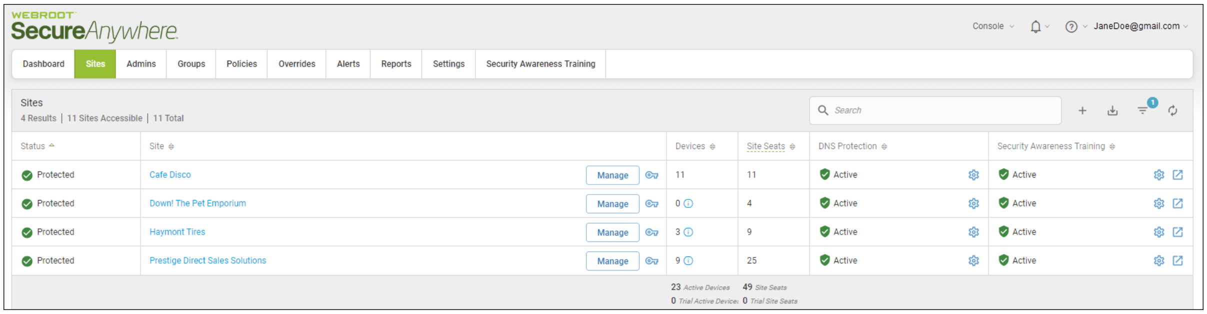
# Adding Groups

When you first deploy to endpoints, the system assigns them to the Default group. If needed, you can add more groups for different management purposes and re-assign endpoints to those new groups.

**To add a group:**

1. Log in to the management console.

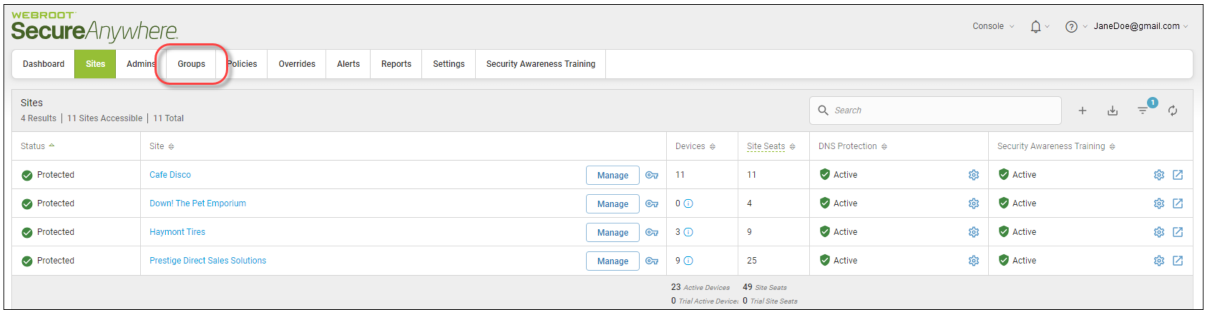
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

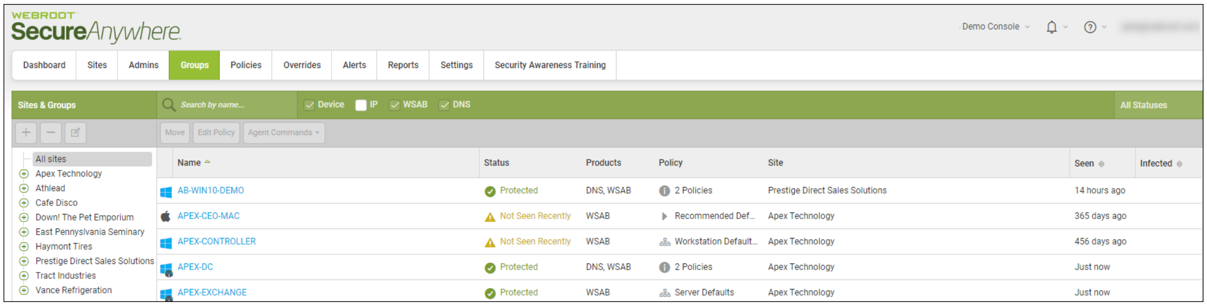
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

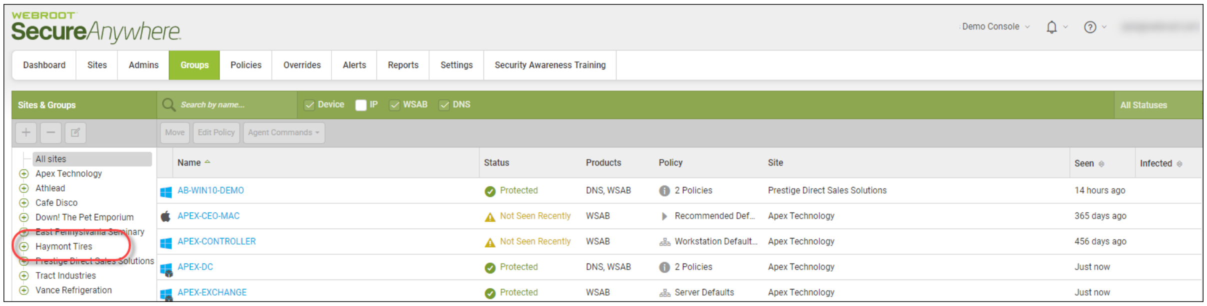
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



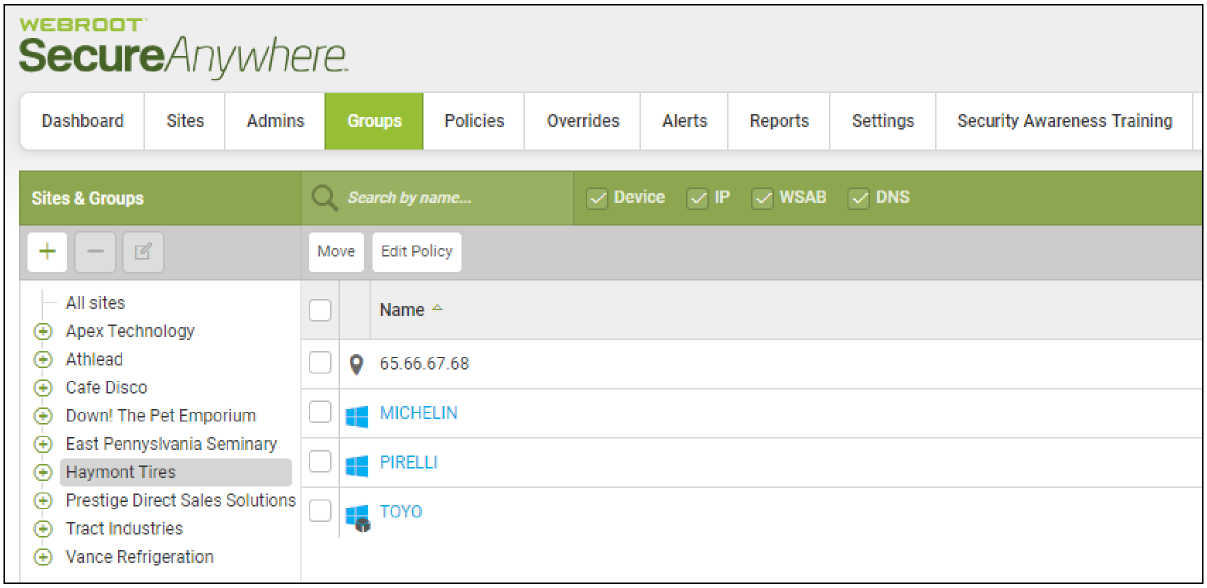
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. In the left column, select a site to which you want to add groups.



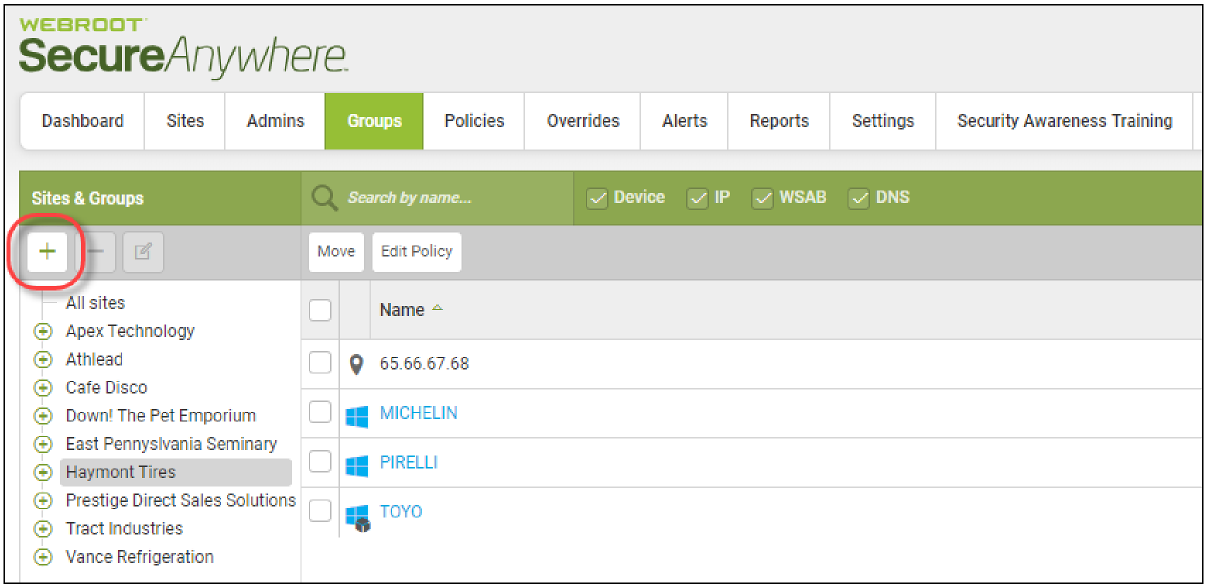
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The Plus (+) button becomes active.



| | Name |
|---|---|
| □ | 65.66.67.68 |
| □ | MICHELIN |
| □ | PIRELLI |
| □ | TOYO |

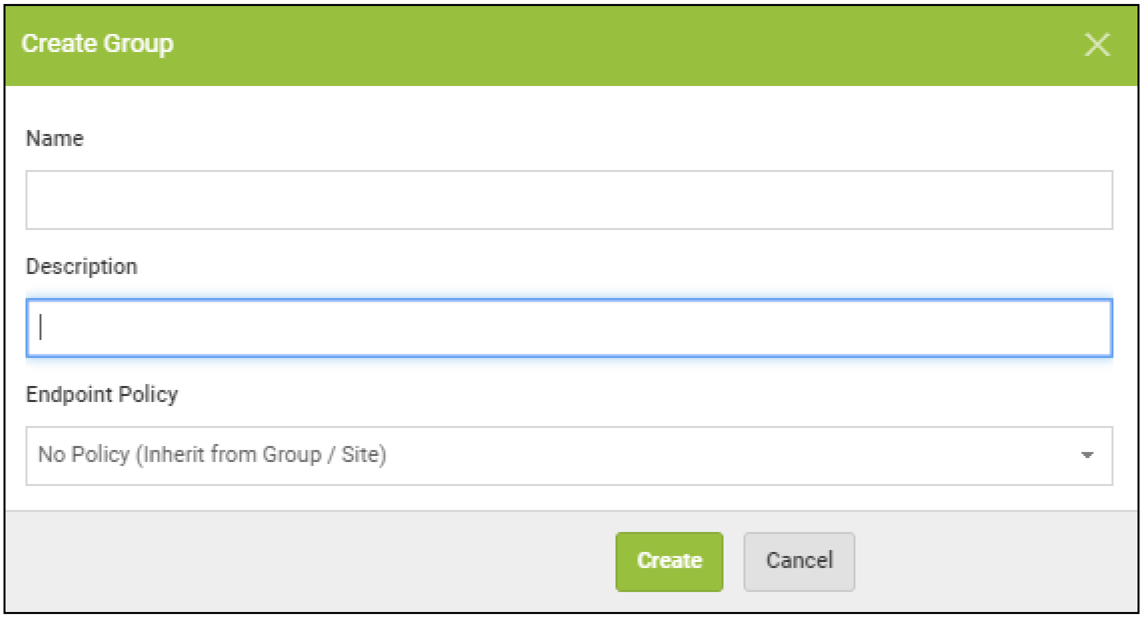
4. Click the **Plus (+)** button.



All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| □ | Name |
|---|---|
| □ | 65.66.67.68 |
| □ | MICHELIN |
| □ | PIRELLI |
| □ | TOYO |

The Create Group window displays.



Create Group

Name:

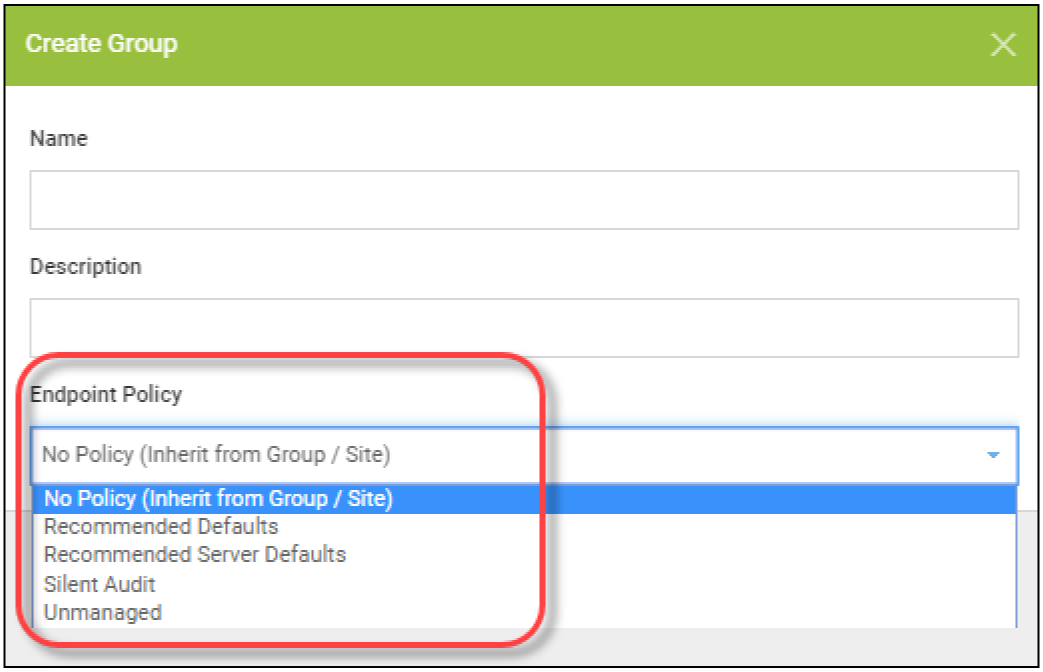
Description:

Endpoint Policy: No Policy (Inherit from Group / Site)

5. In the Name field, enter a name for the group.

6. In the Description field, enter a brief description for the group.

7. From the Endpoint Policy drop-down menu, select one of the following policies:
   - **No Policy**
   - **Recommended Defaults**
   - **Recommended Server Defaults**
   - **Silent Audit**
   - **Unmanaged**


Create Group

Name

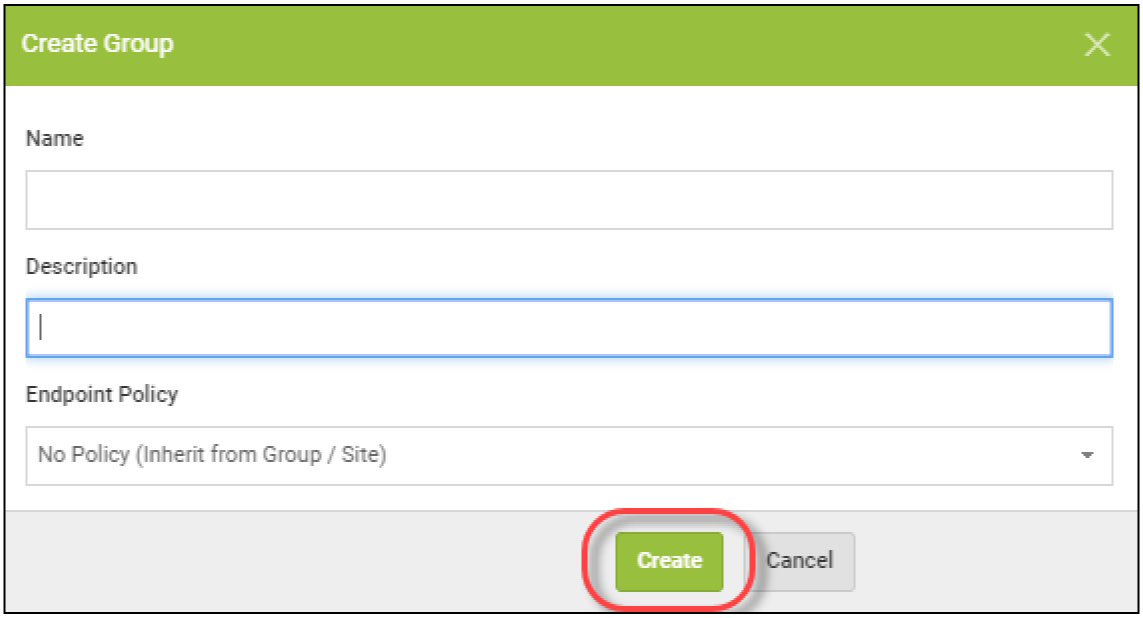
Description

Endpoint Policy

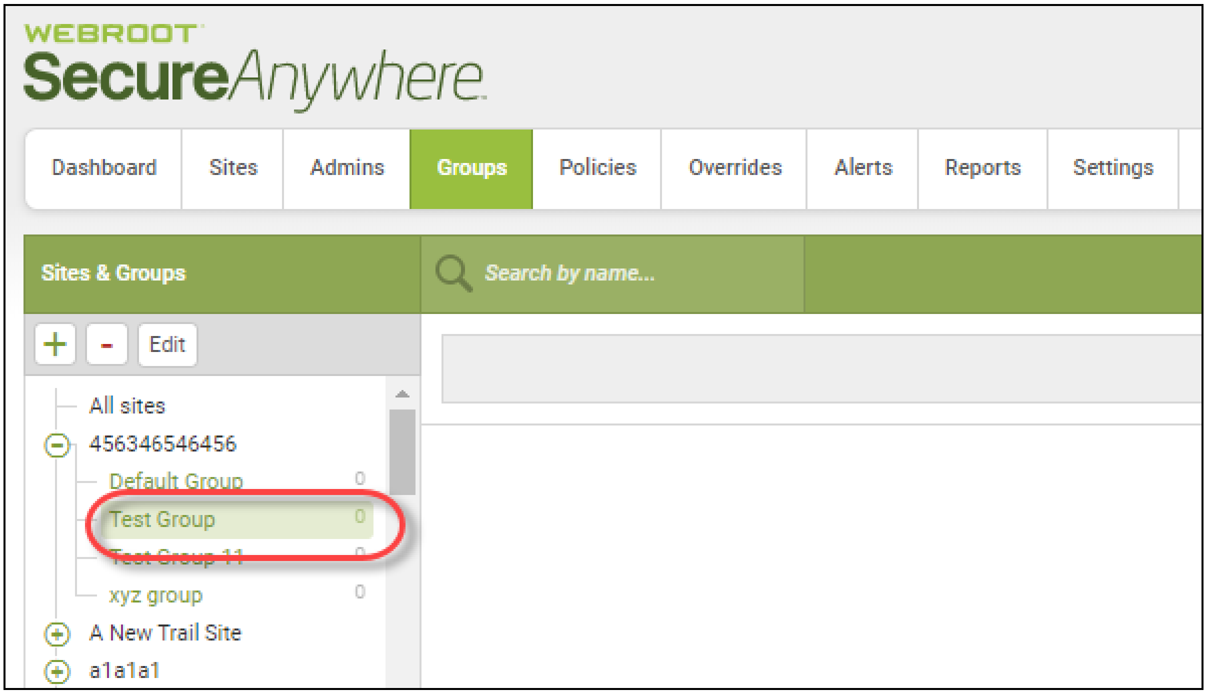
No Policy (Inherit from Group / Site)

No Policy (Inherit from Group / Site)
Recommended Defaults
Recommended Server Defaults
Silent Audit
Unmanaged

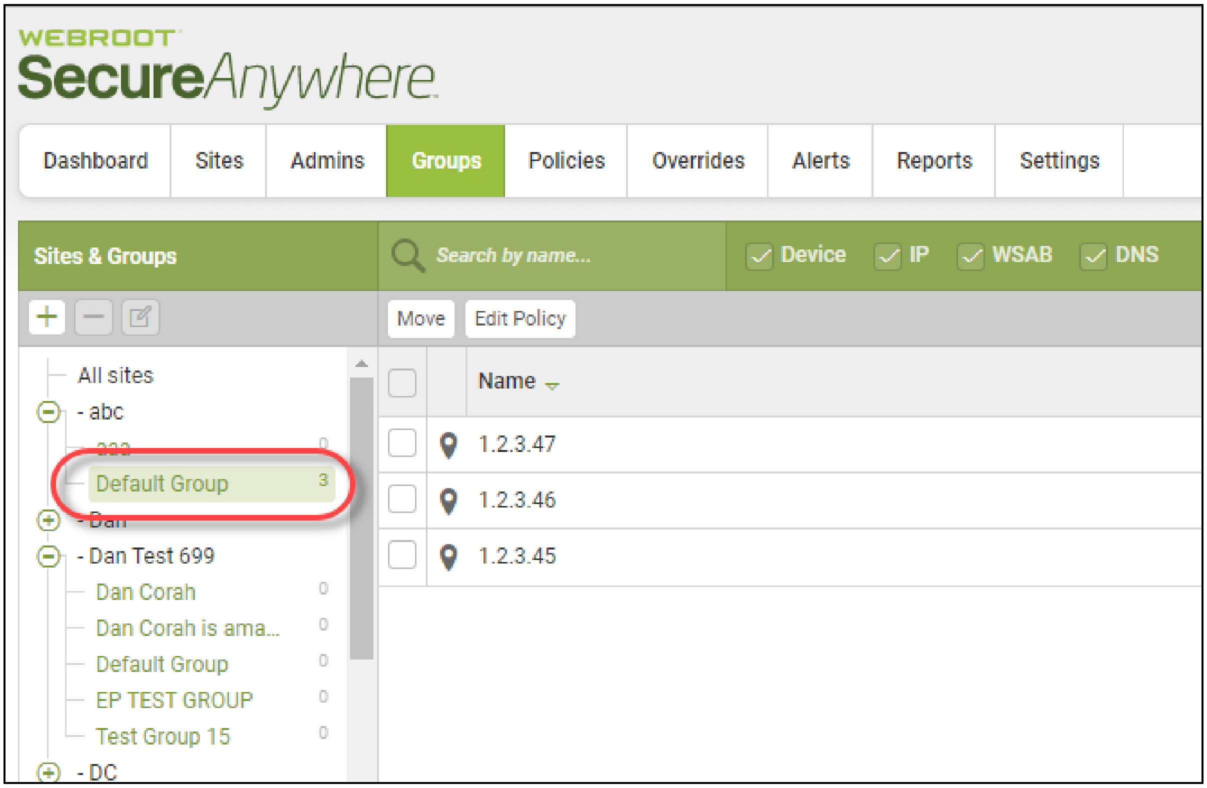
8. Click the **Create** button.



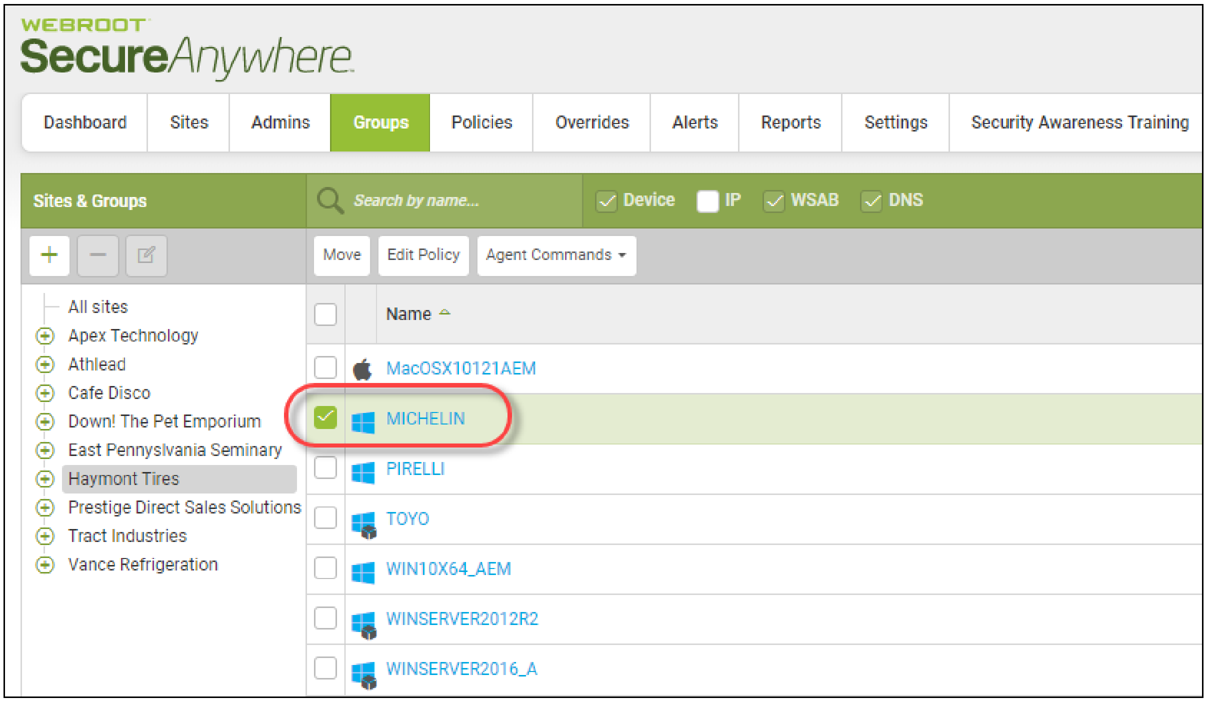
The new group displays in the Groups panel on the left.



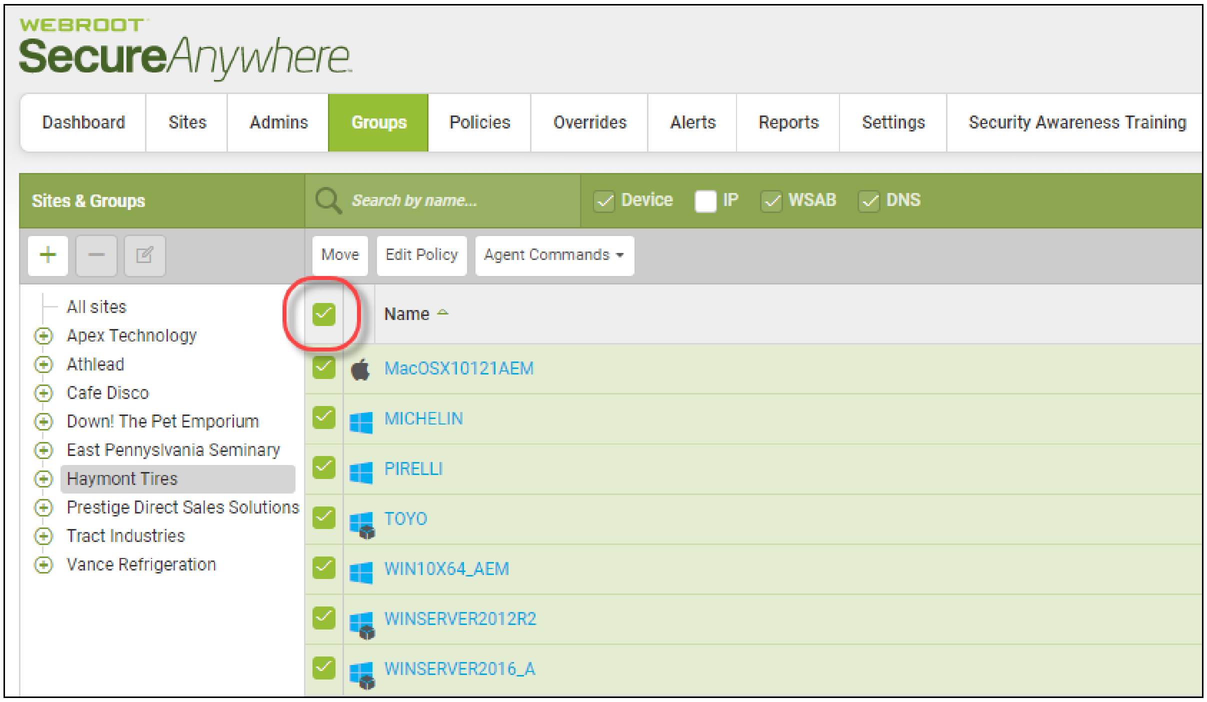
9. To move endpoints into this group, click the group where the endpoints you want to move currently reside.



10. Select one or more endpoints from the Devices panel on the right.



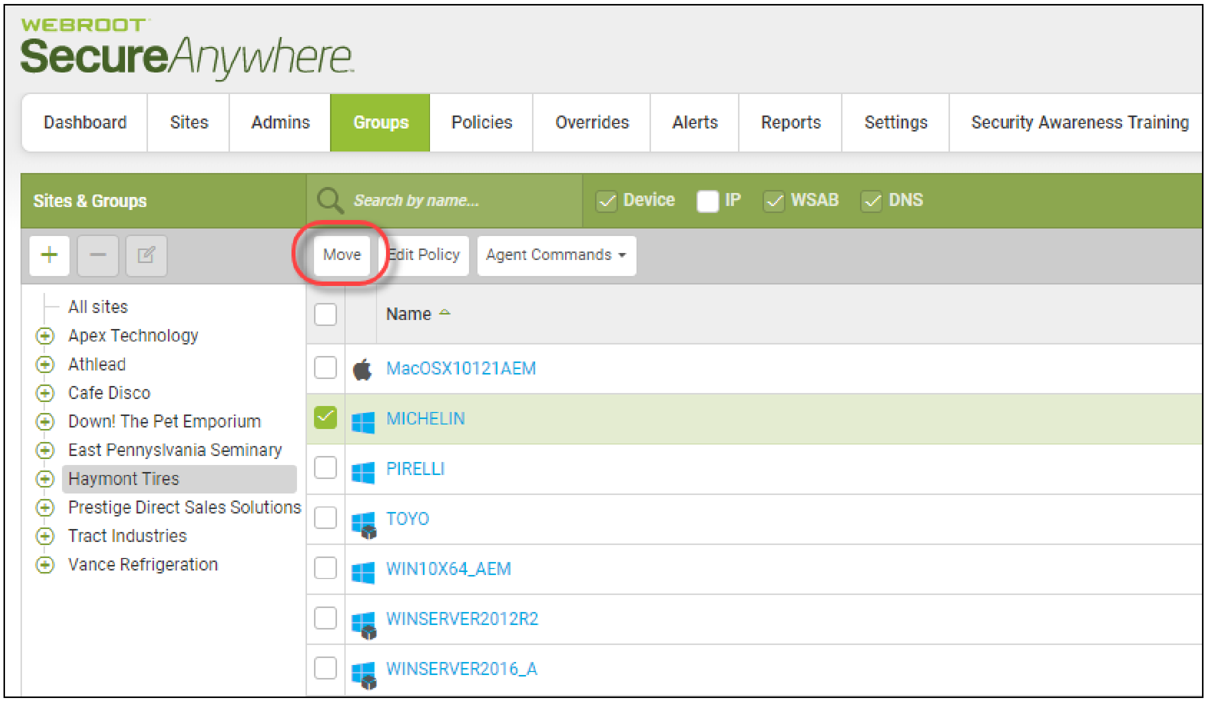
To select all endpoints, select the checkbox at the top of the column.



All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| ☑ | Name |
|---|---|
| ☑ | MacOSX10121AEM |
| ☑ | MICHELIN |
| ☑ | PIRELLI |
| ☑ | TOYO |
| ☑ | WIN10X64_AEM |
| ☑ | WINSERVER2012R2 |
| ☑ | WINSERVER2016_A |

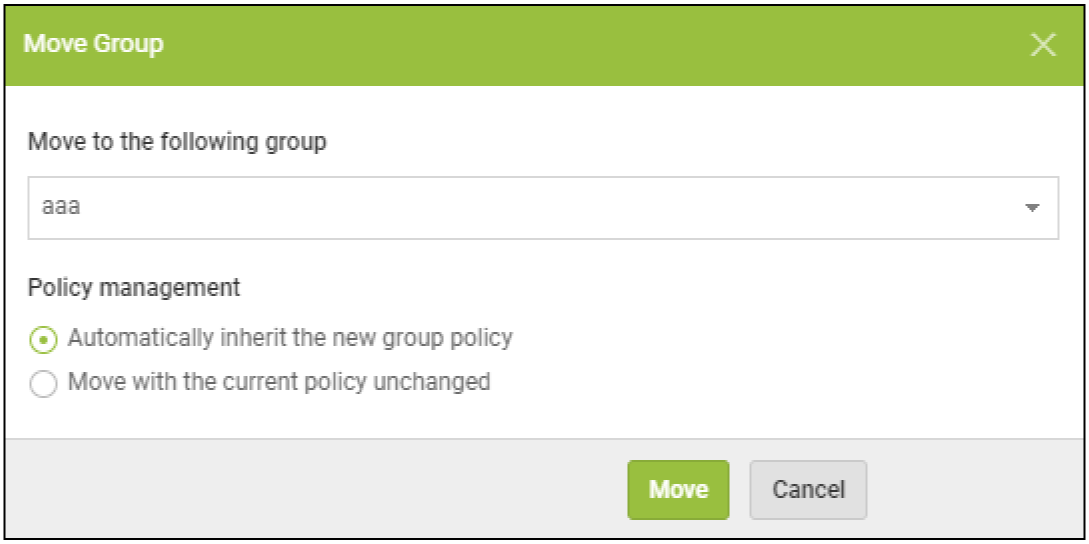
11. Click the **Move** button.



All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennsylvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| ☐ | Name ▴ |
|---|---|
| ☐ | MacOSX10121AEM |
| ☑ | MICHELIN |
| ☐ | PIRELLI |
| ☐ | TOYO |
| ☐ | WIN10X64_AEM |
| ☐ | WINSERVER2012R2 |
| ☐ | WINSERVER2016_A |

The Move Group window displays.



Move to the following group

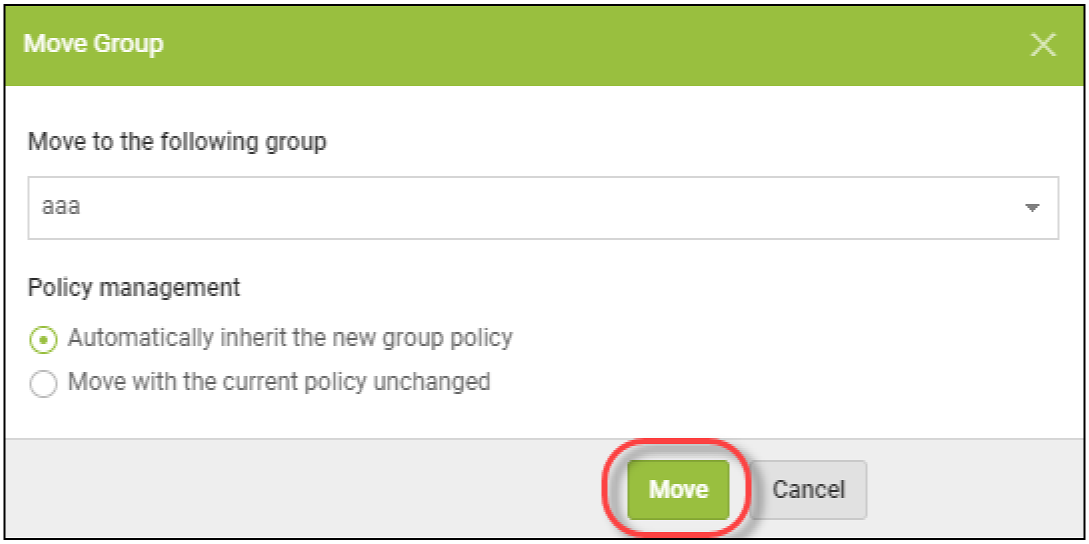
aaa ▾

Policy management

● Automatically inherit the new group policy

○ Move with the current policy unchanged

12. From the Move to the following group drop-down menu, select the new group you want to move the endpoint to.
13. Select one of the following Policy management radio buttons:
    - **Automatically inherit the new group policy**
    - **Move with the current policy unchanged**
14. Click the **Move** button.



Move Group

Move to the following group

aaa

Policy management

● Automatically inherit the new group policy

○ Move with the current policy unchanged

The group has been moved to the new group.

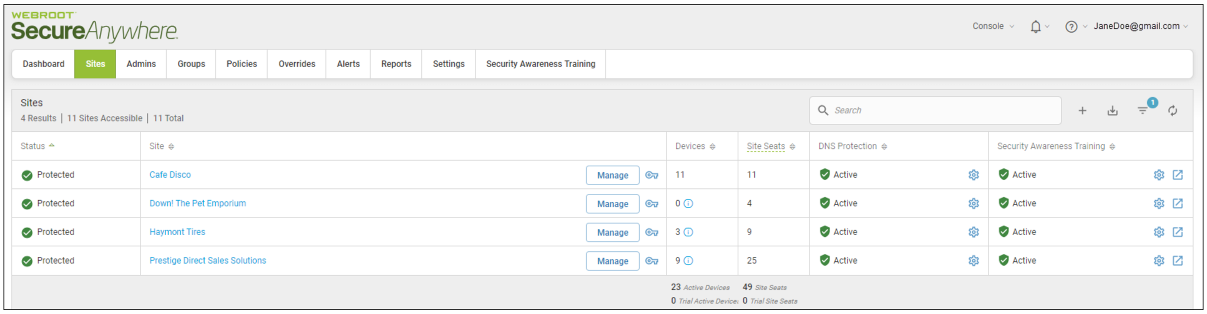
# Editing Groups

Follow this procedure to edit a group.

### To edit a group:

1. Log in to the management console.

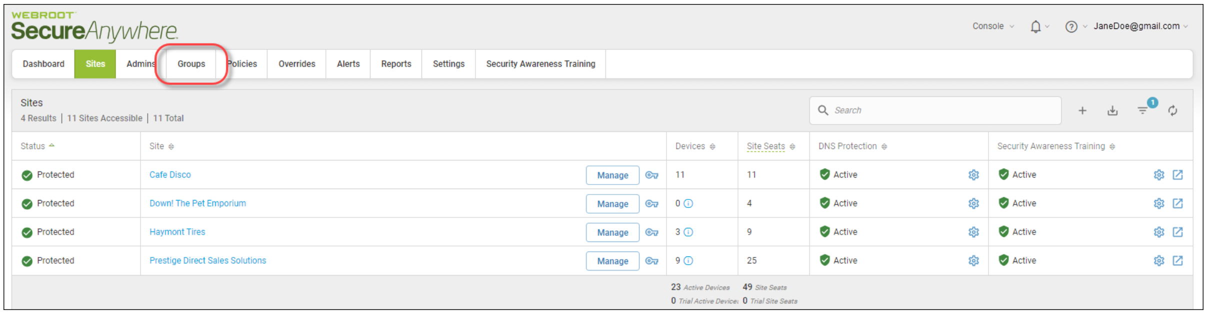
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

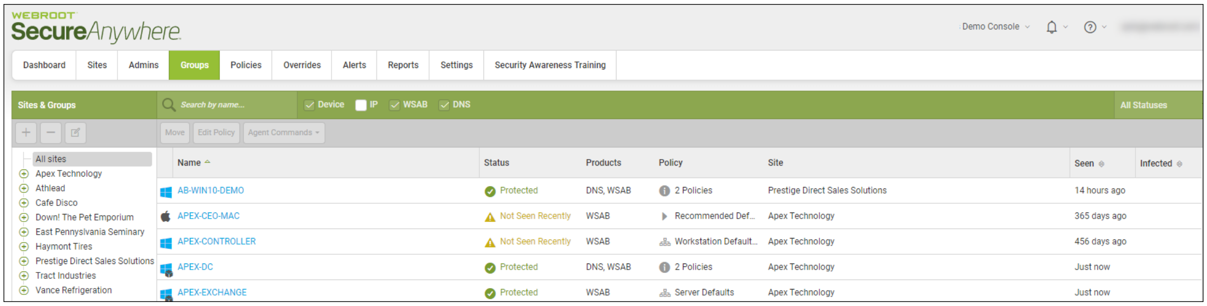
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

The Groups tab displays.



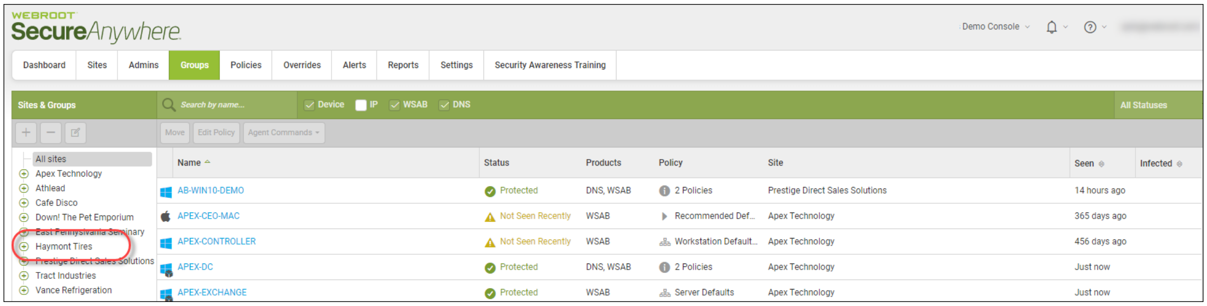
[redacted]

☑ Device □ IP ☑ WSAB ☑ DNS

All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

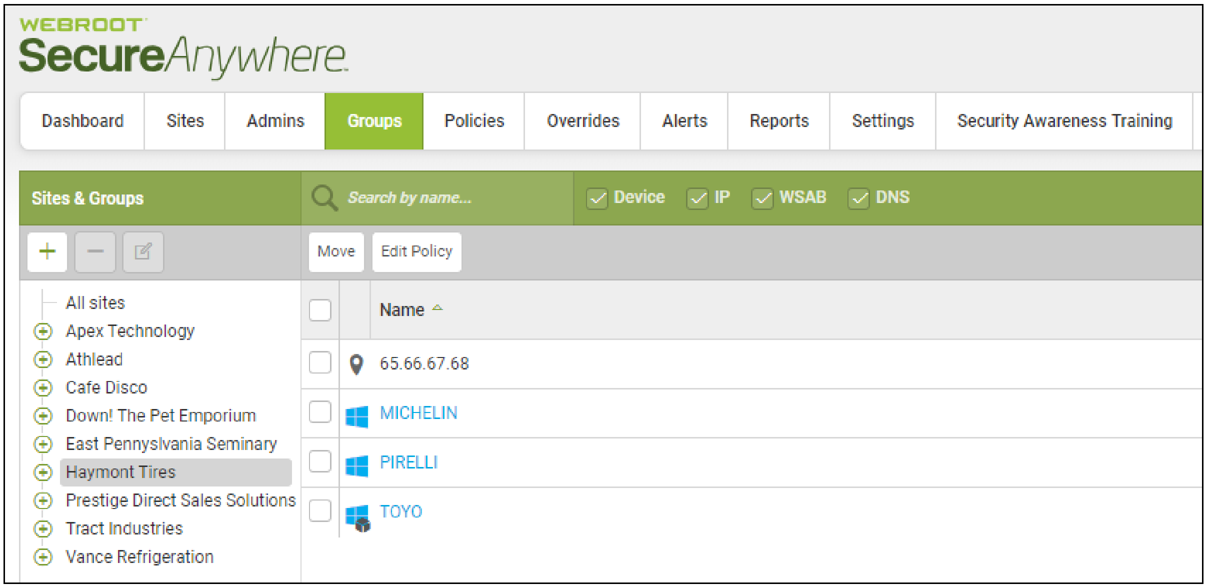
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. In the left column, select a site that contains a group you want to edit.



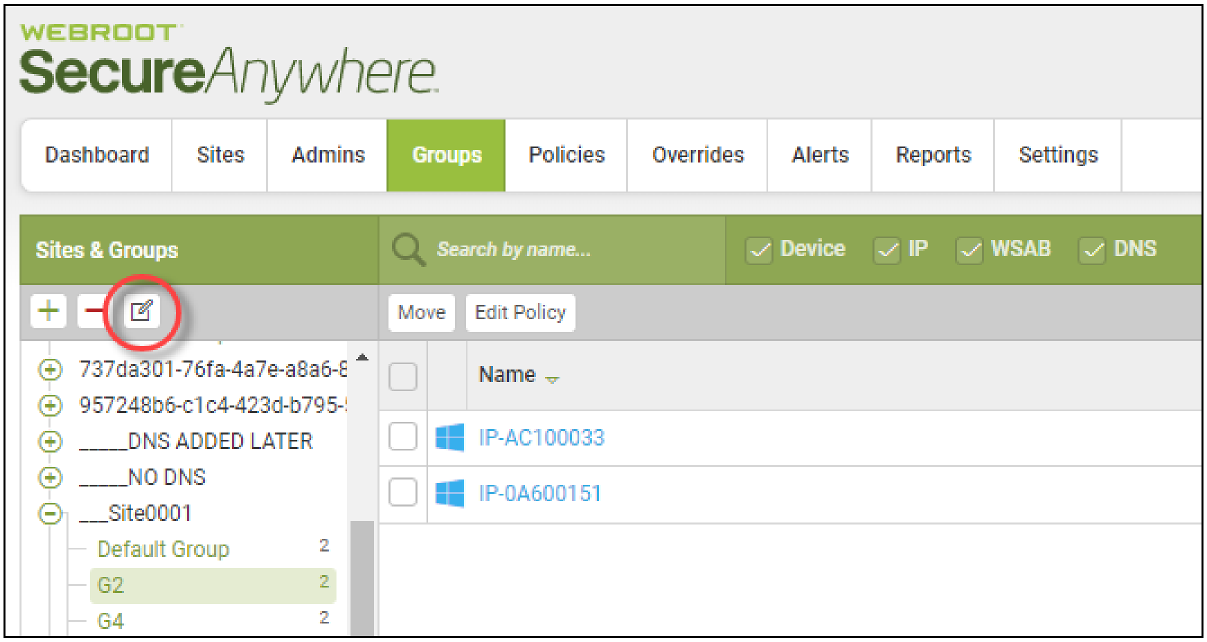
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The Edit button becomes active.

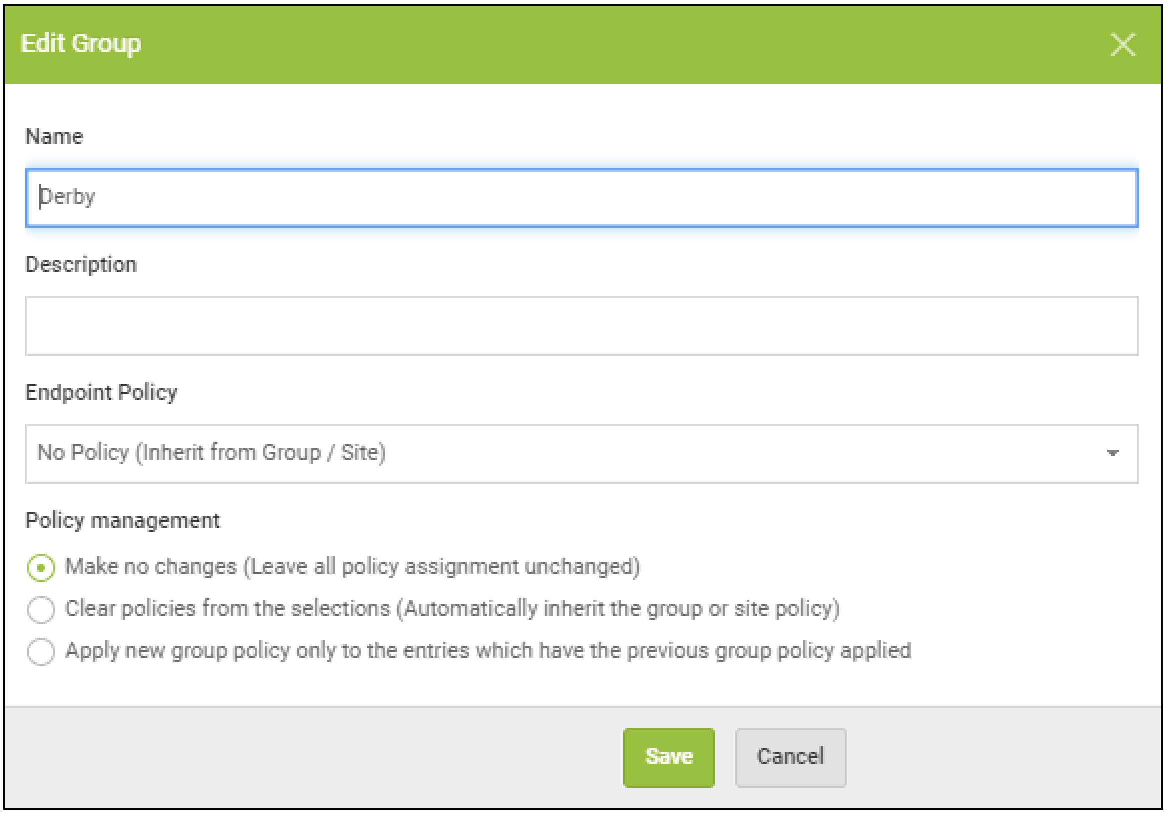


| Name |
|---|
| 65.66.67.68 |
| MICHELIN |
| PIRELLI |
| TOYO |

4. Click the **Edit** button.



The Edit Group window displays.



Edit Group

Name

Derby

Description

Endpoint Policy

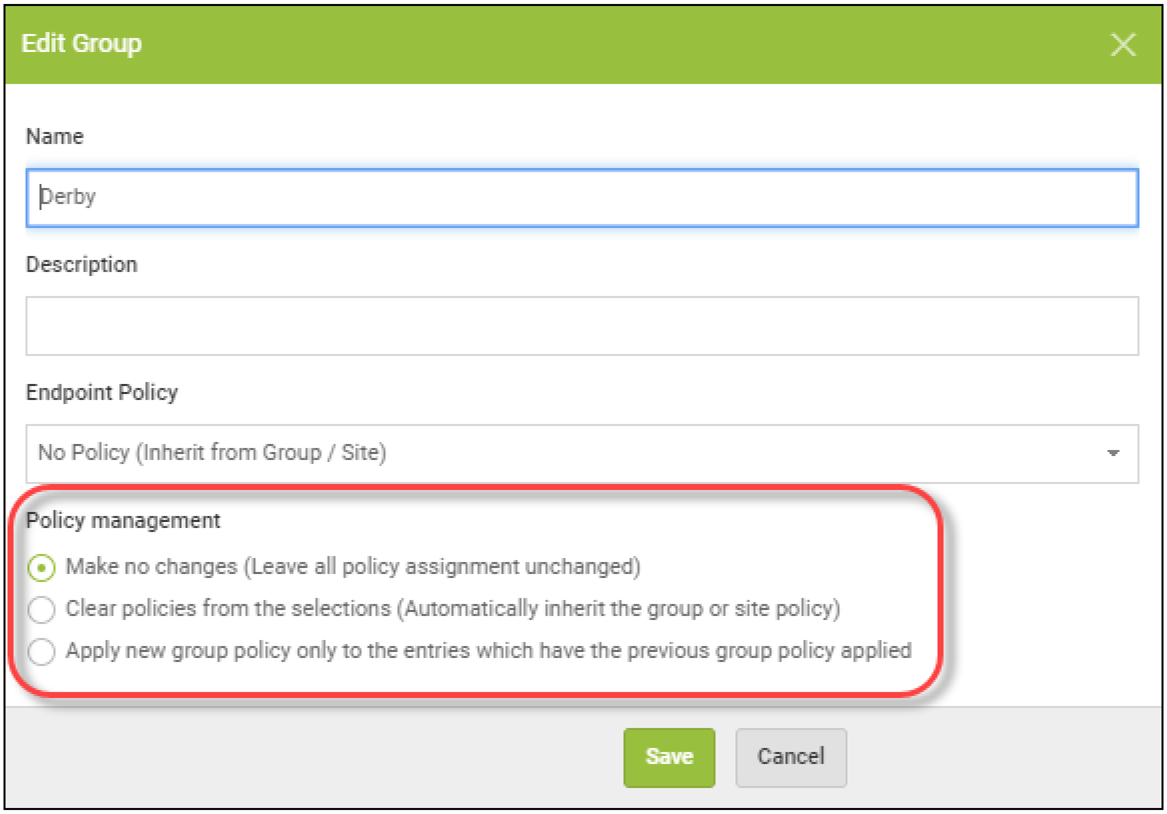
No Policy (Inherit from Group / Site)

Policy management

- ● Make no changes (Leave all policy assignment unchanged)
- ○ Clear policies from the selections (Automatically inherit the group or site policy)
- ○ Apply new group policy only to the entries which have the previous group policy applied

5. In the Name field, edit the name of the group. This is an optional step.
6. In the Description field, edit the description of the group. This is an optional step.
7. From the Endpoint Policy drop-down menu, select a different policy for the group. This is an optional step.

8. Select one of the following Policy Management radio buttons. This is an optional step.



Edit Group

Name

Derby

Description

Endpoint Policy

No Policy (Inherit from Group / Site)

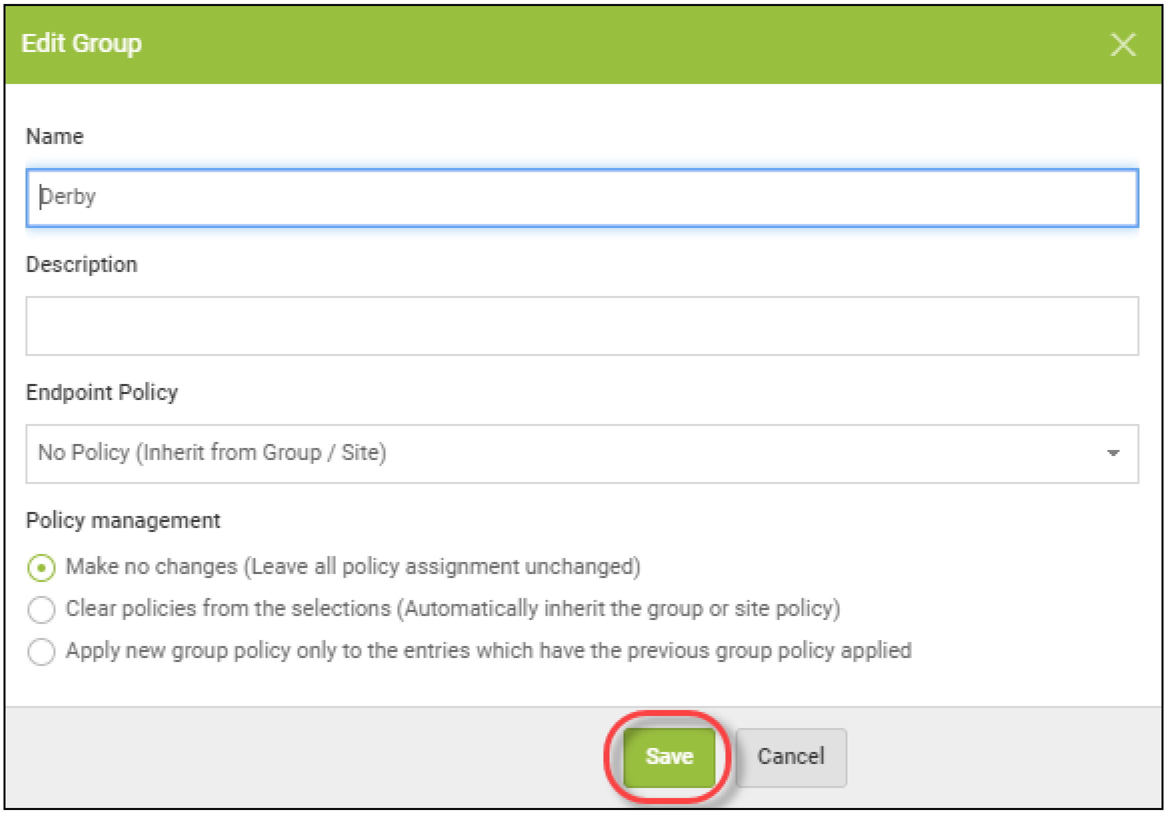
Policy management

● Make no changes (Leave all policy assignment unchanged)

○ Clear policies from the selections (Automatically inherit the group or site policy)

○ Apply new group policy only to the entries which have the previous group policy applied

9. When you're done, click the **Save** button.



Edit Group

Name

Derby

Description

Endpoint Policy

No Policy (Inherit from Group / Site)

Policy management

● Make no changes (Leave all policy assignment unchanged)

○ Clear policies from the selections (Automatically inherit the group or site policy)

○ Apply new group policy only to the entries which have the previous group policy applied

The information for the group is updated.

# Deleting Groups

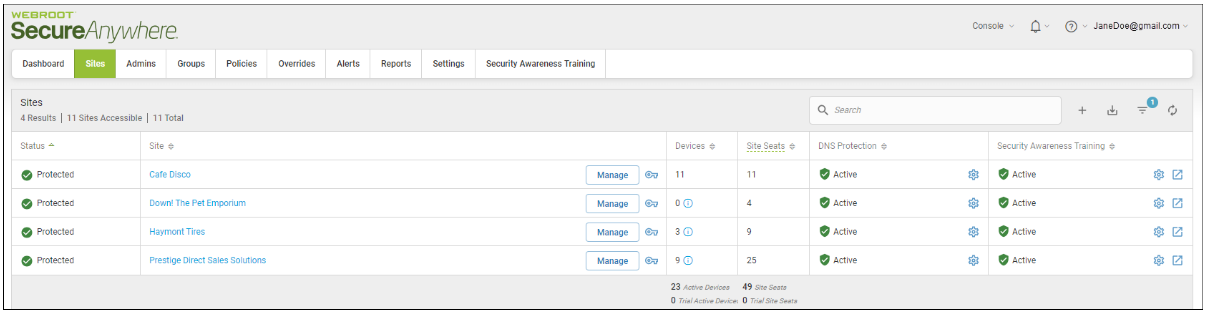
In the Groups tab, you can easily delete a group from the list and move its endpoints to another group.

You cannot retrieve a deleted group; however, you can re-use a deleted group name.

**To delete a group:**

1. Log in to the management console.

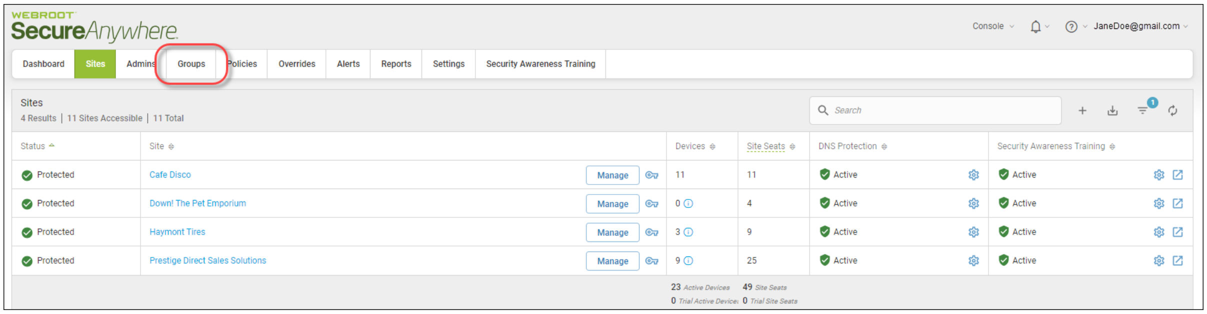
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

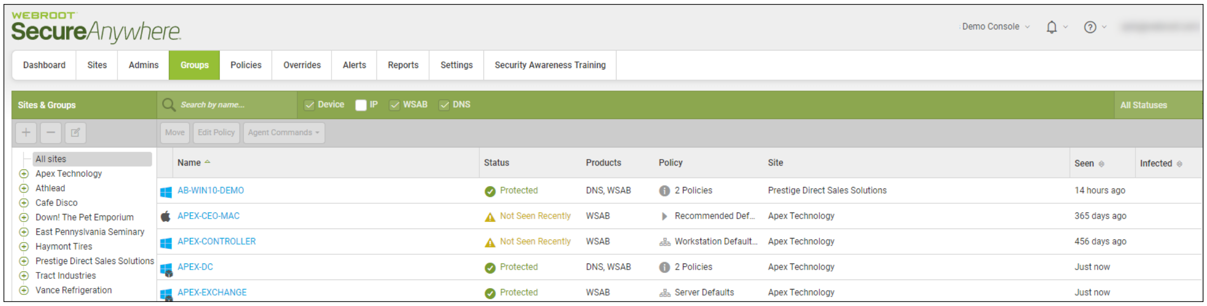
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

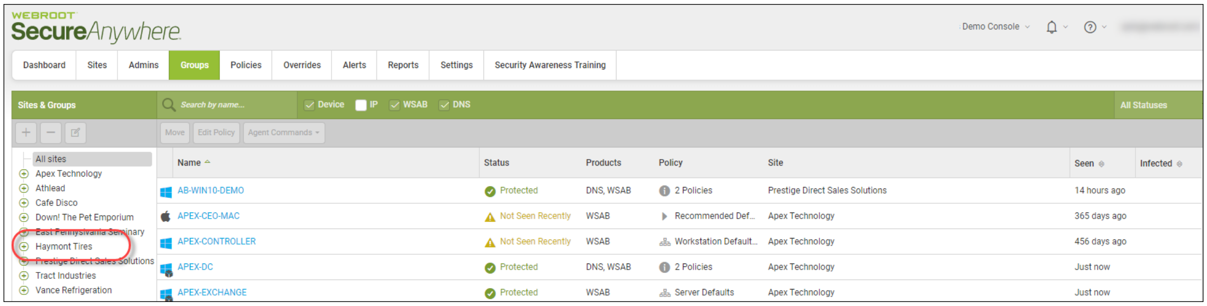
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



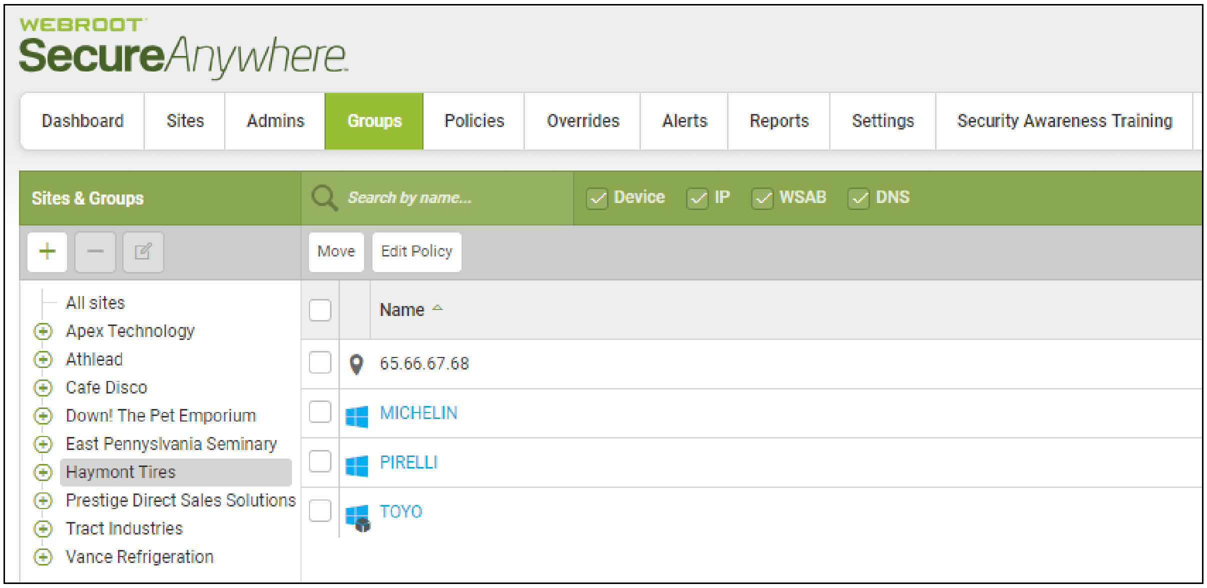
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. From the Sites & Groups column, select the group you want to delete.



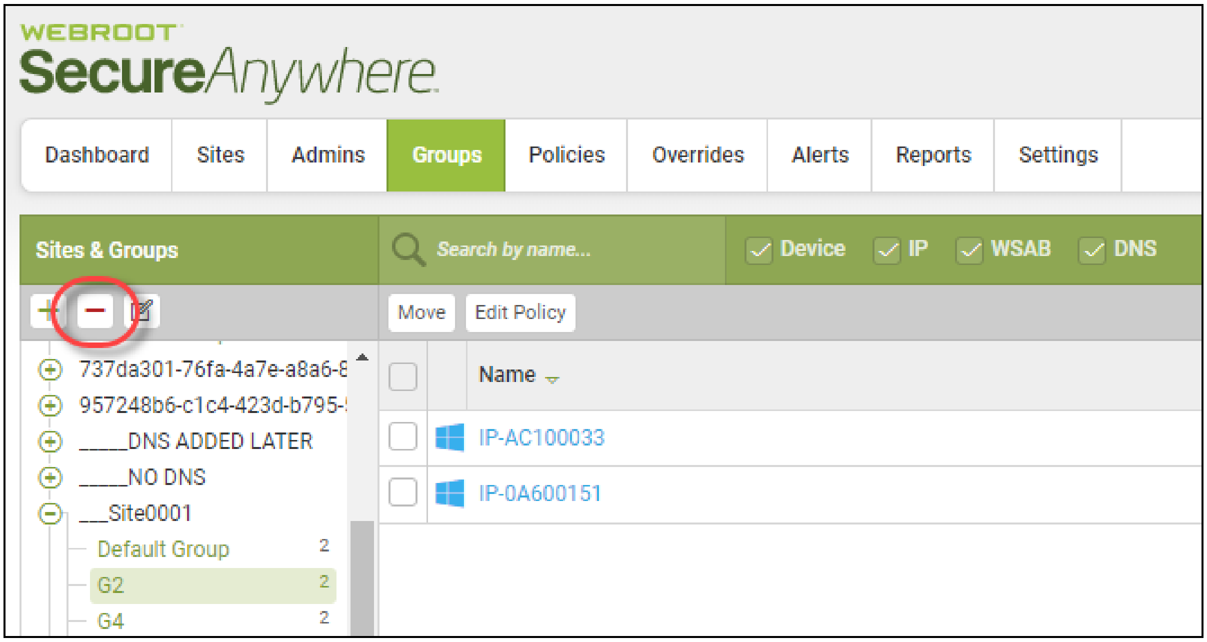
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The Minus (-) button becomes active.



| □ | Name |
|---|---|
| □ | 65.66.67.68 |
| □ | MICHELIN |
| □ | PIRELLI |
| □ | TOYO |

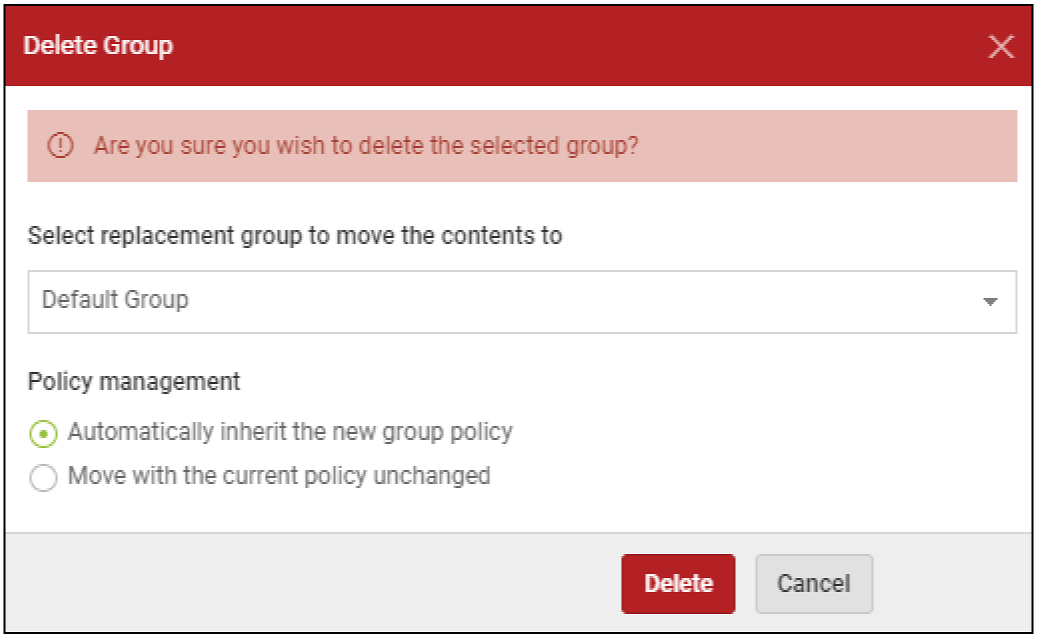
4. Click the **Minus (-)** button.



- 737da301-76fa-4a7e-a8a6-8
- 957248b6-c1c4-423d-b795-
- _____DNS ADDED LATER
- _____NO DNS
- ___Site0001
  - Default Group 2
  - G2 2
  - G4 2

| □ | Name |
|---|---|
| □ | IP-AC100033 |
| □ | IP-0A600151 |

The Delete Group window displays.



Delete Group

ⓘ Are you sure you wish to delete the selected group?

Select replacement group to move the contents to

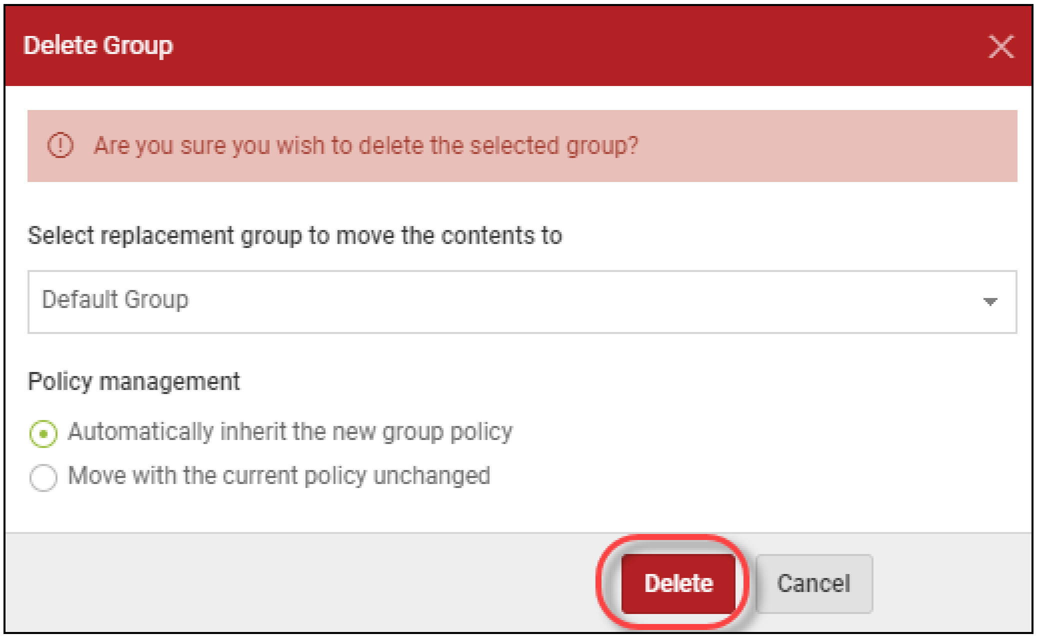
Default Group

Policy management

● Automatically inherit the new group policy

○ Move with the current policy unchanged

5. From the Select replacement group drop-down menu, select the replacement group to move the contents to.
6. Select one of the following Policy management radio buttons:
   - **Automatically inherit the new group policy**
   - **Move with the current policy unchanged**
7. Click the **Delete** button.



Delete Group

Are you sure you wish to delete the selected group?

Select replacement group to move the contents to

Default Group

Policy management

● Automatically inherit the new group policy

○ Move with the current policy unchanged

The group is deleted.

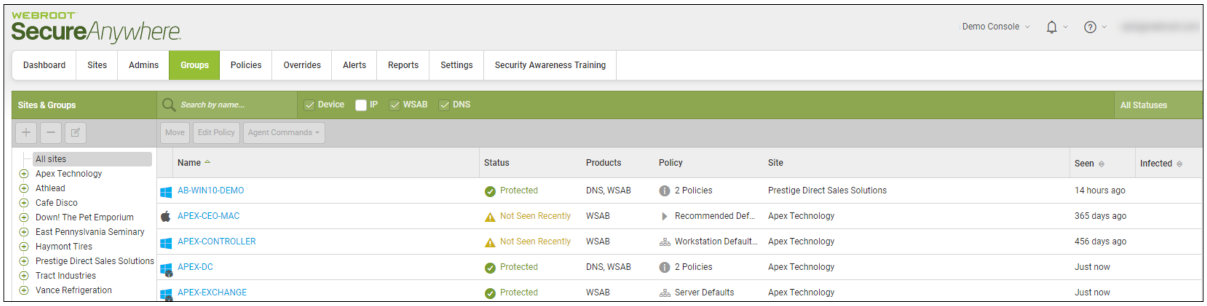
# Chapter 6: Working With Devices

To work with devices, see the following topics:

# Device Management Overview

Included in the management console is the ability to see an overview of all devices across all sites. In addition, admins can filter by site or status, and drill-down on a particular device to view information about threats encountered on the device, blocked URLs. Admins can also restore files or quarantine files.

All Device Management functionality is located in the management console under the Groups tab.



All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

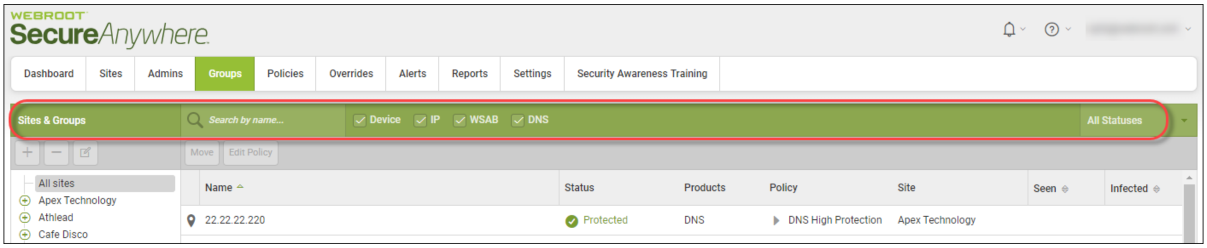
There are three main areas in the Groups tab:

- Filters
- Columns
- Page-Through Functionality

## Groups Tab Filters

The Groups tab has three built-in filters, so you can:

- Filter Devices by Sites Names
- Filter Devices by Statuses
- Filter Devices Within Groups
- Sort Devices Within Groups
- Search for Devices



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| 22.22.22.220 | Protected | DNS | DNS High Protection | Apex Technology | | |

## Groups Tab Columns

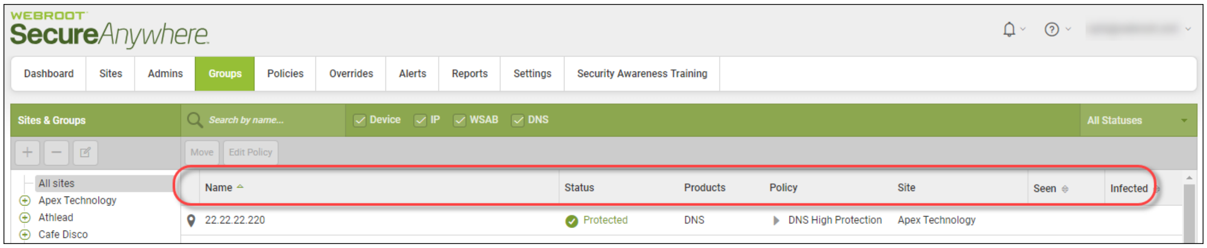
The main part of the Devices tab displays all of your devices in the following columns:

- **Name** — Displays the name of the device, and includes an icon that indicates the type of device.

| DEVICE ICON | DESCRIPTION |
|---|---|
| ⊞ | Indicates that the device is a Windows PC. |
| ⊞ | Indicates that the device is a Windows server. |
|  | Indicates that the device is an Apple Mac. |

- **Status** — Displays the current status of the device, as described in the following table:

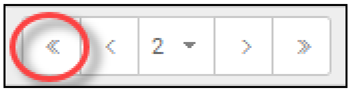
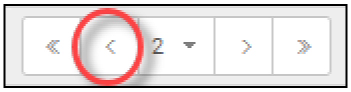
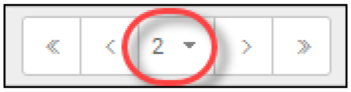
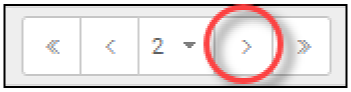
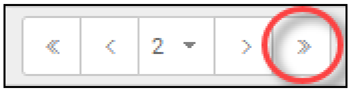
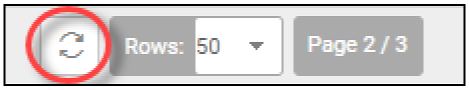
| STATUS ICON | DESCRIPTION |
|---|---|
| ✓ Protected | **Protected** — Indicates that the device is protected |
| ✗ Needs Attention | **Needs Attention** — Indicates that the device needs attention. |
| ⚠ Expired | **Expired** — Indicates that the device license has expired and is no longer being protected by Webroot SecureAnywhere. |
| ✗ Attention & Expired | **Attention & Expired** — Indicates that as well as needing attention, the device license has expired and is no longer being protected by Webroot SecureAnywhere. |
| ⚠ Not Seen Recently | **Not Seen Recently** — Indicates that the device has not checked in recently. |

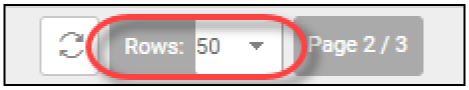
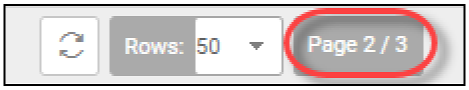


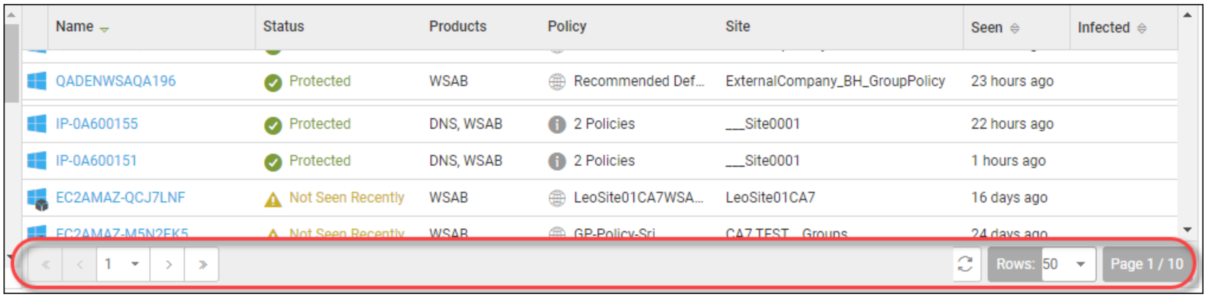
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| 22.22.22.220 | ✓ Protected | DNS | ▸ DNS High Protection | Apex Technology | | |

## Groups Tab Page-Through Functionality

The bottom of the Devices tab has the page-through functionality, as described in the following table.

| FUNCTION | DESCRIPTION |
|---|---|
|  | Click the **Double Left** arrow to go to the first page in the list |
|  | Click the **Left** arrow to go to the previous page in the list. |
|  | Indicates which page in the list displays. |
|  | Click the **Right** arrow to go to the next page in the list.<br>From the drop-down menu, select any page in the list to go directly to that page. |
|  | Click the **Double Right** arrow to go to the last page in the list. |
|  | Click the Refresh icon to refresh the information on the page. |

| FUNCTION | DESCRIPTION |
|---|---|
|  | Indicates how many rows display on a page. From the drop-down menu, you can select any of the following increments:<br>• 50<br>• 100<br>• 200<br>• 500 |
|  | Gives a numerical indicator as to which page out of how many pages in the list that displays. |



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| QADENWSAQA196 | Protected | WSAB | Recommended Def... | ExternalCompany_BH_GroupPolicy | 23 hours ago | |
| IP-0A600155 | Protected | DNS, WSAB | 2 Policies | ___Site0001 | 22 hours ago | |
| IP-0A600151 | Protected | DNS, WSAB | 2 Policies | ___Site0001 | 1 hours ago | |
| EC2AMAZ-QCJ7LNF | Not Seen Recently | WSAB | LeoSite01CA7WSA... | LeoSite01CA7 | 16 days ago | |
| EC2AMAZ-M5N2FK5 | Not Seen Recently | WSAB | GP-Policy-Sri | CA7 TEST_ Groups | 24 days ago | |

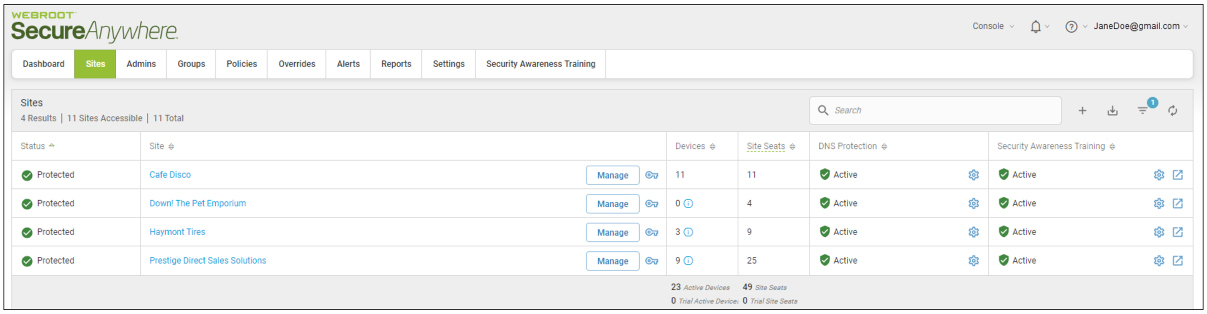
# Editing Policies Applied To Devices

Follow this procedure to edit which policy is applied to a device.

**To edit a policy:**

1. Log in to the management console.

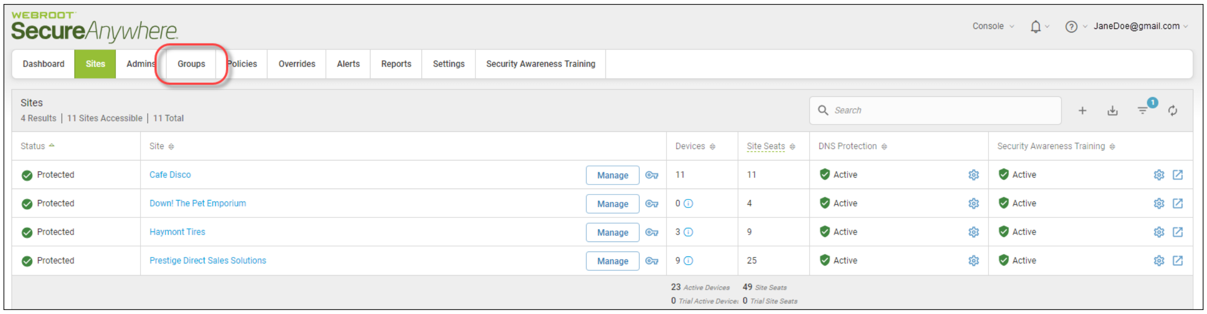
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

2. Click the **Groups** tab.

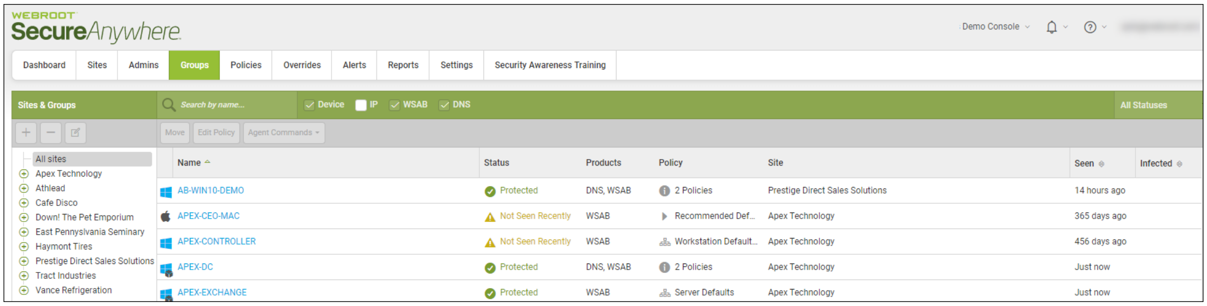


WEBROOT SecureAnywhere
Console
JaneDoe@gmail.com
Dashboard | Sites | Admins | Groups | Policies | Overrides | Alerts | Reports | Settings | Security Awareness Training

Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

The Groups tab displays.



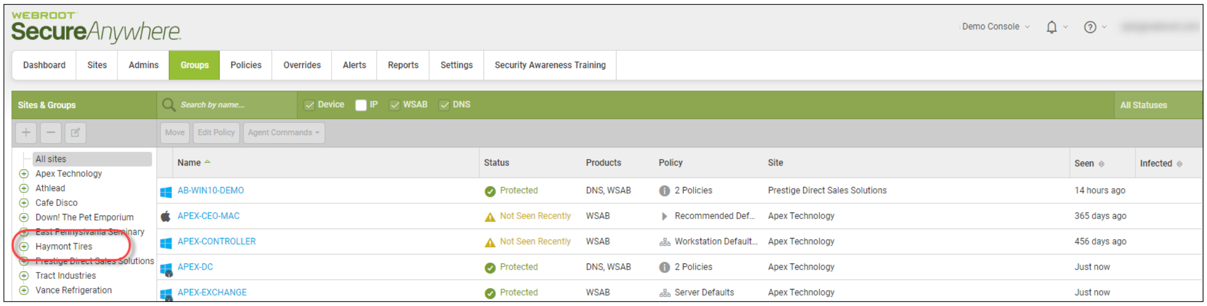
[redacted]

☑ Device □ IP ☑ WSAB ☑ DNS

All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

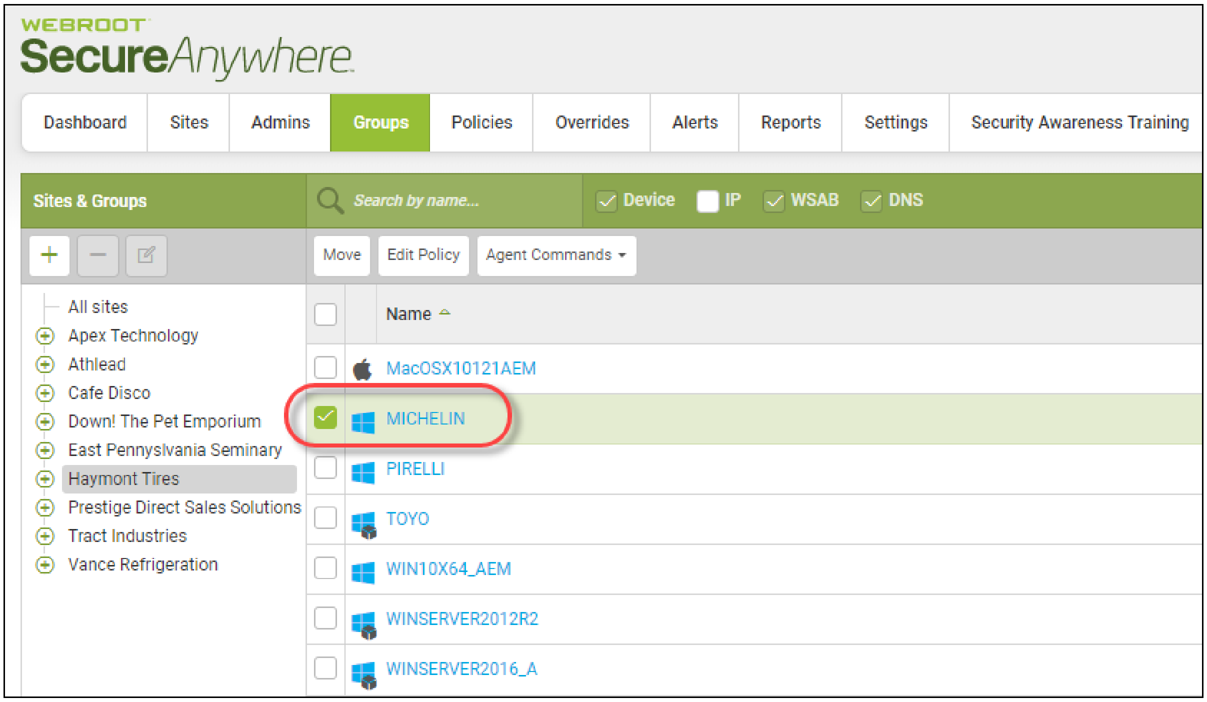
3. In the left column, select the site that contains the group and device you want to edit the policy for.



All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennysilvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

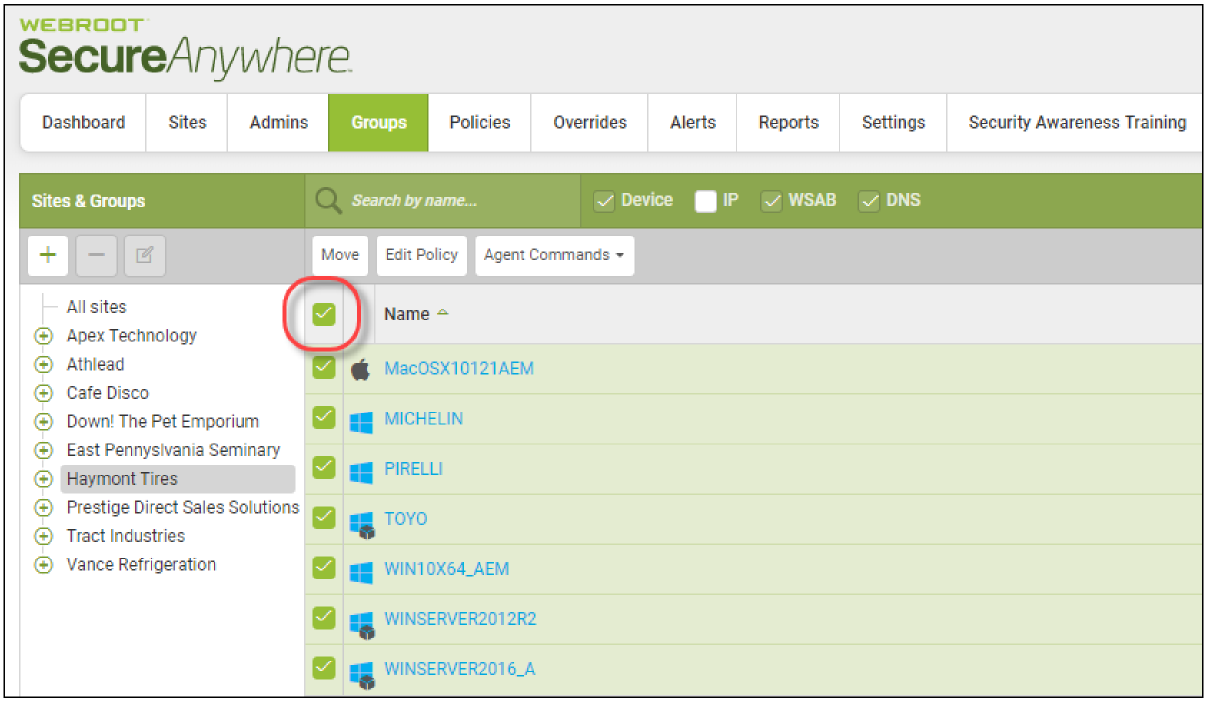
4. In the Devices panel, select the device that you want to edit the policy for.



All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| | Name |
|---|---|
| □ | MacOSX10121AEM |
| ☑ | MICHELIN |
| □ | PIRELLI |
| □ | TOYO |
| □ | WIN10X64_AEM |
| □ | WINSERVER2012R2 |
| □ | WINSERVER2016_A |

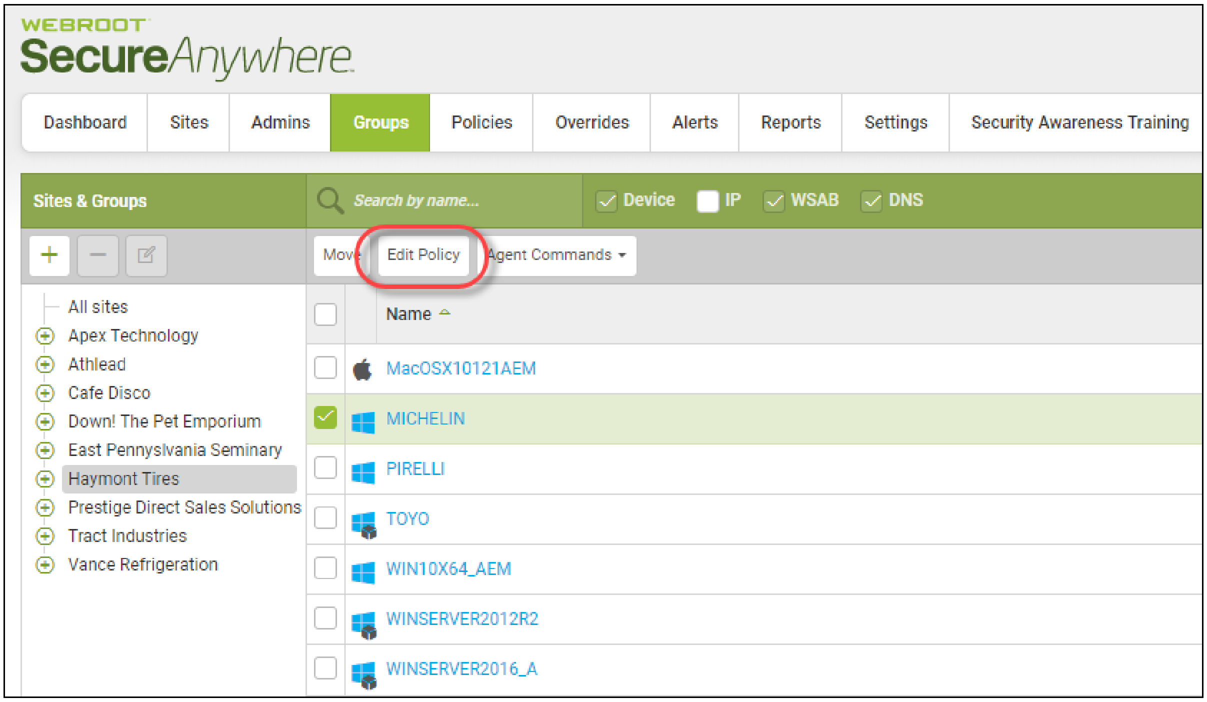
To select all devices, select the checkbox at the top of the column.



All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| ☑ | Name |
|---|---|
| ☑ | MacOSX10121AEM |
| ☑ | MICHELIN |
| ☑ | PIRELLI |
| ☑ | TOYO |
| ☑ | WIN10X64_AEM |
| ☑ | WINSERVER2012R2 |
| ☑ | WINSERVER2016_A |

5. Click the **Edit Policy** button.

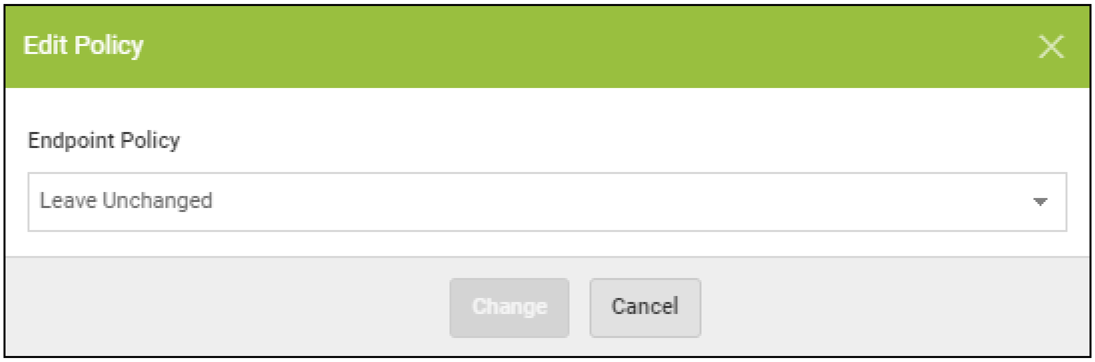


Sites & Groups:

- All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennsylvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| | Name |
|---|---|
| □ | MacOSX10121AEM |
| ☑ | MICHELIN |
| □ | PIRELLI |
| □ | TOYO |
| □ | WIN10X64_AEM |
| □ | WINSERVER2012R2 |
| □ | WINSERVER2016_A |

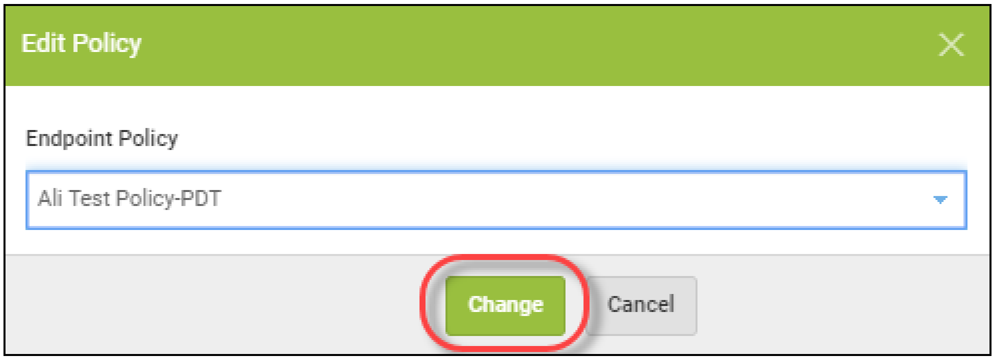
The Edit Policy window displays.



Endpoint Policy: Leave Unchanged

6. From the Endpoint Policy drop-down menu, select the policy you want to apply to the device.

7. Click the **Change** button.



The new policy is applied to the device.

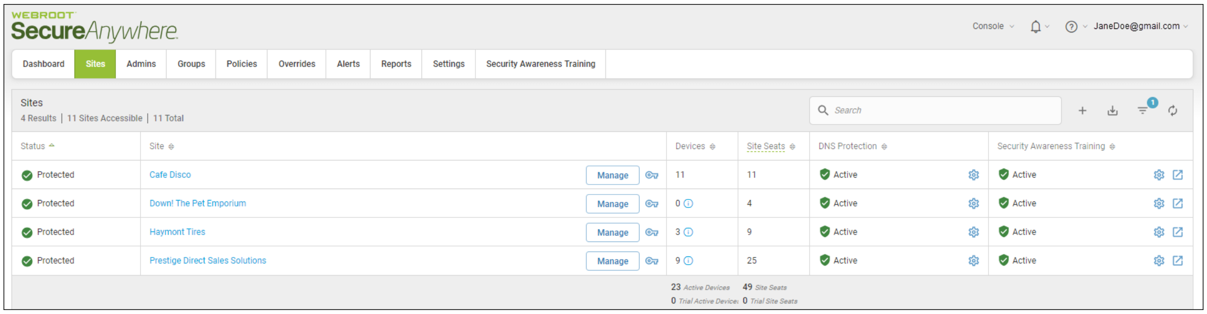
# Adding Web Overrides to Devices

Any device, regardless of its status, can have URLs that have been blocked. Follow this procedure to add a web override to any device.

### To add a web override to a device:

1. Log in to the management console.

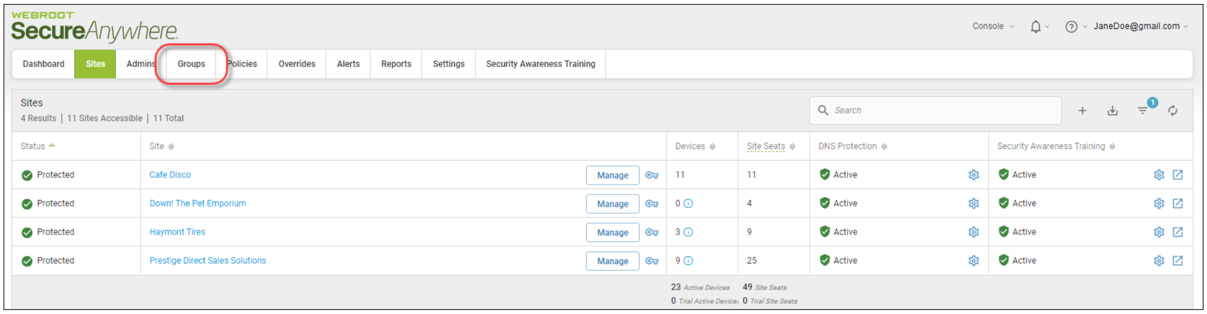
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

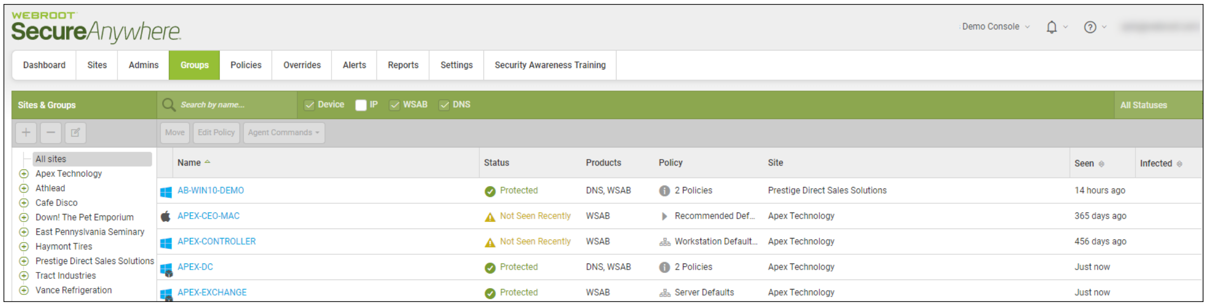
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

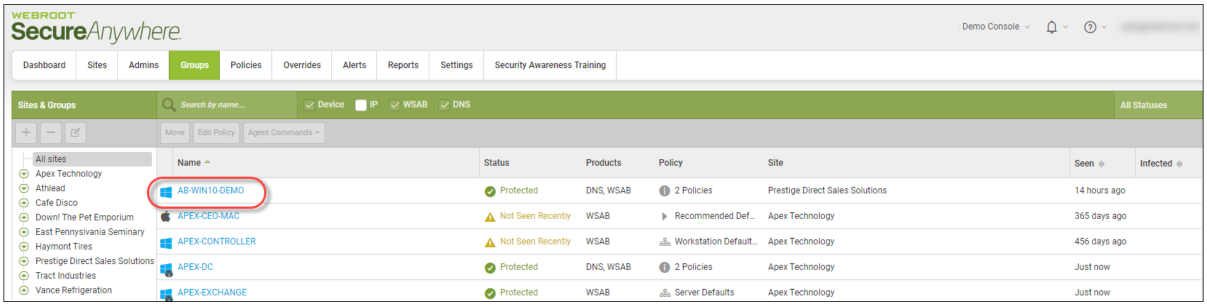
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



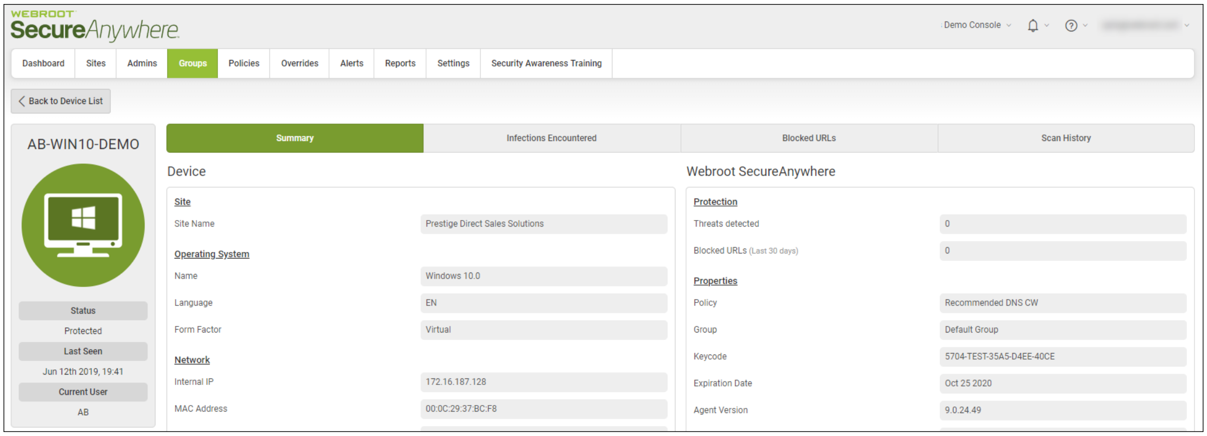
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. Select the device that has blocked URLs that you want to override.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The Status Panel for the device you selected displays.



AB-WIN10-DEMO

Status: Protected

Last Seen: Jun 12th 2019, 19:41

Current User: AB

Device

Site
| | |
|---|---|
| Site Name | Prestige Direct Sales Solutions |

Operating System
| | |
|---|---|
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Virtual |

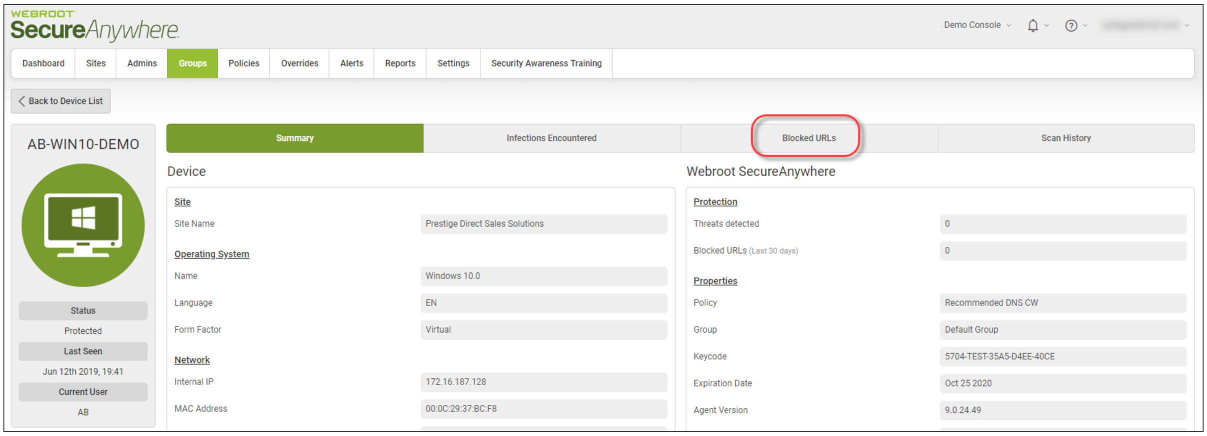
Network
| | |
|---|---|
| Internal IP | 172.16.187.128 |
| MAC Address | 00:0C:29:37:BC:F8 |

Webroot SecureAnywhere

Protection
| | |
|---|---|
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |

Properties
| | |
|---|---|
| Policy | Recommended DNS CW |
| Group | Default Group |
| Keycode | 5704-TEST-35A5-D4EE-40CE |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |

4. Click the **Blocked URLs** tab.



AB-WIN10-DEMO

| | |
|---|---|
| Status | Protected |
| Last Seen | Jun 12th 2019, 19:41 |
| Current User | AB |

Device

Site

| | |
|---|---|
| Site Name | Prestige Direct Sales Solutions |

Operating System

| | |
|---|---|
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Virtual |

Network

| | |
|---|---|
| Internal IP | 172.16.187.128 |
| MAC Address | 00:0C:29:37:BC:F8 |

Webroot SecureAnywhere

Protection

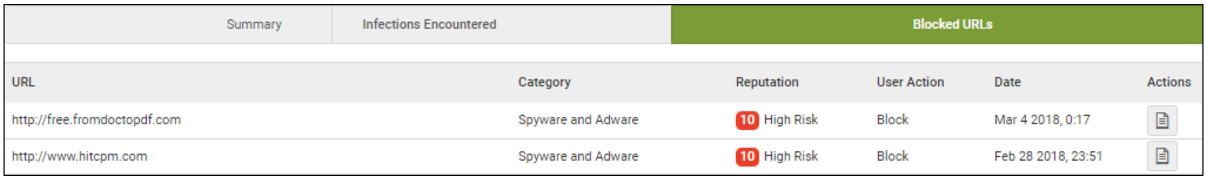
| | |
|---|---|
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |

Properties

| | |
|---|---|
| Policy | Recommended DNS CW |
| Group | Default Group |
| Keycode | 5704-TEST-35A5-D4EE-40CE |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |

The Blocked URLs tab displays with the following columns:

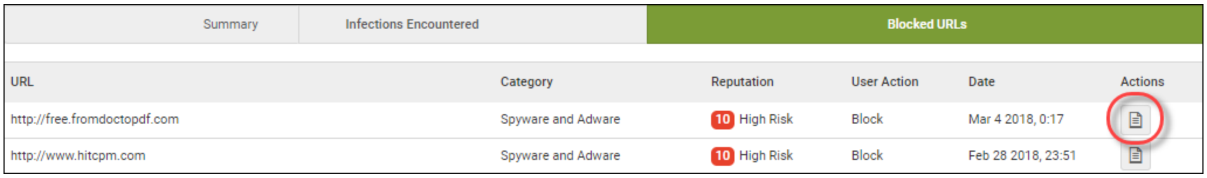
- **URL** — The URL that has been blocked.
- **Category** — The type of URL that has been blocked. For more information about the categories of websites, see Webroot's Category Descriptions.
- **Reputation** — The reputation of the URL that has been blocked. For more information about the reputation of websites, see Webroot's Reputation Descriptions.
- **User Action** — TBD.
- **Date** — The date the URL first displayed in the list.
- **Actions** — Displays the Create New Entry window, where you can enter information to create a web override.



| URL | Category | Reputation | User Action | Date | Actions |
|---|---|---|---|---|---|
| http://free.fromdoctopdf.com | Spyware and Adware | 10 High Risk | Block | Mar 4 2018, 0:17 | 🗎 |
| http://www.hitcpm.com | Spyware and Adware | 10 High Risk | Block | Feb 28 2018, 23:51 | 🗎 |

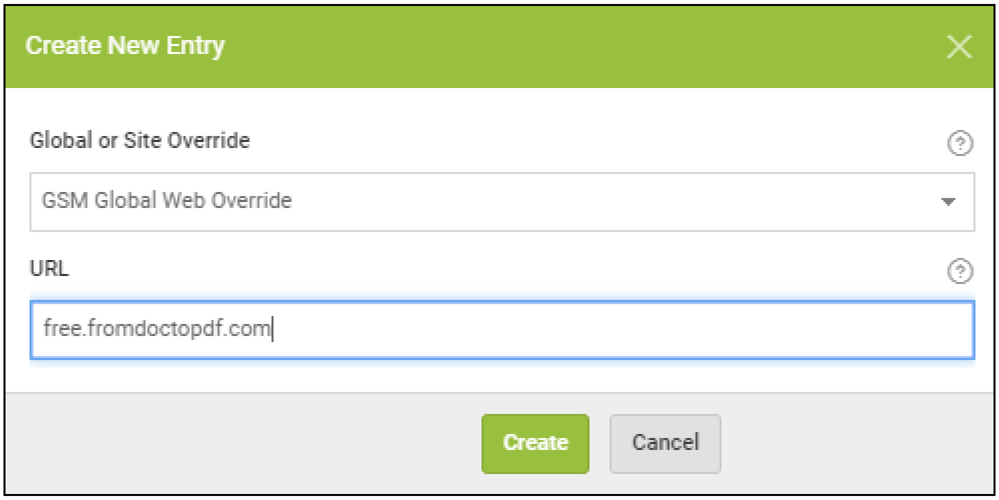
**Note:** Only when there are blocked URLs does the additional functionality display. If there are no blocked URLs, then only the URL column displays.

5. Click the **Action** icon.



| URL | Category | Reputation | User Action | Date | Actions |
|---|---|---|---|---|---|
| http://free.fromdoctopdf.com | Spyware and Adware | 10 High Risk | Block | Mar 4 2018, 0:17 | |
| http://www.hitcpm.com | Spyware and Adware | 10 High Risk | Block | Feb 28 2018, 23:51 | |

The Create New Entry window displays.

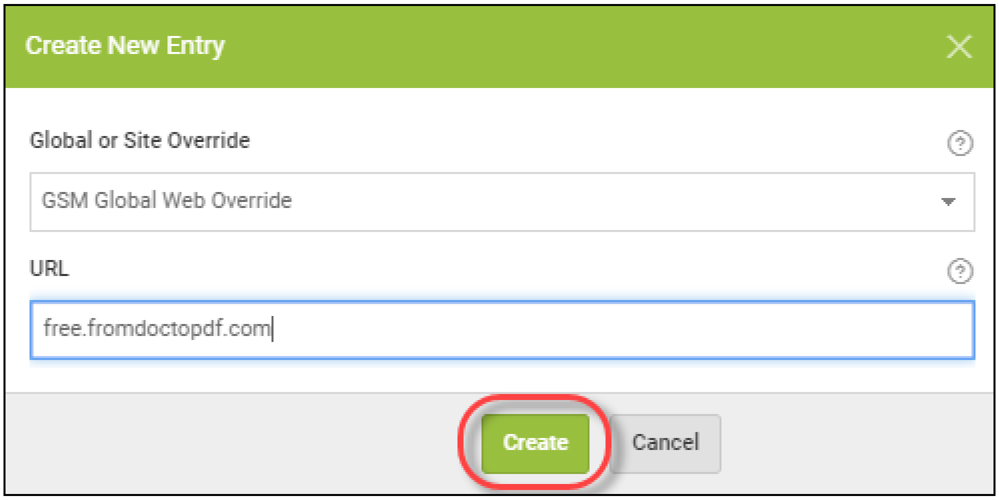

Create New Entry

Global or Site Override: GSM Global Web Override

URL: free.fromdoctopdf.com

6. In the URL column, the URL that is blocked displays. Alternately, you can enter a new URL to apply the web override to.
7. From the Global or Site Override drop-down menu, select one of the following to determine whether to create the web override at the management console or Site level:
   - **GSM Global Web Override**
   - **Site Name**

8. When you're done, click the **Create** button.



Create New Entry

Global or Site Override: GSM Global Web Override

URL: free.fromdoctopdf.com

The system creates the web override.

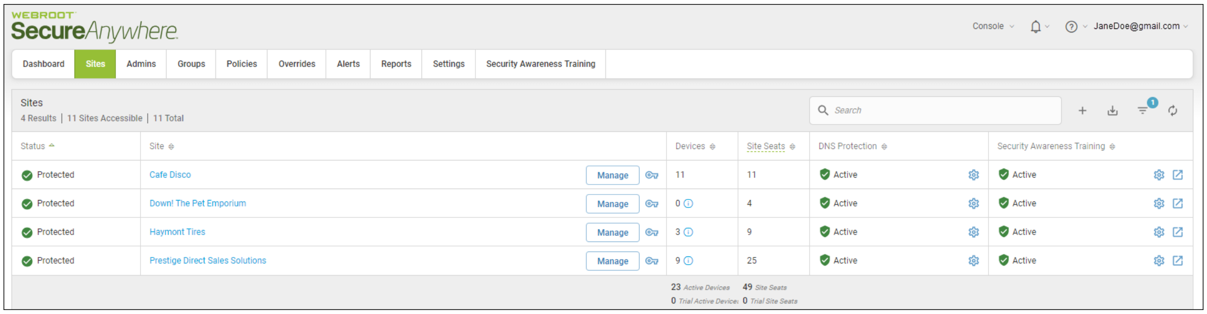
# Whitelisting Files on Devices

Any device, regardless of its status, can have files that have been quarantined. Follow this procedure to whitelist a file on a device.

**To whitelist a file on a device:**

1. Log in to the management console.

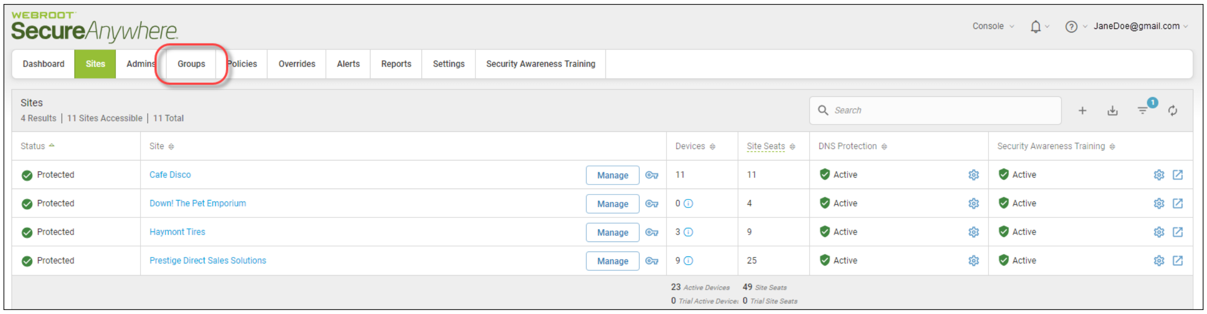
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

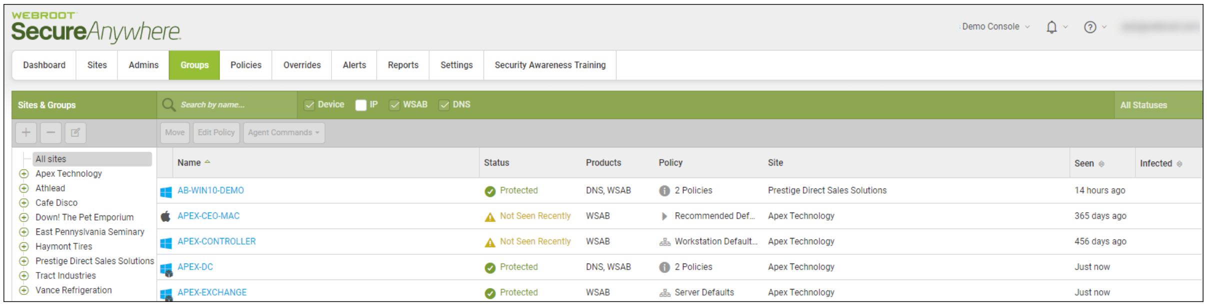
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

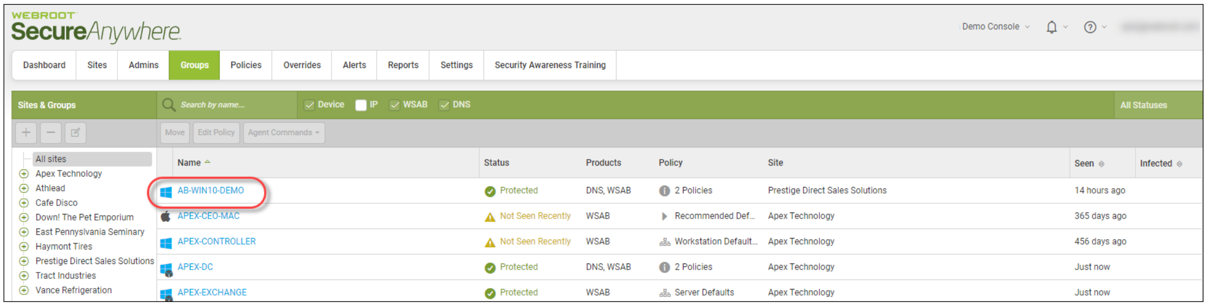
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

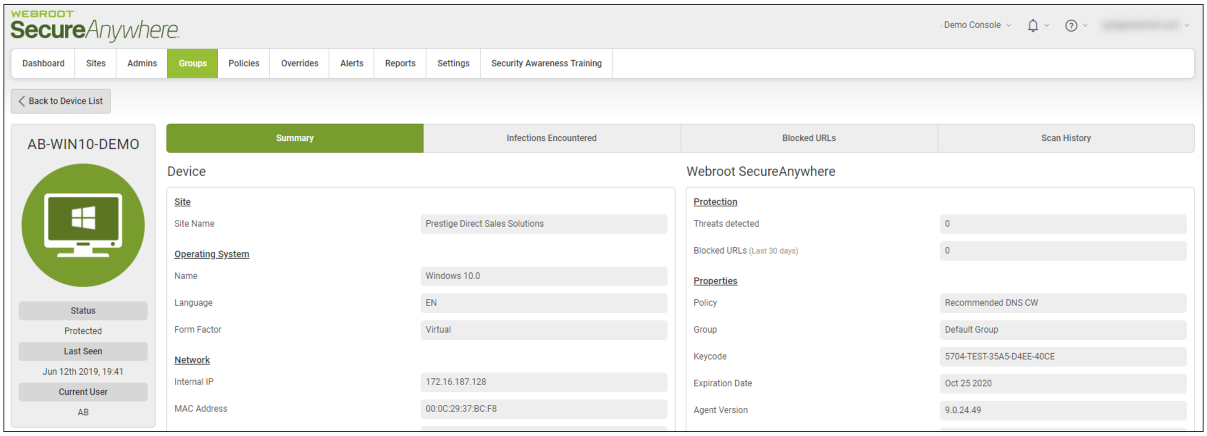
3. Select the device that has blocked URLs that you want to override.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

> **Note:** The example shows a device with a Protected status however you can whitelist files on devices regardless of their status.

The Status and Summary panel for the device you selected displays.



AB-WIN10-DEMO

Status
Protected
Last Seen
Jun 12th 2019, 19:41
Current User
AB

Device

Site
Site Name: Prestige Direct Sales Solutions

Operating System
Name: Windows 10.0
Language: EN
Form Factor: Virtual

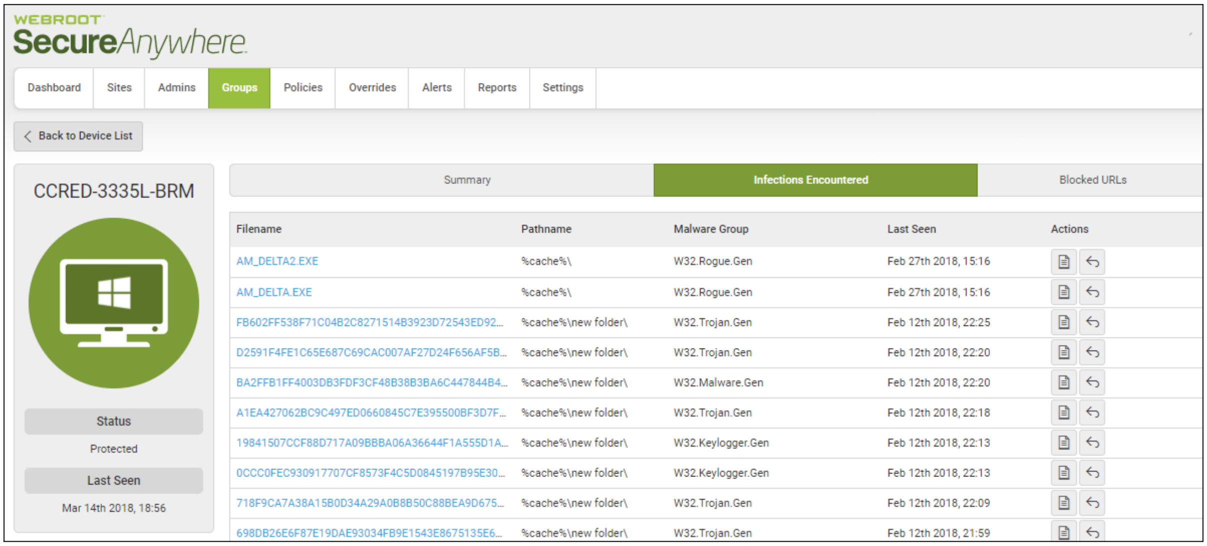
Network
Internal IP: 172.16.187.128
MAC Address: 00:0C:29:37:BC:F8

Webroot SecureAnywhere

Protection
Threats detected: 0
Blocked URLs (Last 30 days): 0

Properties
Policy: Recommended DNS CW
Group: Default Group
Keycode: 5704-TEST-35A5-D4EE-40CE
Expiration Date: Oct 25 2020
Agent Version: 9.0.24.49

4. Click the **Infections Encountered** tab.



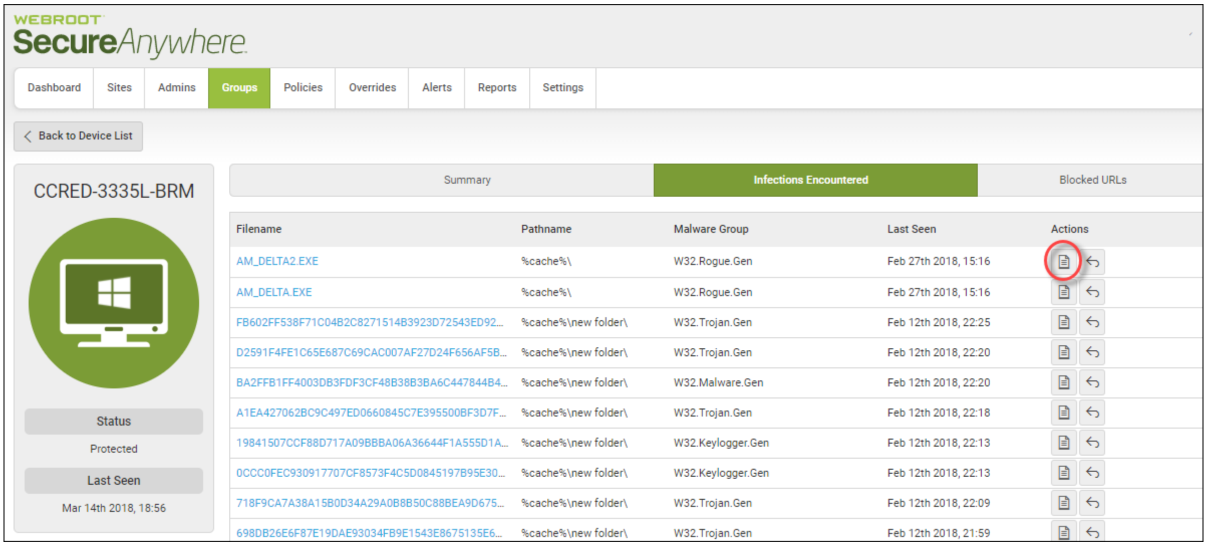
CCRED-3335L-BRM

Status: Protected

Last Seen: Mar 14th 2018, 18:56

| Filename | Pathname | Malware Group | Last Seen | Actions |
|---|---|---|---|---|
| AM_DELTA2.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↶ |
| AM_DELTA.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↶ |
| FB602FF538F71C04B2C8271514B3923D72543ED92... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:25 | 🗎 ↶ |
| D2591F4FE1C65E687C69CAC007AF27D24F656AF5B... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:20 | 🗎 ↶ |
| BA2FFB1FF4003DB3FDF3CF48B38B3BA6C447844B4... | %cache%\new folder\ | W32.Malware.Gen | Feb 12th 2018, 22:20 | 🗎 ↶ |
| A1EA427062BC9C497ED0660845C7E395500BF3D7F... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:18 | 🗎 ↶ |
| 19841507CCF88D717A09BBBA06A36644F1A555D1A... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↶ |
| 0CCC0FEC930917707CF8573F4C5D0845197B95E30... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↶ |
| 718F9CA7A38A15B0D34A29A0B8B50C88BEA9D675... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:09 | 🗎 ↶ |
| 698DB26E6F87E19DAE93034FB9E1543E8675135E6... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 21:59 | 🗎 ↶ |

5. For the file you want to whitelist, click the **Whitelist Files** icon.



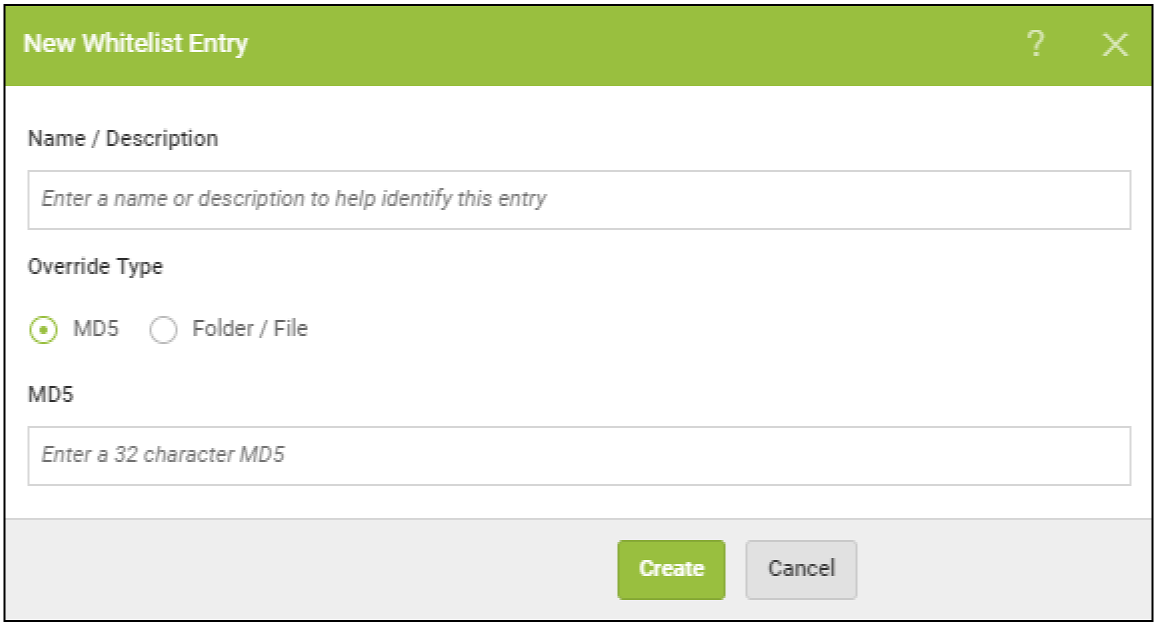
CCRED-3335L-BRM

Status: Protected

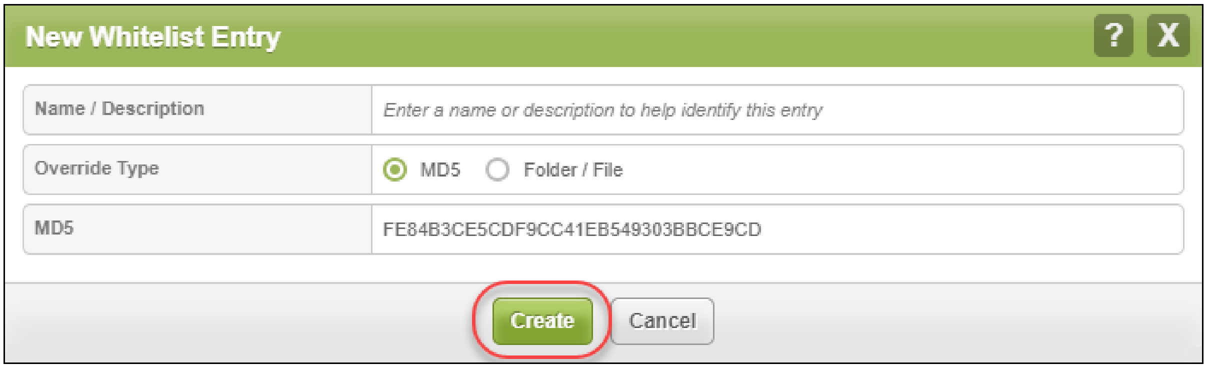
Last Seen: Mar 14th 2018, 18:56

| Filename | Pathname | Malware Group | Last Seen | Actions |
|---|---|---|---|---|
| AM_DELTA2.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↶ |
| AM_DELTA.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↶ |
| FB602FF538F71C04B2C8271514B3923D72543ED92... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:25 | 🗎 ↶ |
| D2591F4FE1C65E687C69CAC007AF27D24F656AF5B... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:20 | 🗎 ↶ |
| BA2FFB1FF4003DB3FDF3CF48B38B3BA6C447844B4... | %cache%\new folder\ | W32.Malware.Gen | Feb 12th 2018, 22:20 | 🗎 ↶ |
| A1EA427062BC9C497ED0660845C7E395500BF3D7F... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:18 | 🗎 ↶ |
| 19841507CCF88D717A09BBBA06A36644F1A555D1A... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↶ |
| 0CCC0FEC930917707CF8573F4C5D0845197B95E30... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↶ |
| 718F9CA7A38A15B0D34A29A0B8B50C88BEA9D675... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:09 | 🗎 ↶ |
| 698DB26E6F87E19DAE93034FB9E1543E8675135E6... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 21:59 | 🗎 ↶ |

6. In the Name/Description field, enter a name for the file.



7. In the Override Type area, select one of the following radio buttons:
   - **MD5**
   - **Folder/File**
8. The MD5 field displays the MD5 information.
9. When you're done, click the **Create** button.



| | |
|---|---|
| MD5 | FE84B3CE5CDF9CC41EB549303BBCE9CD |

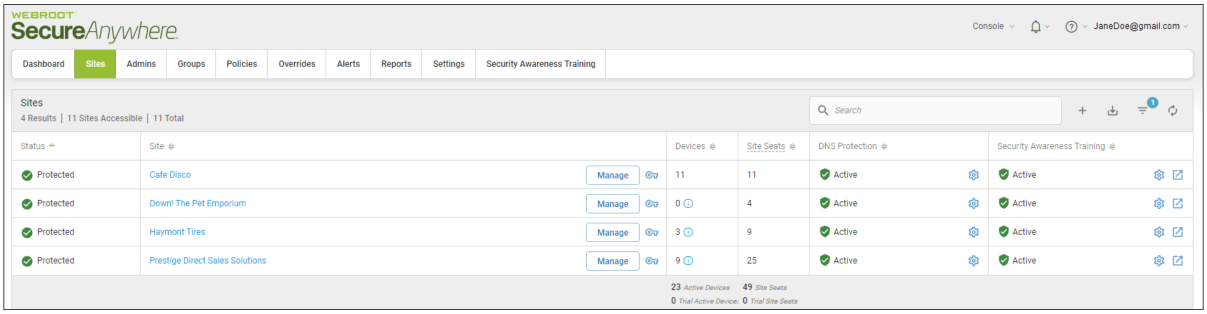
# Restoring Files From Quarantine

Any device, regardless of its status, can have files that have been quarantined. Follow this procedure to restore a file from quarantine.

**To restore a file from quarantine on a device:**

1. Log in to the management console.

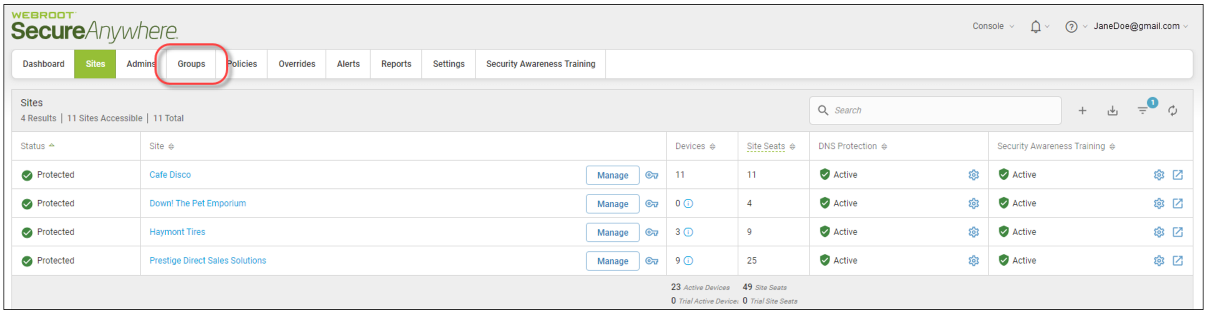
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

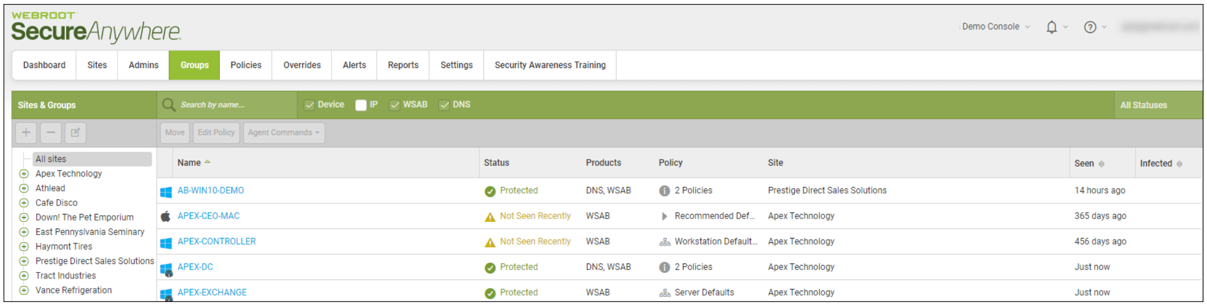
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

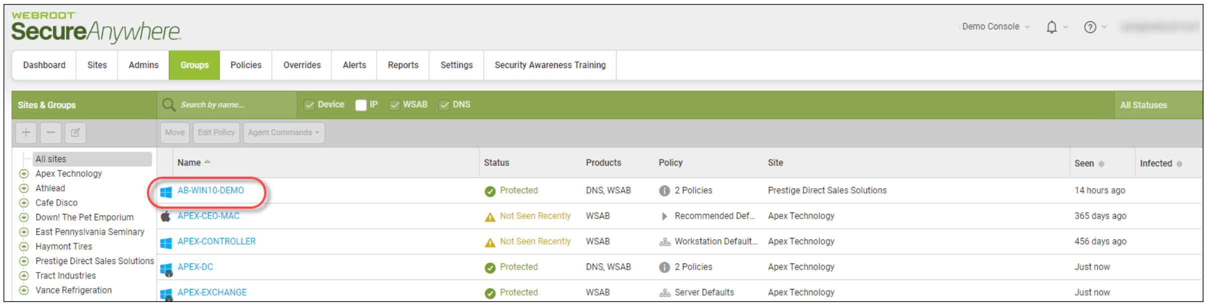
   The Groups tab displays.



- All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennsylvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. Select the device that has blocked URLs that you want to override.

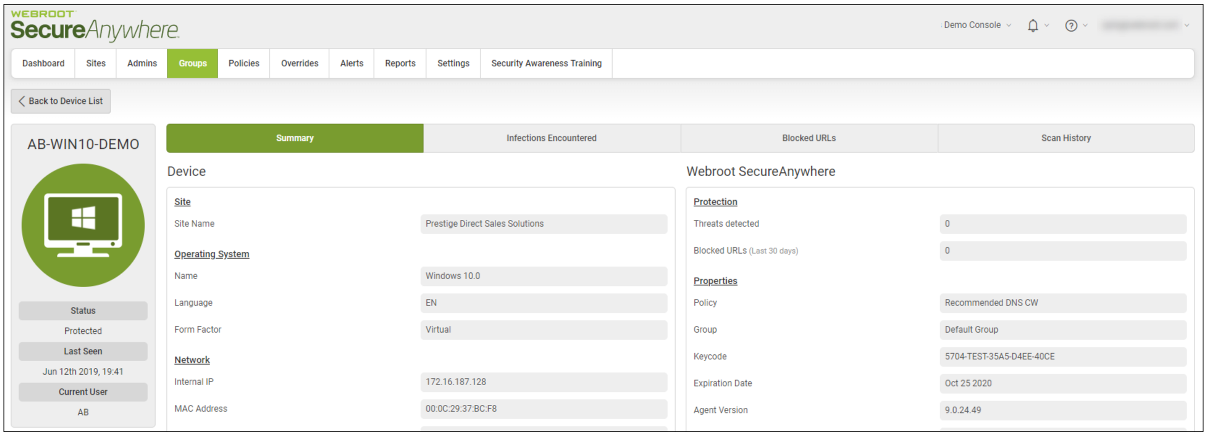


- All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennsylvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

**Note:** The example shows a device with a Protected status however you can restore files on devices regardless of their status.

The Status Panel for the device you selected displays.



AB-WIN10-DEMO

Status: Protected
Last Seen: Jun 12th 2019, 19:41
Current User: AB

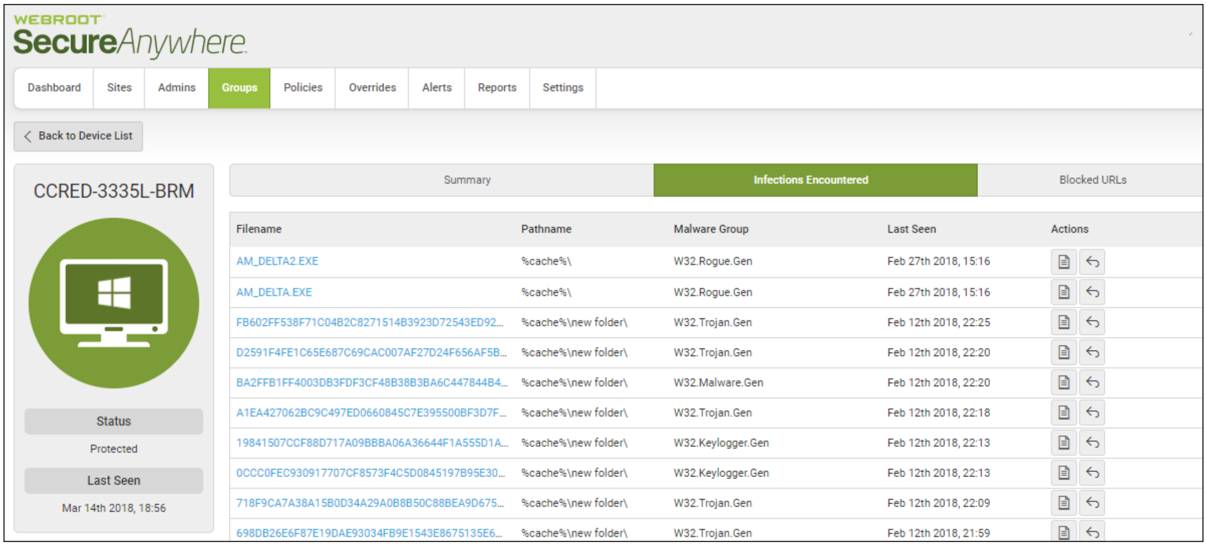
Device

| | |
|---|---|
| **Site** | |
| Site Name | Prestige Direct Sales Solutions |
| **Operating System** | |
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Virtual |
| **Network** | |
| Internal IP | 172.16.187.128 |
| MAC Address | 00:0C:29:37:BC:F8 |

Webroot SecureAnywhere

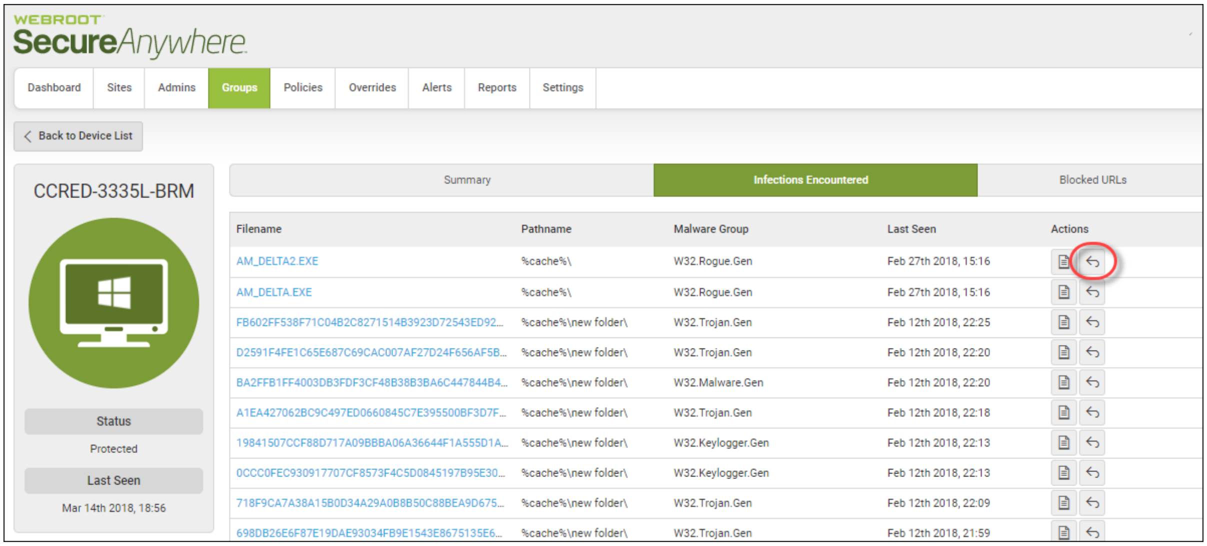
| | |
|---|---|
| **Protection** | |
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |
| **Properties** | |
| Policy | Recommended DNS CW |
| Group | Default Group |
| Keycode | 5704-TEST-35A5-D4EE-40CE |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |

4. Click the **Infections Encountered** tab.



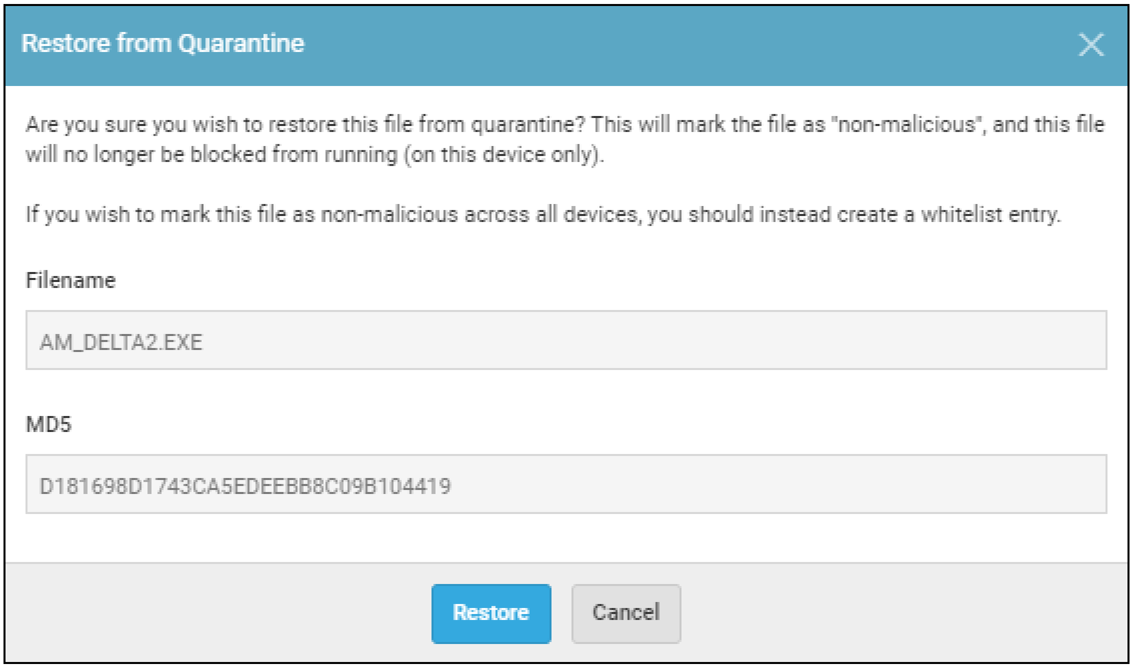
| Filename | Pathname | Malware Group | Last Seen | Actions |
|---|---|---|---|---|
| AM_DELTA2.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↩ |
| AM_DELTA.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↩ |
| FB602FF538F71C04B2C8271514B3923D72543ED92... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:25 | 🗎 ↩ |
| D2591F4FE1C65E687C69CAC007AF27D24F656AF5B... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:20 | 🗎 ↩ |
| BA2FFB1FF4003DB3FDF3CF48B38B3BA6C447844B4... | %cache%\new folder\ | W32.Malware.Gen | Feb 12th 2018, 22:20 | 🗎 ↩ |
| A1EA427062BC9C497ED0660845C7E395500BF3D7F... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:18 | 🗎 ↩ |
| 19841507CCF88D717A09BBBA06A36644F1A555D1A... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↩ |
| 0CCC0FEC930917707CF8573F4C5D0845197B95E30... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↩ |
| 718F9CA7A38A15B0D34A29A0B8B50C88BEA9D675... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:09 | 🗎 ↩ |
| 698DB26E6F87E19DAE93034FB9E1543E8675135E6... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 21:59 | 🗎 ↩ |

5. Click the **Restore Files** icon.



| Filename | Pathname | Malware Group | Last Seen | Actions |
|---|---|---|---|---|
| AM_DELTA2.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↩ |
| AM_DELTA.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↩ |
| FB602FF538F71C04B2C8271514B3923D72543ED92... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:25 | 🗎 ↩ |
| D2591F4FE1C65E687C69CAC007AF27D24F656AF5B... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:20 | 🗎 ↩ |
| BA2FFB1FF4003DB3FDF3CF48B38B3BA6C447844B4... | %cache%\new folder\ | W32.Malware.Gen | Feb 12th 2018, 22:20 | 🗎 ↩ |
| A1EA427062BC9C497ED0660845C7E395500BF3D7F... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:18 | 🗎 ↩ |
| 19841507CCF88D717A09BBBA06A36644F1A555D1A... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↩ |
| 0CCC0FEC930917707CF8573F4C5D0845197B95E30... | %cache%\new folder\ | W32.Keylogger.Gen | Feb 12th 2018, 22:13 | 🗎 ↩ |
| 718F9CA7A38A15B0D34A29A0B8B50C88BEA9D675... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 22:09 | 🗎 ↩ |
| 698DB26E6F87E19DAE93034FB9E1543E8675135E6... | %cache%\new folder\ | W32.Trojan.Gen | Feb 12th 2018, 21:59 | 🗎 ↩ |

The Restore From Quarantine window displays, with the file name and the MD5 information displayed in the fields.



Restore from Quarantine

Are you sure you wish to restore this file from quarantine? This will mark the file as "non-malicious", and this file will no longer be blocked from running (on this device only).

If you wish to mark this file as non-malicious across all devices, you should instead create a whitelist entry.

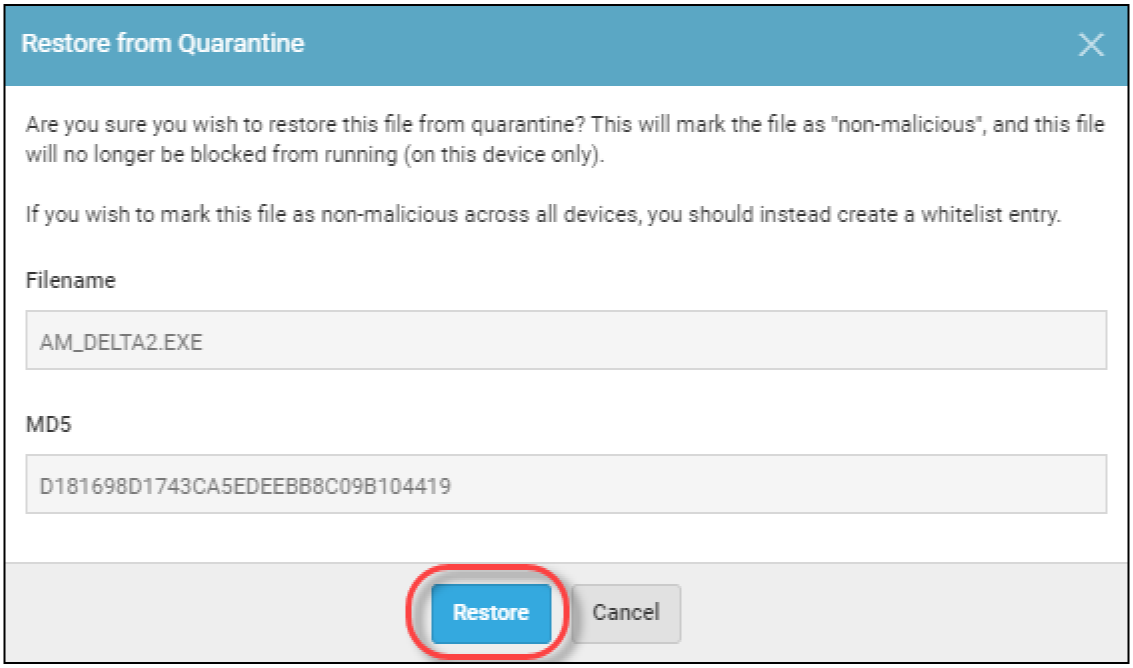
Filename

AM_DELTA2.EXE

MD5

D181698D1743CA5EDEEBB8C09B104419

6. To restore the file, click the **Restore** button.



Restore from Quarantine

Are you sure you wish to restore this file from quarantine? This will mark the file as "non-malicious", and this file will no longer be blocked from running (on this device only).

If you wish to mark this file as non-malicious across all devices, you should instead create a whitelist entry.

Filename

AM_DELTA2.EXE

MD5

D181698D1743CA5EDEEBB8C09B104419

The system restores the file to the device.

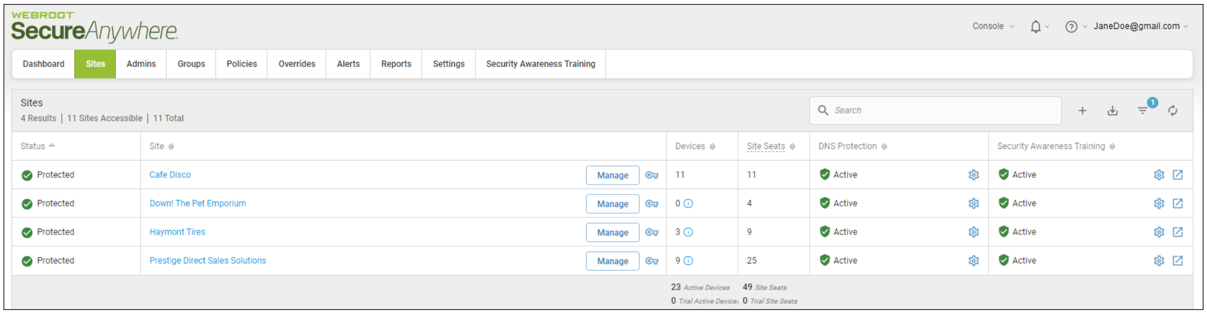
# Viewing Protected Devices

Follow this procedure to view information about devices with a status of Protected.

### To view a protected device:

1. Log in to the management console.

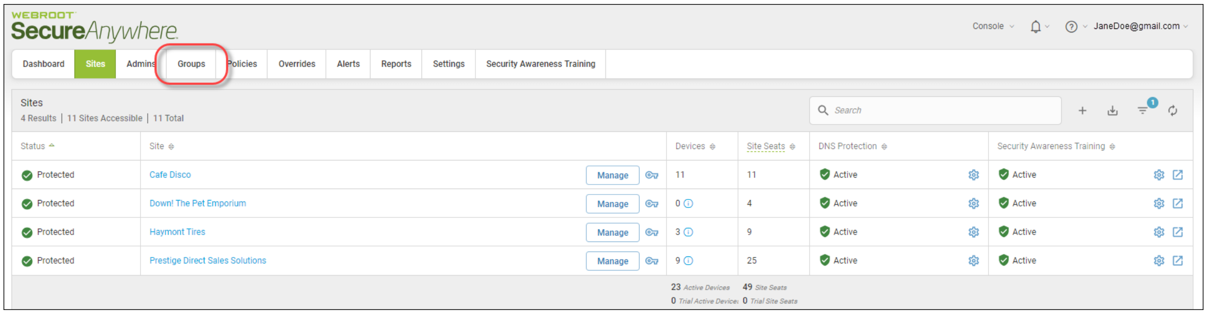
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

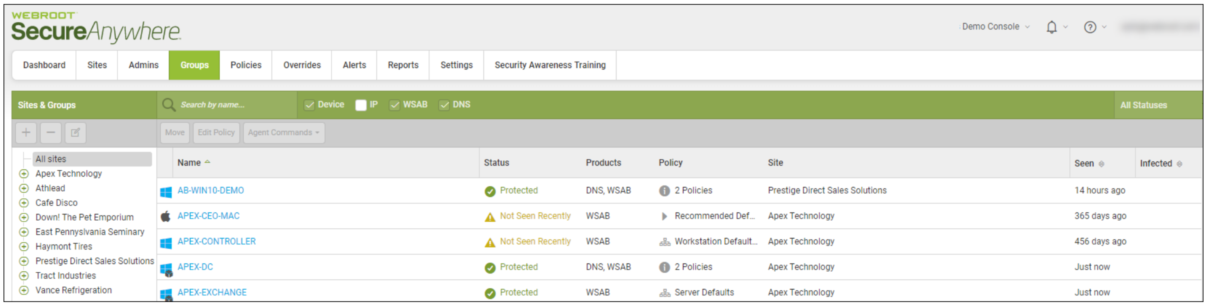
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

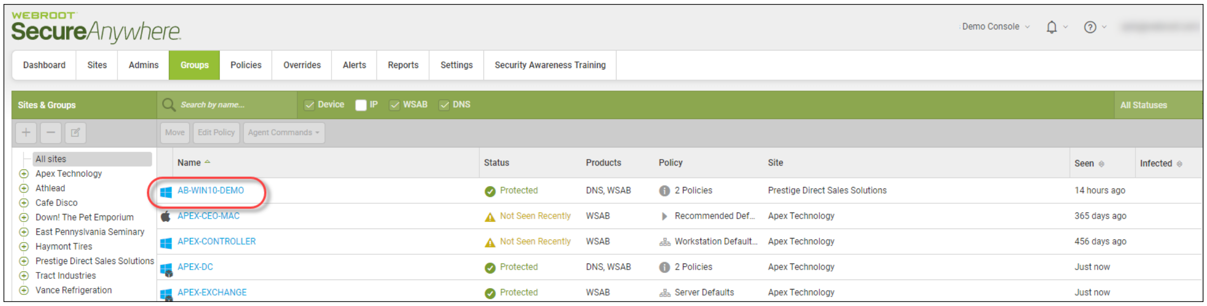
The Groups tab displays.



All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

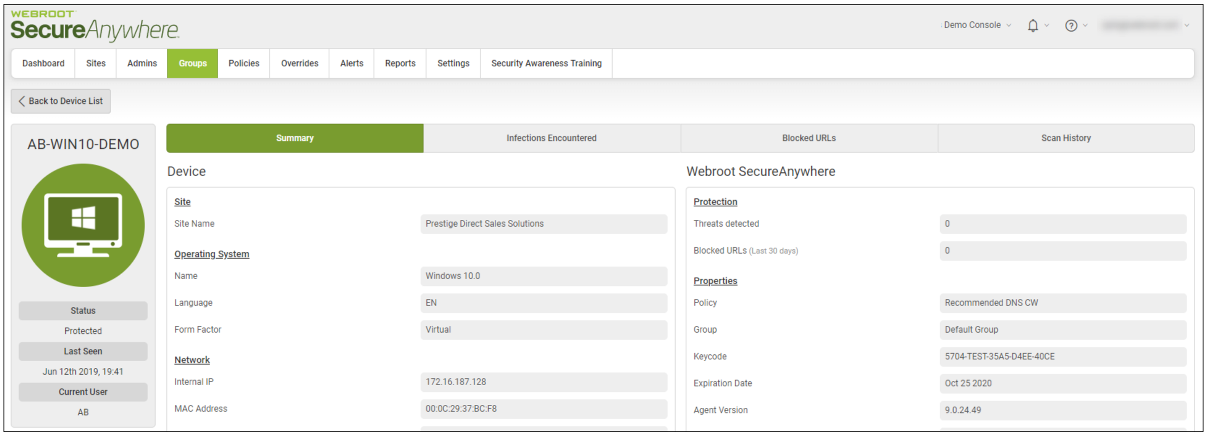
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. Select a device with the status of Protected that you want to view, and double-click.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The Status Panel for the device you selected displays.



AB-WIN10-DEMO

Status: Protected
Last Seen: Jun 12th 2019, 19:41
Current User: AB

Device

Site
Site Name: Prestige Direct Sales Solutions

Operating System
Name: Windows 10.0
Language: EN
Form Factor: Virtual

Network
Internal IP: 172.16.187.128
MAC Address: 00:0C:29:37:BC:F8

Webroot SecureAnywhere

Protection
Threats detected: 0
Blocked URLs (Last 30 days): 0

Properties
Policy: Recommended DNS CW
Group: Default Group
Keycode: 5704-TEST-35A5-D4EE-40CE
Expiration Date: Oct 25 2020
Agent Version: 9.0.24.49

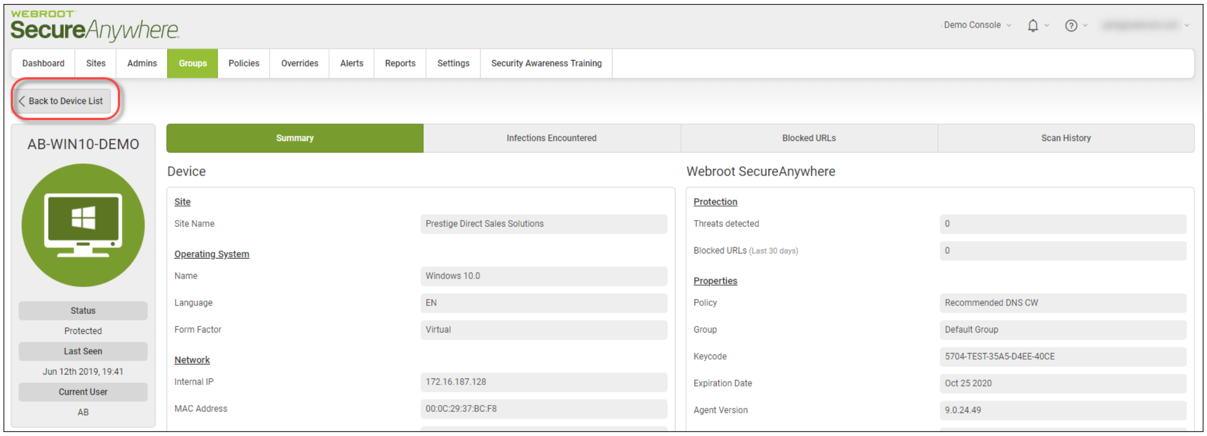
4. The Device Info column on the left displays the name of the device, as well as the following information:
   - **Status** — The status of the device. For more information, see *Device Management Overview on page 209*.
   - **Last Seen** — The date and time the last time the device checked in with the system.
   - **Current User** — The last name of the admin who is currently logged in and displaying the Status Panel.

   The main part of the panel displays information about the following:

   - **Site**
   - **Operating System**
   - **Network**

- **Protection**
- **Properties**
- **Shields**

5. Click any of the following three tabs for additional information:
   - **Summary** — Displays a summary of information about the device.
   - **Infections Encountered** — Displays a list of the infections encountered on this device.
   - **Blocked URLs** — Displays a list of any URLs that were blocked by the Web Threat Shield program. From this tab you can also add a web override to any URL that you don't want blocked. For more information, see *Adding Web Overrides to Devices on page 219*.
   - **Scan History** — Displays a list of every scan that has taken place for a particular device, including any threats that have been found during the scan. For more information, see *Displaying Scan Histories on page 277*.
6. When you're done, click the **Back to Device List** button.



AB-WIN10-DEMO

Status: Protected
Last Seen: Jun 12th 2019, 19:41
Current User: AB

Device

Site
Site Name: Prestige Direct Sales Solutions

Operating System
Name: Windows 10.0
Language: EN
Form Factor: Virtual

Network
Internal IP: 172.16.187.128
MAC Address: 00:0C:29:37:BC:F8

Webroot SecureAnywhere

Protection
Threats detected: 0
Blocked URLs (Last 30 days): 0

Properties
Policy: Recommended DNS CW
Group: Default Group
Keycode: 5704-TEST-35A5-D4EE-40CE
Expiration Date: Oct 25 2020
Agent Version: 9.0.24.49

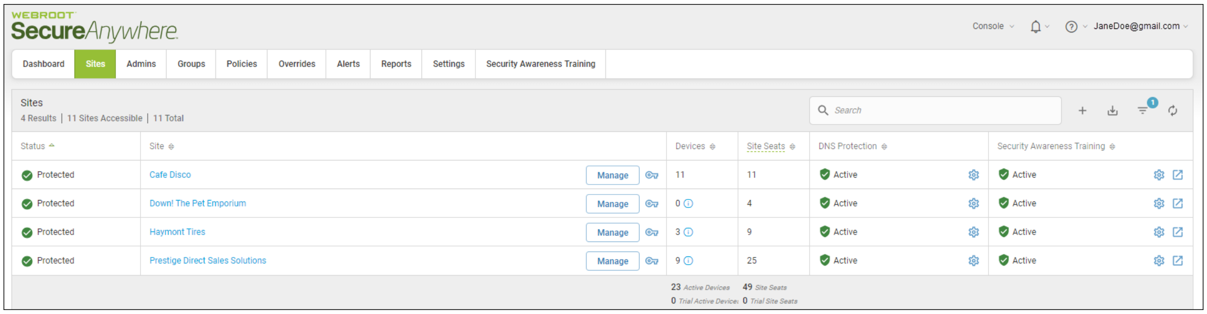
# Viewing Devices Not Seen Recently

Follow this procedure to view information about devices with a status of Not Seen Recently.

### To view a device that has not been seen recently:

1. Log in to the management console.

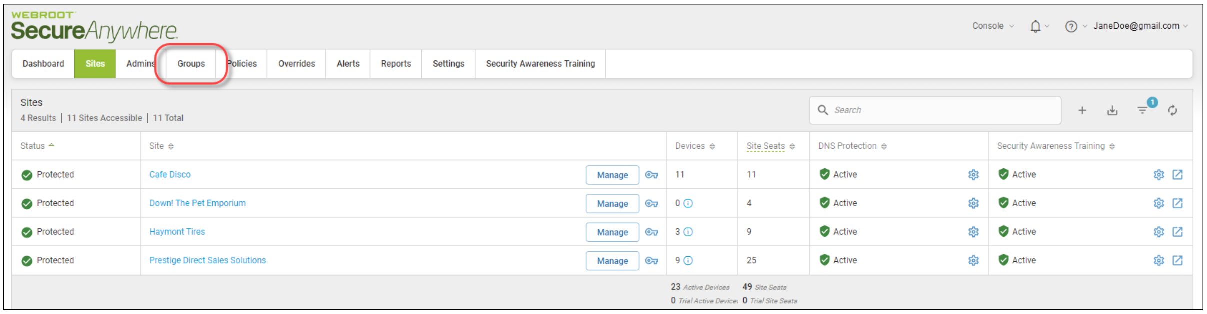
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

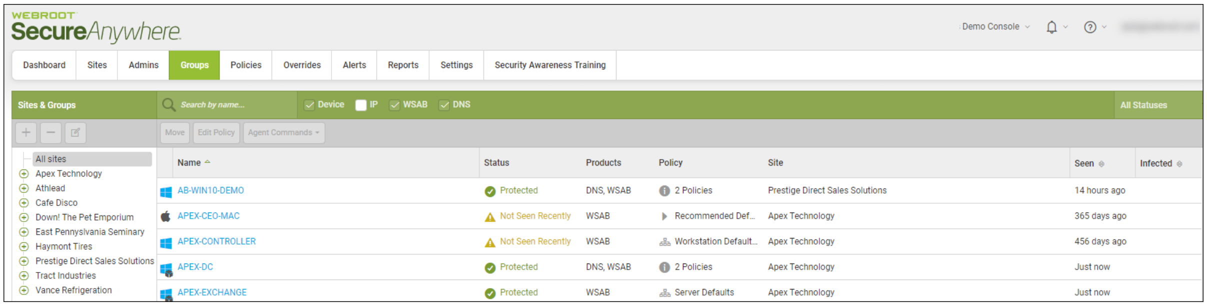
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

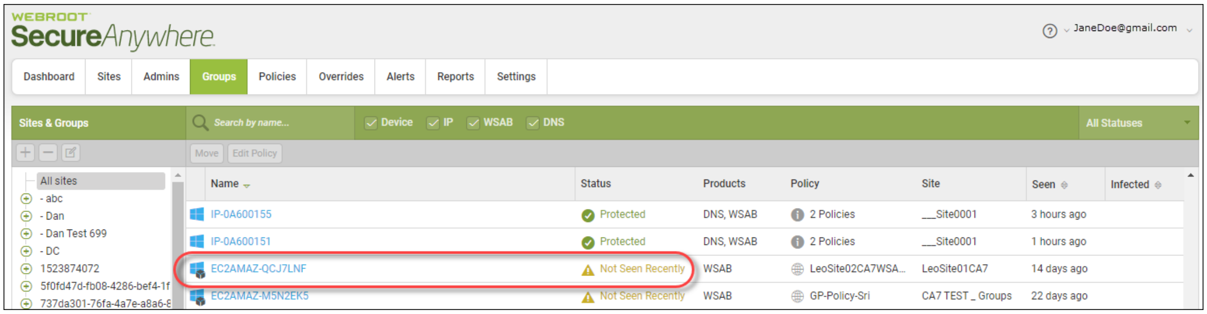
The Groups tab displays.



All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennysivania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

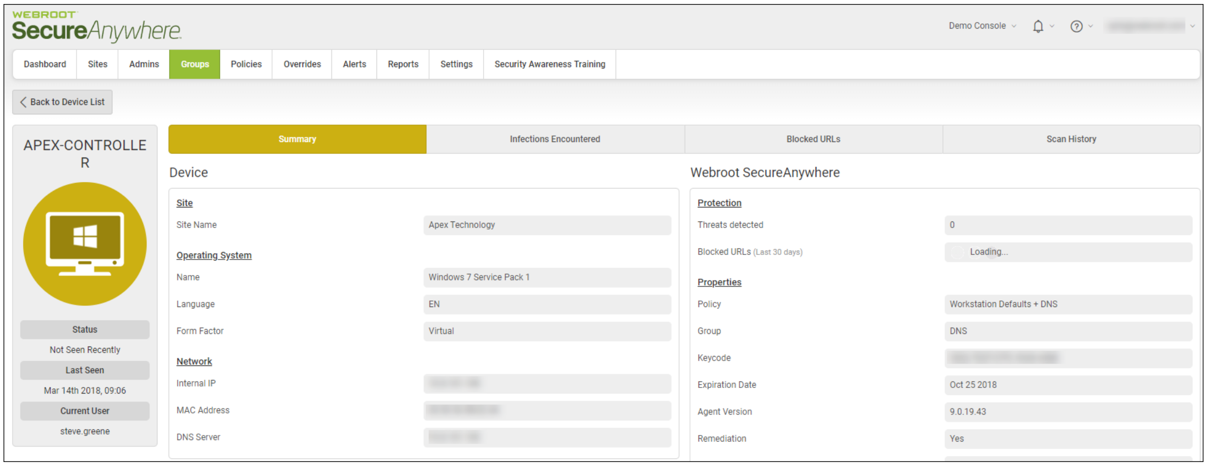
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. Select a device with the status of **Not Seen Recently** that you want to view, and double-click.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| IP-0A600155 | Protected | DNS, WSAB | 2 Policies | __Site0001 | 3 hours ago | |
| IP-0A600151 | Protected | DNS, WSAB | 2 Policies | __Site0001 | 1 hours ago | |
| EC2AMAZ-QCJ7LNF | Not Seen Recently | WSAB | LeoSite02CA7WSA... | LeoSite01CA7 | 14 days ago | |
| EC2AMAZ-M5N2EK5 | Not Seen Recently | WSAB | GP-Policy-Sri | CA7 TEST _ Groups | 22 days ago | |

The Status Panel for the device you selected displays.



[redacted]

APEX-CONTROLLE
R

Status
Not Seen Recently

Last Seen
Mar 14th 2018, 09:06

Current User
steve.greene

Device

Site

Site Name: Apex Technology

Operating System

Name: Windows 7 Service Pack 1
Language: EN
Form Factor: Virtual

Network

Internal IP: [redacted]
MAC Address: [redacted]
DNS Server: [redacted]

Webroot SecureAnywhere

Protection

Threats detected: 0
Blocked URLs (Last 30 days): Loading...

Properties

Policy: Workstation Defaults + DNS
Group: DNS
Keycode: [redacted]
Expiration Date: Oct 25 2018
Agent Version: 9.0.19.43
Remediation: Yes

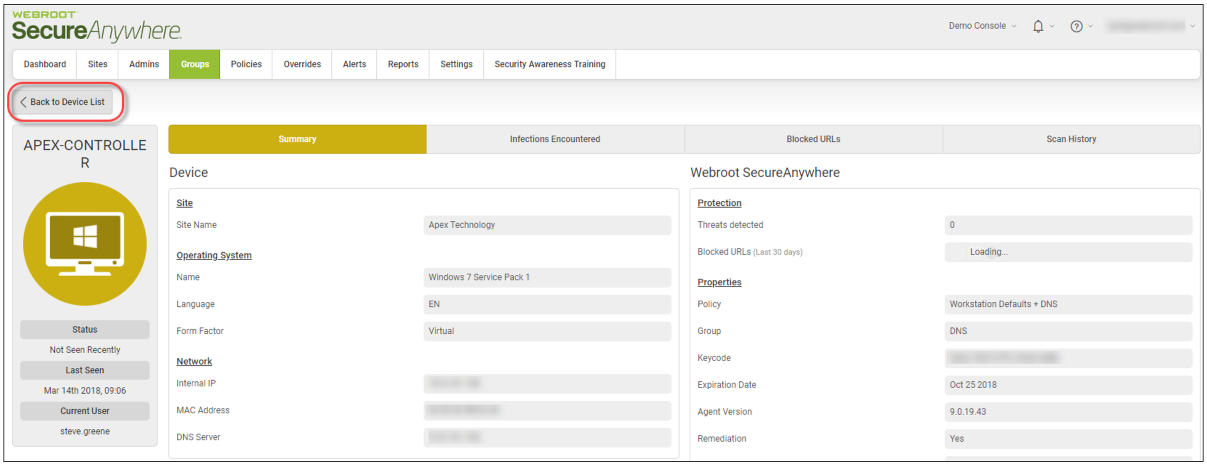
4. The Device Info column on the left displays the name of the device, as well as the following information:
   - **Status** — The status of the device. For more information, see *Device Management Overview on page 209*.
   - **Last Seen** — The date and time the last time the device checked in with the system.
   - **Current User** — The last name of the admin who is currently logged in and displaying the Status Panel.

The main part of the panel displays information about the following:

- **Site**
- **Operating System**

- **Network**
- **Protection**
- **Properties**
- **Shields**

5. Click any of the following three tabs for additional information:
   - **Summary** — Displays a summary of information about the device.
   - **Infections Encountered** — Displays a list of the infections encountered on this device.
   - **Blocked URLs** — Displays a list of any URLs that were blocked by the Web Threat Shield program. From this tab you can also add a web override to any URL that you don't want blocked. For more information, see *Adding Web Overrides to Devices on page 219*.
   - **Scan History** — Displays a list of every scan that has taken place for a particular device, including any threats that have been found during the scan. For more information, see *Displaying Scan Histories on page 277*.
6. When you're done, click the **Back to Device List** button.



APEX-CONTROLLER

Status
Not Seen Recently

Last Seen
Mar 14th 2018, 09:06

Current User
steve.greene

Device

Site
Site Name: Apex Technology

Operating System
Name: Windows 7 Service Pack 1
Language: EN
Form Factor: Virtual

Network
Internal IP: [redacted]
MAC Address: [redacted]
DNS Server: [redacted]

Webroot SecureAnywhere

Protection
Threats detected: 0
Blocked URLs (Last 30 days): Loading...

Properties
Policy: Workstation Defaults + DNS
Group: DNS
Keycode: [redacted]
Expiration Date: Oct 25 2018
Agent Version: 9.0.19.43
Remediation: Yes

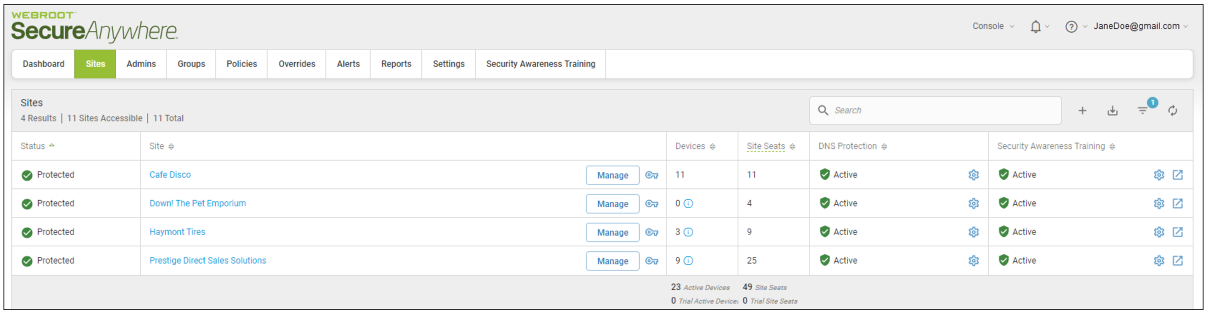
# Viewing Devices That Need Attention

Follow this procedure to view information about devices with a status of Needs Attention.

### To view a device that needs attention:

1. Log in to the management console.

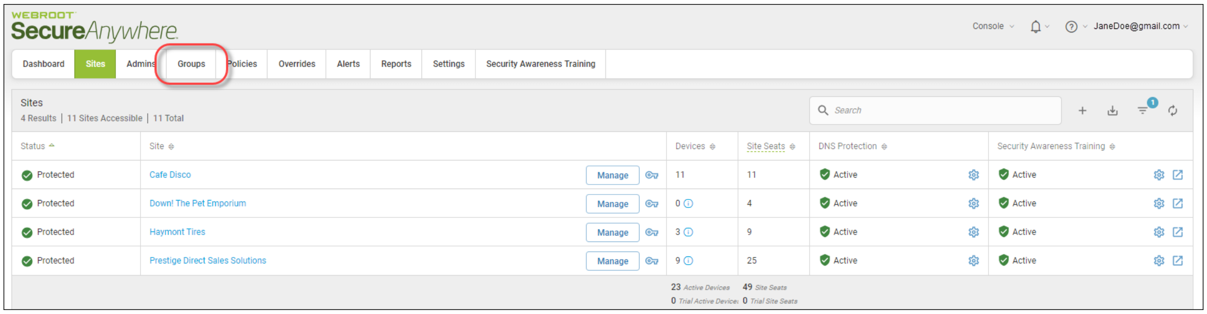
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

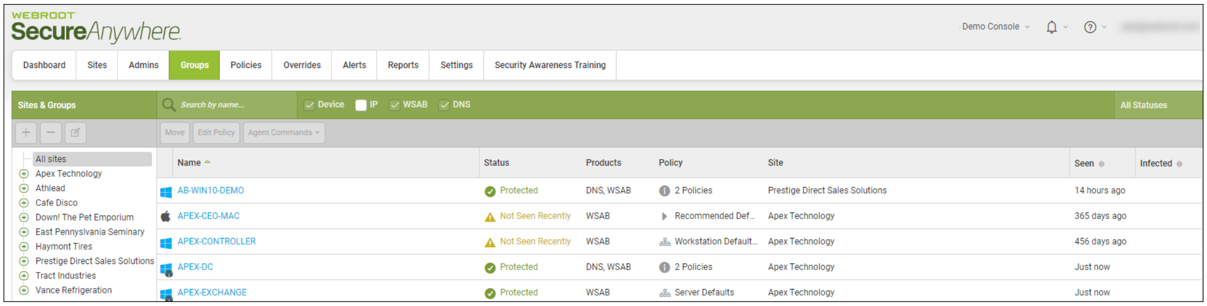
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

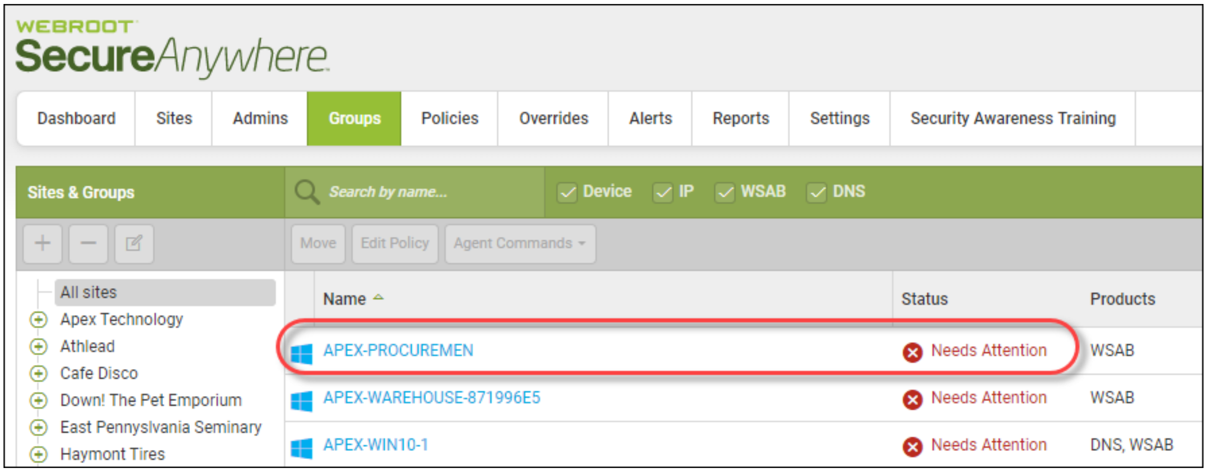
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



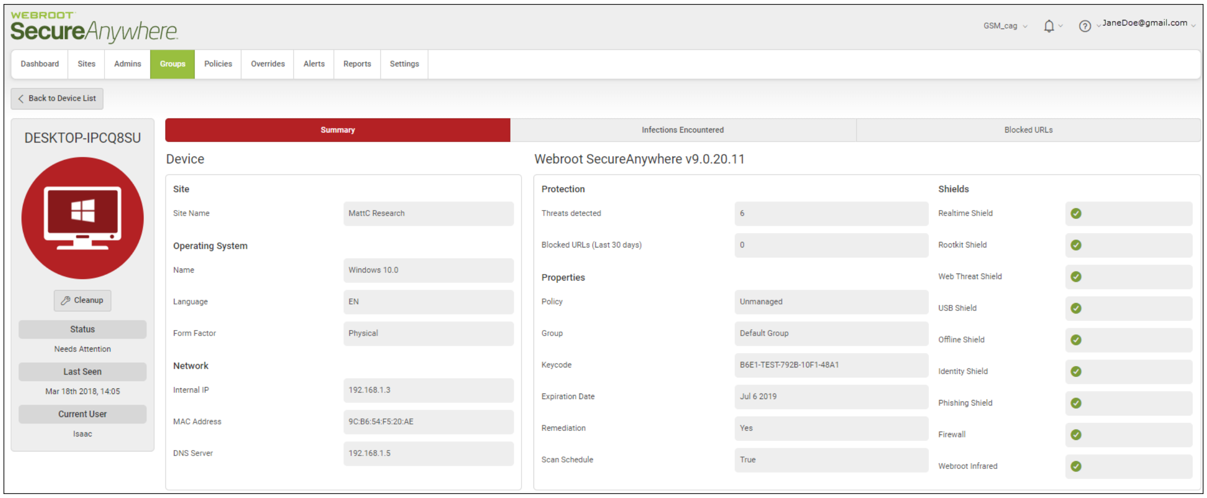
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. Select a device with the status of the Needs Attention that you want to view, and double-click.



| Name | Status | Products |
|---|---|---|
| APEX-PROCUREMEN | Needs Attention | WSAB |
| APEX-WAREHOUSE-871996E5 | Needs Attention | WSAB |
| APEX-WIN10-1 | Needs Attention | DNS, WSAB |

The Status Panel for the device you selected displays.



DESKTOP-IPCQ8SU

Status
Needs Attention

Last Seen
Mar 18th 2018, 14:05

Current User
Isaac

Device

**Site**

| | |
|---|---|
| Site Name | MattC Research |

**Operating System**

| | |
|---|---|
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Physical |

**Network**

| | |
|---|---|
| Internal IP | 192.168.1.3 |
| MAC Address | 9C:B6:54:F5:20:AE |
| DNS Server | 192.168.1.5 |

Webroot SecureAnywhere v9.0.20.11

**Protection**

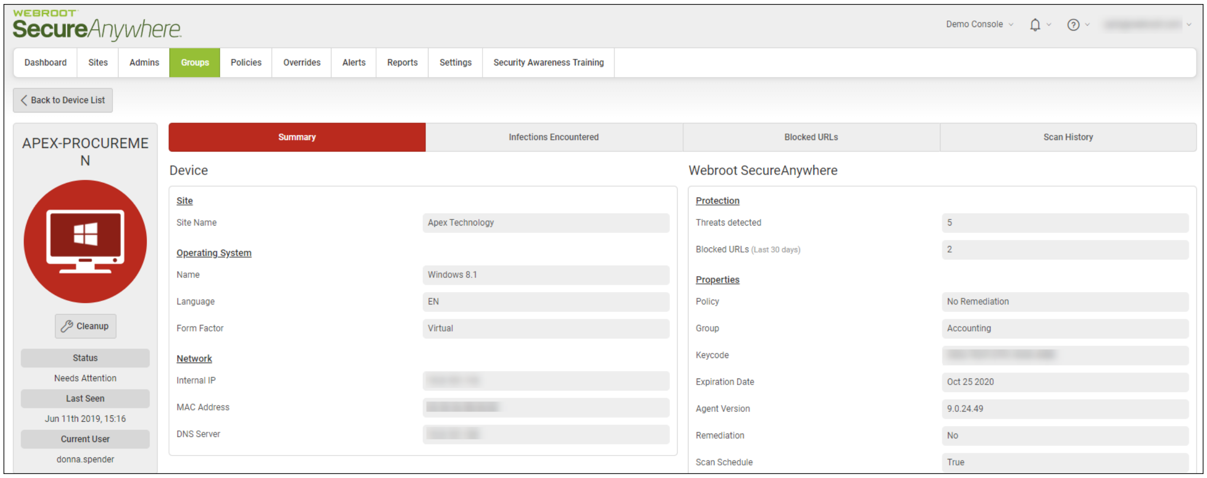
| | |
|---|---|
| Threats detected | 6 |
| Blocked URLs (Last 30 days) | 0 |

**Properties**

| | |
|---|---|
| Policy | Unmanaged |
| Group | Default Group |
| Keycode | B6E1-TEST-792B-10F1-48A1 |
| Expiration Date | Jul 6 2019 |
| Remediation | Yes |
| Scan Schedule | True |

**Shields**

| | |
|---|---|
| Realtime Shield | ✓ |
| Rootkit Shield | ✓ |
| Web Threat Shield | ✓ |
| USB Shield | ✓ |
| Offline Shield | ✓ |
| Identity Shield | ✓ |
| Phishing Shield | ✓ |
| Firewall | ✓ |
| Webroot Infrared | ✓ |



APEX-PROCUREME
N

Status
Needs Attention
Last Seen
Jun 11th 2019, 15:16
Current User
donna.spender

Device

Site

| | |
|---|---|
| Site Name | Apex Technology |

Operating System

| | |
|---|---|
| Name | Windows 8.1 |
| Language | EN |
| Form Factor | Virtual |

Network

| | |
|---|---|
| Internal IP | [redacted] |
| MAC Address | [redacted] |
| DNS Server | [redacted] |

Webroot SecureAnywhere

Protection

| | |
|---|---|
| Threats detected | 5 |
| Blocked URLs (Last 30 days) | 2 |

Properties

| | |
|---|---|
| Policy | No Remediation |
| Group | Accounting |
| Keycode | [redacted] |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |
| Remediation | No |
| Scan Schedule | True |

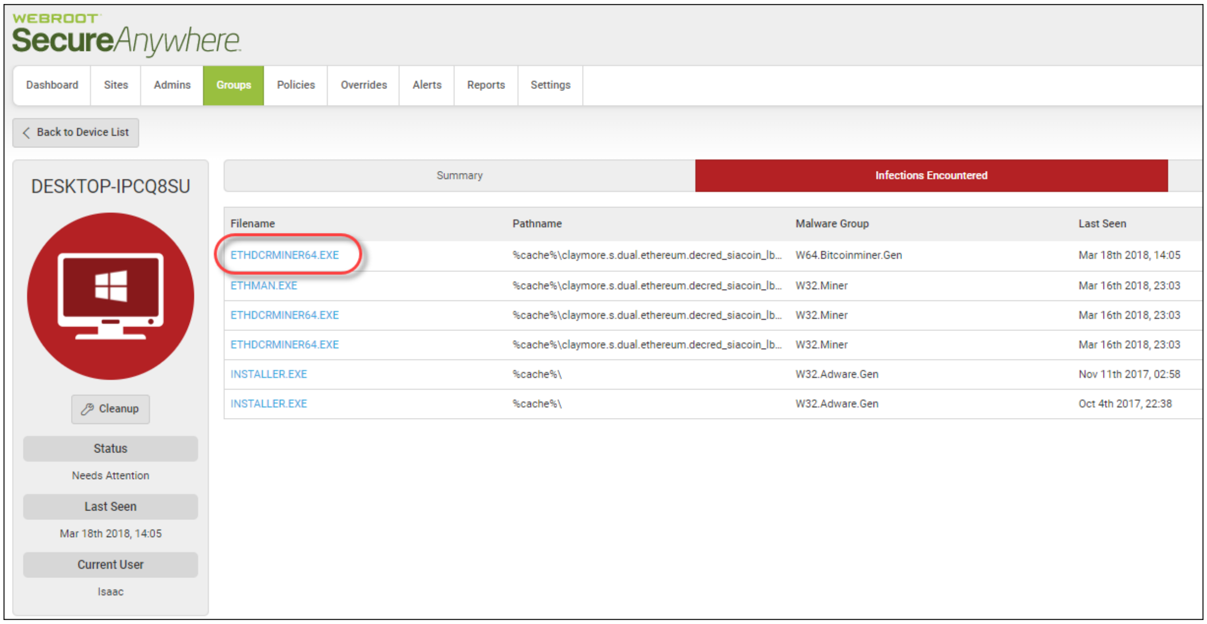
4. The Device Info column on the left displays the name of the device, as well as the following information:
   - **Status** — The status of the device. For more information, see *Device Management Overview on page 209*.
   - **Last Seen** — The date and time the last time the device checked in with the system.
   - **Current User** — The last name of the admin who is currently logged in and displaying the Status Panel.

   The main part of the panel displays information about the following:

   - **Site**
   - **Operating System**
   - **Network**
   - **Protection**
   - **Properties**
   - **Shields**
5. Click any of the following three tabs for additional information:
   - **Summary** — Displays a summary of information about the device.
   - **Infections Encountered** — Displays a list of the infections encountered on this device.
   - **Blocked URLs** — Displays a list of any URLs that were blocked by the Web Threat Shield program. From this tab you can also add a web override to any URL that you don't want blocked. For more information, see *Adding Web Overrides to Devices on page 219*.

- **Scan History** — Displays a list of every scan that has taken place for a particular device, including any threats that have been found during the scan. For more information, see *Displaying Scan Histories on page 277*.

6. To view detailed information about the infection, click the **Infections Encountered** tab, then click on the infection whose information you want to view.



DESKTOP-IPCQ8SU

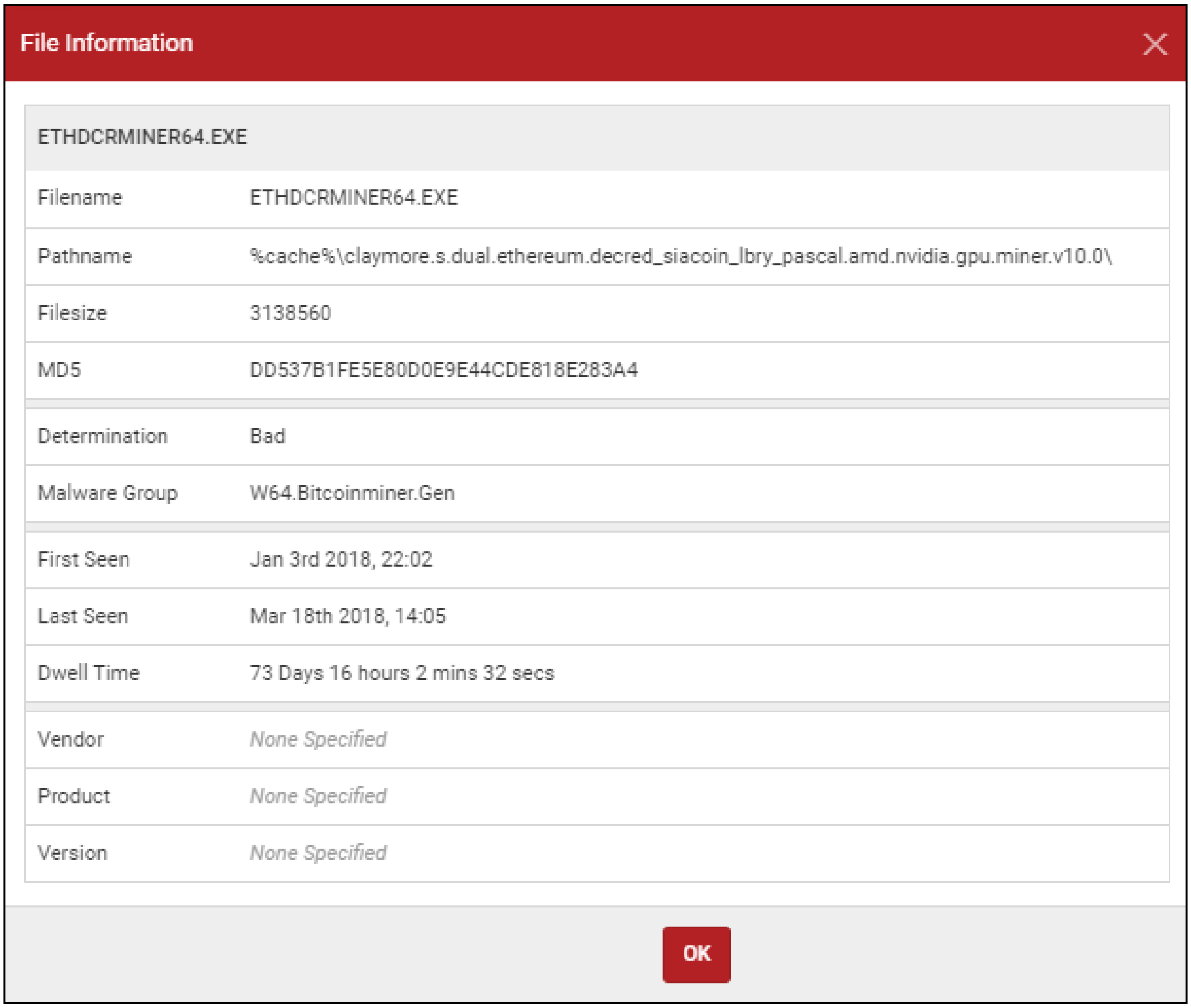
Status
Needs Attention

Last Seen
Mar 18th 2018, 14:05

Current User
Isaac

| Filename | Pathname | Malware Group | Last Seen |
|---|---|---|---|
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W64.Bitcoinminer.Gen | Mar 18th 2018, 14:05 |
| ETHMAN.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| INSTALLER.EXE | %cache%\ | W32.Adware.Gen | Nov 11th 2017, 02:58 |
| INSTALLER.EXE | %cache%\ | W32.Adware.Gen | Oct 4th 2017, 22:38 |

The File Information window displays.

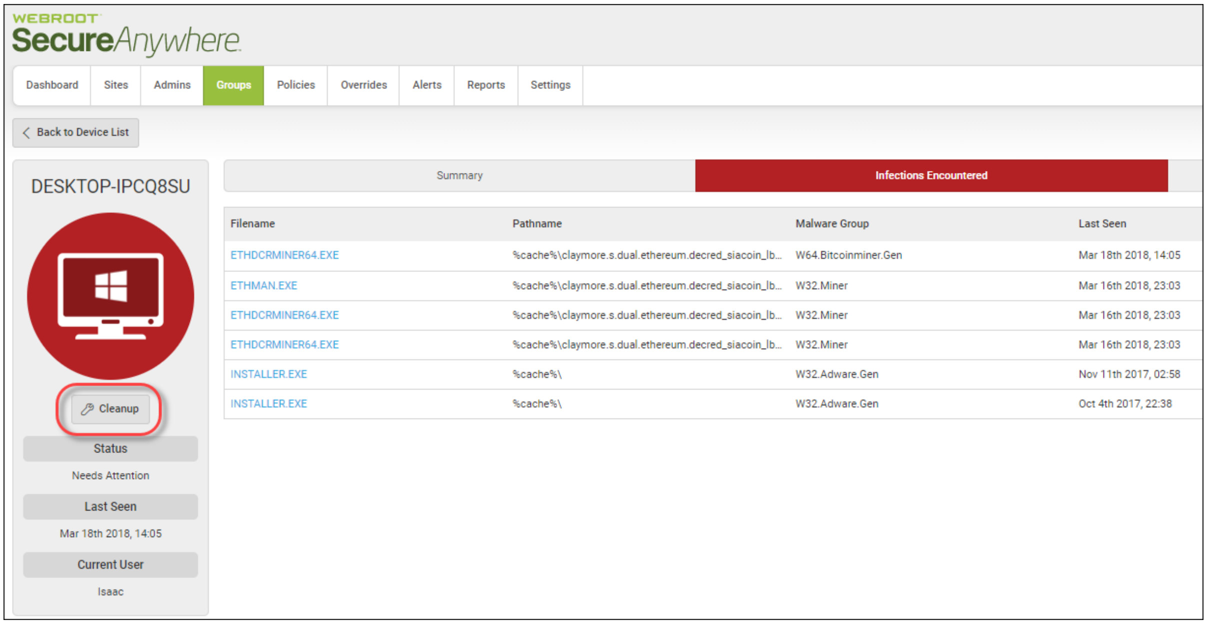


ETHDCRMINER64.EXE

| | |
|---|---|
| Filename | ETHDCRMINER64.EXE |
| Pathname | %cache%\claymore.s.dual.ethereum.decred_siacoin_lbry_pascal.amd.nvidia.gpu.miner.v10.0\ |
| Filesize | 3138560 |
| MD5 | DD537B1FE5E80D0E9E44CDE818E283A4 |
| Determination | Bad |
| Malware Group | W64.Bitcoinminer.Gen |
| First Seen | Jan 3rd 2018, 22:02 |
| Last Seen | Mar 18th 2018, 14:05 |
| Dwell Time | 73 Days 16 hours 2 mins 32 secs |
| Vendor | *None Specified* |
| Product | *None Specified* |
| Version | *None Specified* |

When you're done viewing the information, click the **OK** button.

7. To send a clean command to the device, click the **Cleanup** button.



DESKTOP-IPCQ8SU

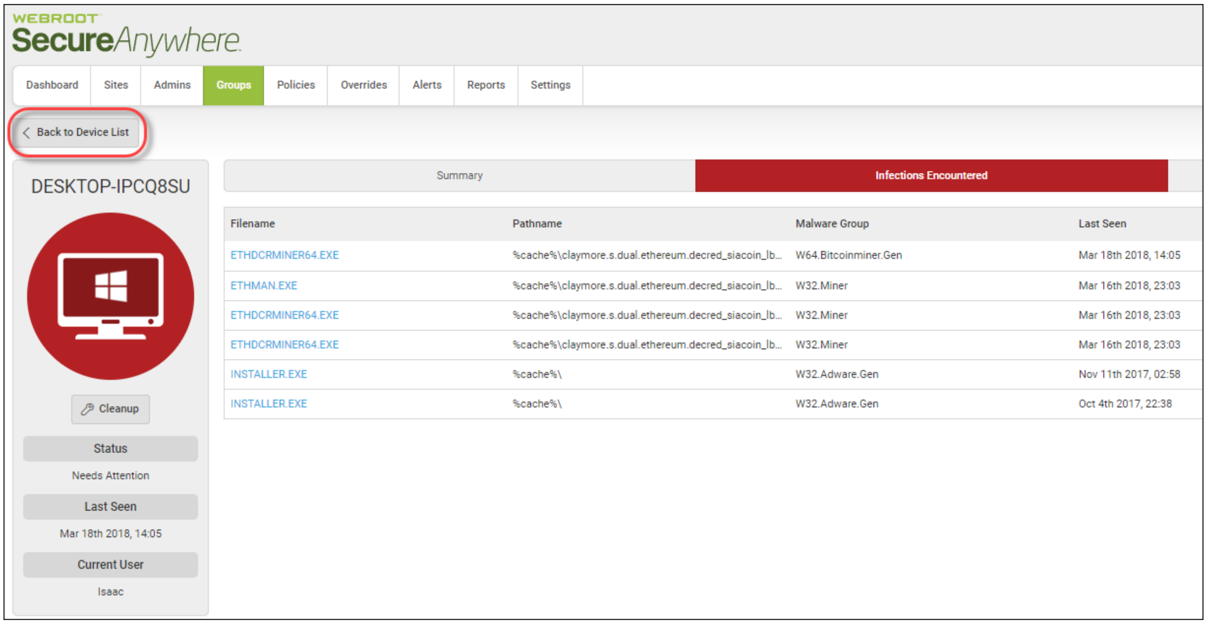
| Filename | Pathname | Malware Group | Last Seen |
|---|---|---|---|
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W64.Bitcoinminer.Gen | Mar 18th 2018, 14:05 |
| ETHMAN.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| INSTALLER.EXE | %cache%\ | W32.Adware.Gen | Nov 11th 2017, 02:58 |
| INSTALLER.EXE | %cache%\ | W32.Adware.Gen | Oct 4th 2017, 22:38 |

Status
Needs Attention

Last Seen
Mar 18th 2018, 14:05

Current User
Isaac

8. When you're done, click the **Back to Device List** button.



DESKTOP-IPCQ8SU

| Filename | Pathname | Malware Group | Last Seen |
|---|---|---|---|
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W64.Bitcoinminer.Gen | Mar 18th 2018, 14:05 |
| ETHMAN.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| ETHDCRMINER64.EXE | %cache%\claymore.s.dual.ethereum.decred_siacoin_lb... | W32.Miner | Mar 16th 2018, 23:03 |
| INSTALLER.EXE | %cache%\ | W32.Adware.Gen | Nov 11th 2017, 02:58 |
| INSTALLER.EXE | %cache%\ | W32.Adware.Gen | Oct 4th 2017, 22:38 |

Status
Needs Attention

Last Seen
Mar 18th 2018, 14:05

Current User
Isaac

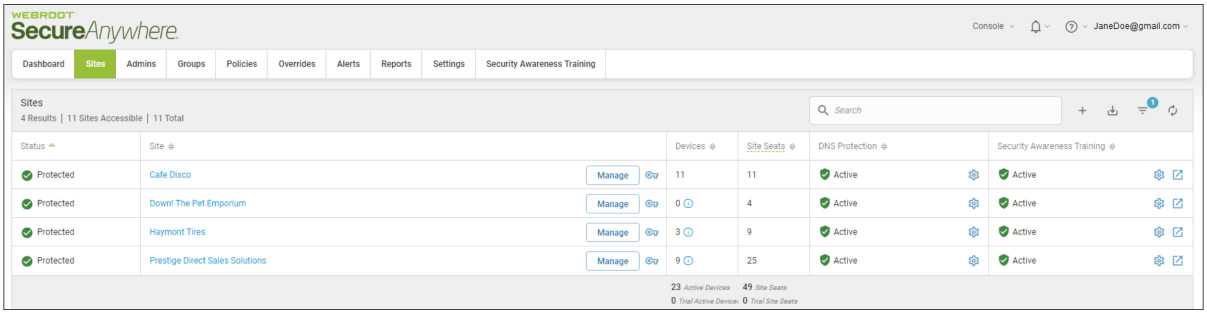
# Viewing Devices That Have Expired

Follow this procedure to view information about devices with a status of Expired.

### To view a protected device:

1. Log in to the management console.

   The management console displays, with the Sites tab active.

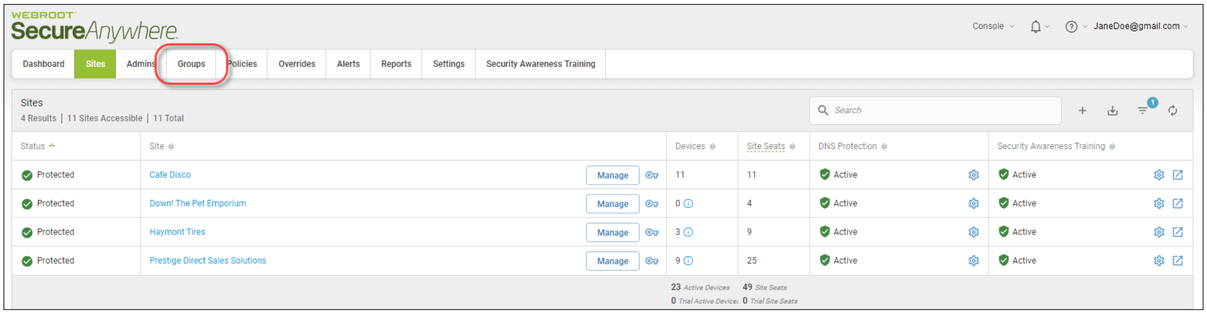


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |

23 *Active Devices* 49 *Site Seats*
0 *Trial Active Device:* 0 *Trial Site Seats*

2. Click the **Groups** tab.

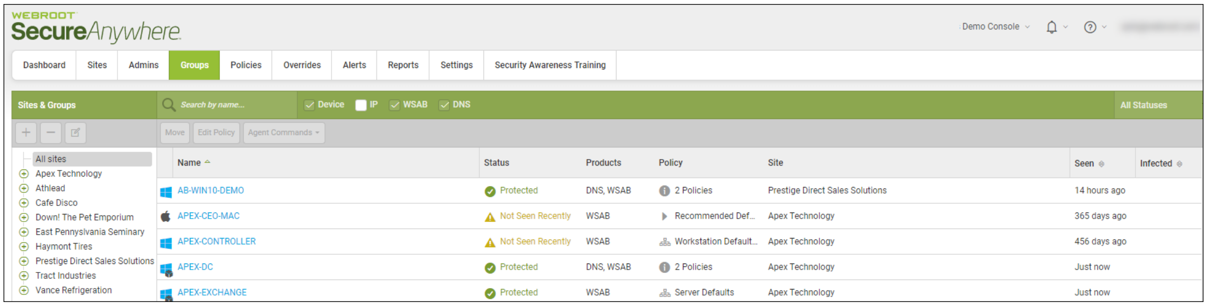


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |

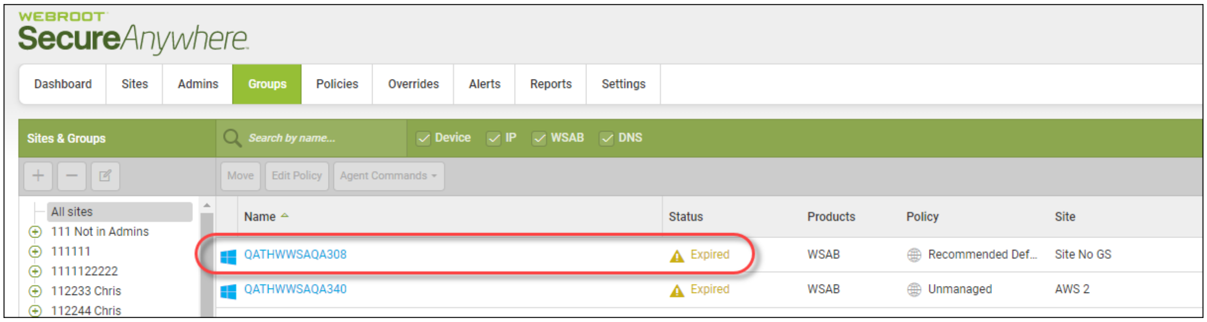
23 *Active Devices* 49 *Site Seats*
0 *Trial Active Device:* 0 *Trial Site Seats*

   The Groups tab displays.



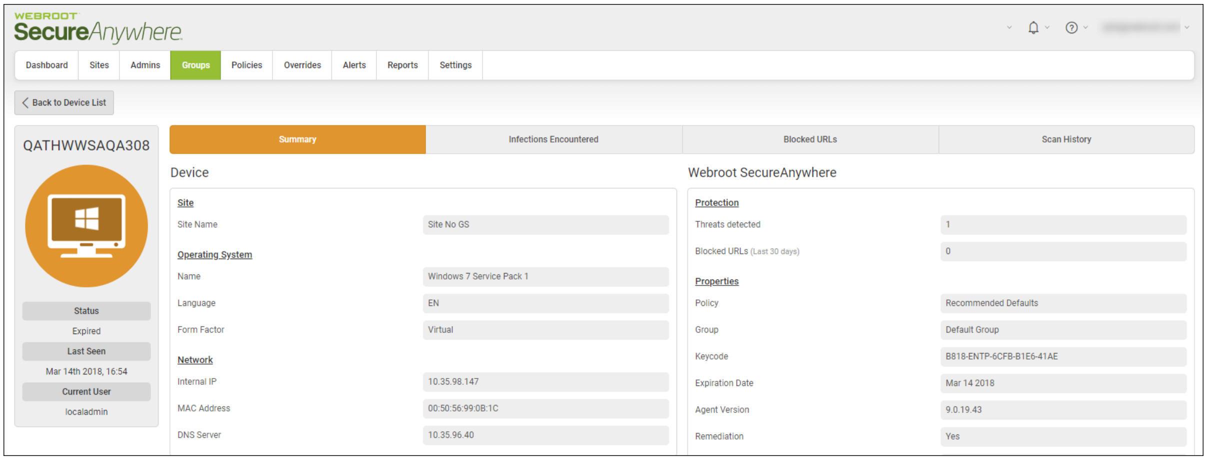
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. Select a device with the status of Expired that you want to view, and double-click.



| Name | Status | Products | Policy | Site |
|---|---|---|---|---|
| QATHWWSAQA308 | Expired | WSAB | Recommended Def... | Site No GS |
| QATHWWSAQA340 | Expired | WSAB | Unmanaged | AWS 2 |

The Status Panel for the device you selected displays.



QATHWWSAQA308

Status
Expired
Last Seen
Mar 14th 2018, 16:54
Current User
localadmin

Device

Site
Site Name: Site No GS

Operating System
Name: Windows 7 Service Pack 1
Language: EN
Form Factor: Virtual

Network
Internal IP: 10.35.98.147
MAC Address: 00:50:56:99:0B:1C
DNS Server: 10.35.96.40

Webroot SecureAnywhere

Protection
Threats detected: 1
Blocked URLs (Last 30 days): 0

Properties
Policy: Recommended Defaults
Group: Default Group
Keycode: B818-ENTP-6CFB-B1E6-41AE
Expiration Date: Mar 14 2018
Agent Version: 9.0.19.43
Remediation: Yes

4. The Device Info column on the left displays the name of the device, as well as the following information:

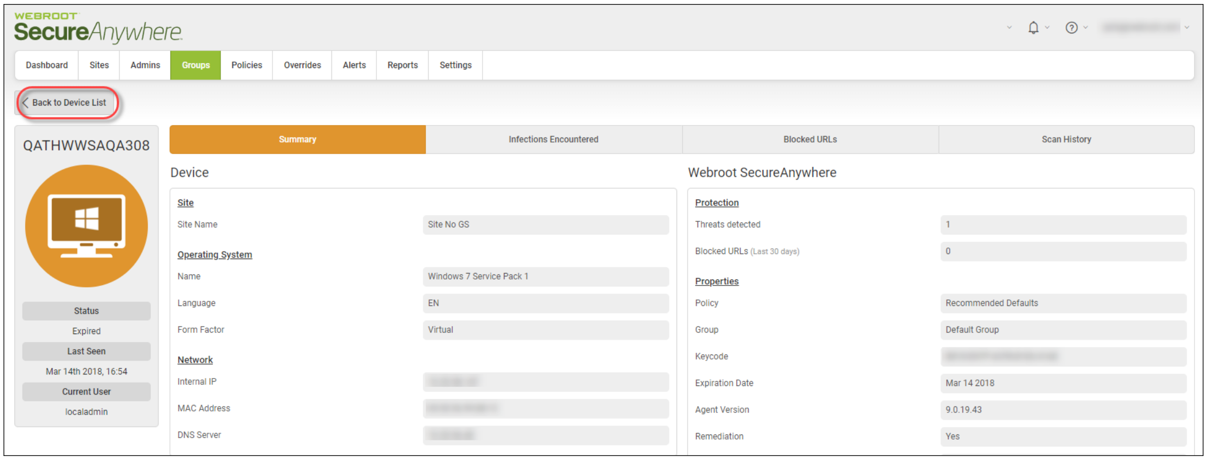
- **Status** — The status of the device. For more information, see *Device Management Overview on page 209*.
- **Last Seen** — The date and time the last time the device checked in with the system.
- **Current User** — The last name of the admin who is currently logged in and displaying the Status Panel.

The main part of the panel displays information about the following:

- **Site**
- **Operating System**

- **Network**
- **Protection**
- **Properties**
- **Shields**

5. Click any of the following three tabs for additional information:
   - **Summary** — Displays a summary of information about the device.
   - **Infections Encountered** — Displays a list of the infections encountered on this device.
   - **Blocked URLs** — Displays a list of any URLs that were blocked by the Web Threat Shield program. From this tab you can also add a web override to any URL that you don't want blocked. For more information, see *Adding Web Overrides to Devices on page 219*.
   - **Scan History** — Displays a list of every scan that has taken place for a particular device, including any threats that have been found during the scan. For more information, see *Displaying Scan Histories on page 277*.
6. When you're done, click the **Back to Device List** button.



QATHWWSAQA308

Status: Expired
Last Seen: Mar 14th 2018, 16:54
Current User: localadmin

Device

Site
Site Name: Site No GS

Operating System
Name: Windows 7 Service Pack 1
Language: EN
Form Factor: Virtual

Network
Internal IP: [redacted]
MAC Address: [redacted]
DNS Server: [redacted]

Webroot SecureAnywhere

Protection
Threats detected: 1
Blocked URLs (Last 30 days): 0

Properties
Policy: Recommended Defaults
Group: Default Group
Keycode: [redacted]
Expiration Date: Mar 14 2018
Agent Version: 9.0.19.43
Remediation: Yes

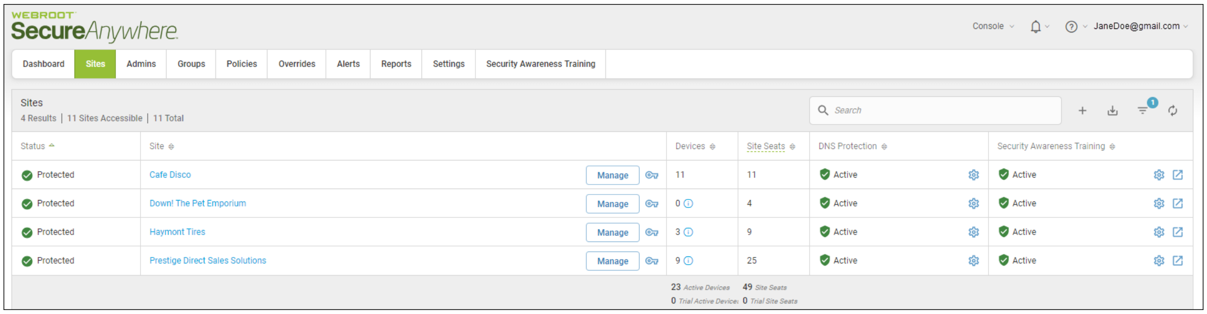
# Viewing Devices That Need Attention And Are Expired

Follow this procedure to view information about devices with a status of Attention & Expired.

**To view a device that needs attention and is expired:**

1. Log in to the management console.

   The management console displays, with the Sites tab active.

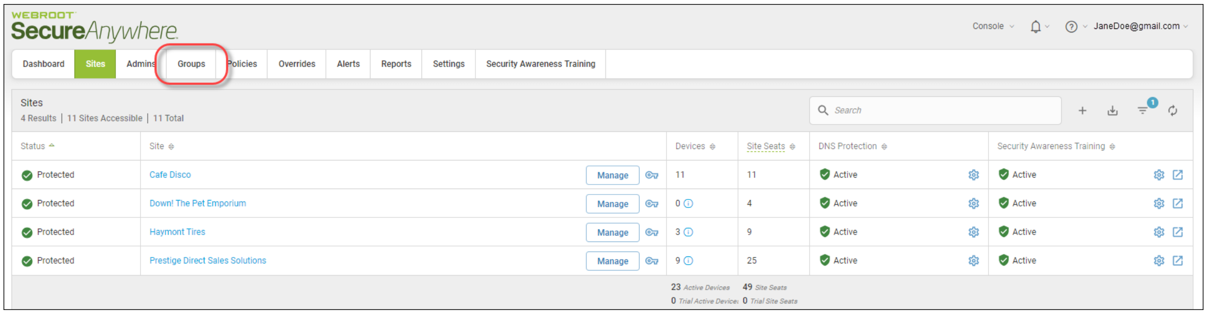


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |

23 *Active Devices* 49 *Site Seats*
0 *Trial Active Devices* 0 *Trial Site Seats*

2. Click the **Devices** tab.

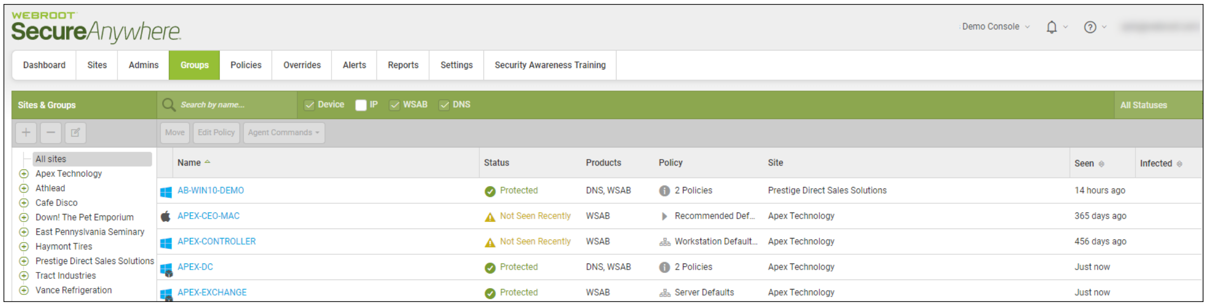


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |

23 *Active Devices* 49 *Site Seats*
0 *Trial Active Devices* 0 *Trial Site Seats*

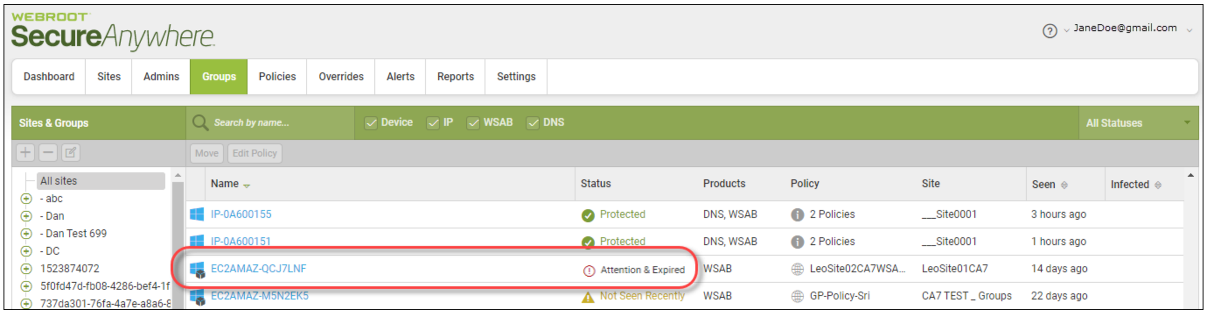
The Groups tab displays.



All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

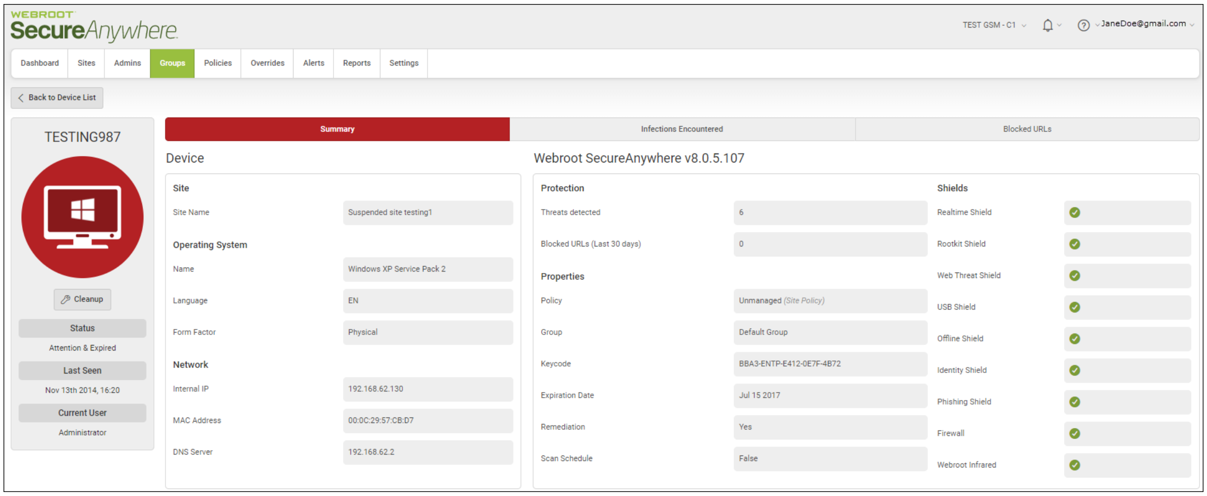
3. Select a device with the status of Attention & Expired that you want to view, and double-click.



All sites
- - abc
- - Dan
- - Dan Test 699
- - DC
- 1523874072
- 5f0fd47d-fb08-4286-bef4-1f
- 737da301-76fa-4a7e-a8a6-8

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| IP-0A600155 | Protected | DNS, WSAB | 2 Policies | __Site0001 | 3 hours ago | |
| IP-0A600151 | Protected | DNS, WSAB | 2 Policies | __Site0001 | 1 hours ago | |
| EC2AMAZ-QCJ7LNF | Attention & Expired | WSAB | LeoSite02CA7WSA... | LeoSite01CA7 | 14 days ago | |
| EC2AMAZ-M5N2EK5 | Not Seen Recently | WSAB | GP-Policy-Sri | CA7 TEST _ Groups | 22 days ago | |

The Status Panel for the device you selected displays.



TESTING987

Status
Attention & Expired

Last Seen
Nov 13th 2014, 16:20

Current User
Administrator

Device

| | |
|---|---|
| **Site** | |
| Site Name | Suspended site testing1 |
| **Operating System** | |
| Name | Windows XP Service Pack 2 |
| Language | EN |
| Form Factor | Physical |
| **Network** | |
| Internal IP | 192.168.62.130 |
| MAC Address | 00:0C:29:57:CB:D7 |
| DNS Server | 192.168.62.2 |

Webroot SecureAnywhere v8.0.5.107

| | |
|---|---|
| **Protection** | |
| Threats detected | 6 |
| Blocked URLs (Last 30 days) | 0 |
| **Properties** | |
| Policy | Unmanaged *(Site Policy)* |
| Group | Default Group |
| Keycode | BBA3-ENTP-E412-0E7F-4B72 |
| Expiration Date | Jul 15 2017 |
| Remediation | Yes |
| Scan Schedule | False |

| **Shields** | |
|---|---|
| Realtime Shield | ✓ |
| Rootkit Shield | ✓ |
| Web Threat Shield | ✓ |
| USB Shield | ✓ |
| Offline Shield | ✓ |
| Identity Shield | ✓ |
| Phishing Shield | ✓ |
| Firewall | ✓ |
| Webroot Infrared | ✓ |

4. The Device Info column on the left displays the name of the device, as well as the following information:

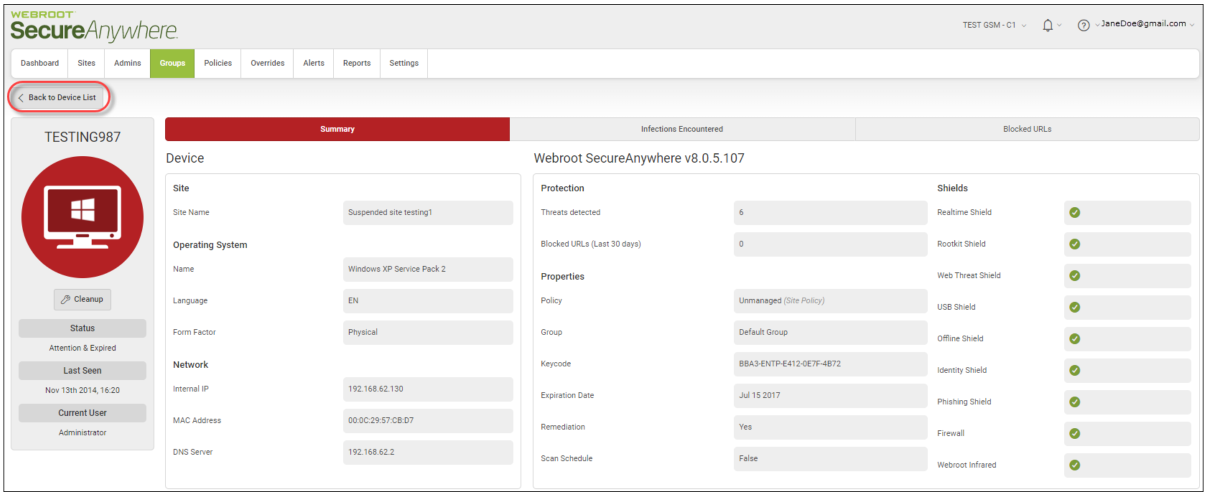
- **Status** — The status of the device. For more information, see *Device Management Overview on page 209*.
- **Last Seen** — The date and time the last time the device checked in with the system.
- **Current User** — The last name of the admin who is currently logged in and displaying the Status Panel.

The main part of the panel displays information about the following:

- **Site**
- **Operating System**
- **Network**
- **Protection**
- **Properties**
- **Shields**

5. Click any of the following three tabs for additional information:
   - **Summary** — Displays a summary of information about the device.
   - **Infections Encountered** — Displays a list of the infections encountered on this device.
   - **Blocked URLs** — Displays a list of any URLs that were blocked by the Web Threat Shield program. From this tab you can also add a web override to any URL that you don't want blocked. For more information, see *Adding Web Overrides to Devices on page 219*.
   - **Scan History** — Displays a list of every scan that has taken place for a particular device, including any threats that have been found during the scan. For more information, see *Displaying Scan Histories on page 277*.

6. When you're done, click the **Back to Device List** button.



TESTING987

Status
Attention & Expired

Last Seen
Nov 13th 2014, 16:20

Current User
Administrator

Device

| | |
|---|---|
| **Site** | |
| Site Name | Suspended site testing1 |
| **Operating System** | |
| Name | Windows XP Service Pack 2 |
| Language | EN |
| Form Factor | Physical |
| **Network** | |
| Internal IP | 192.168.62.130 |
| MAC Address | 00:0C:29:57:CB:D7 |
| DNS Server | 192.168.62.2 |

Webroot SecureAnywhere v8.0.5.107

| | | | |
|---|---|---|---|
| **Protection** | | **Shields** | |
| Threats detected | 6 | Realtime Shield | ✓ |
| Blocked URLs (Last 30 days) | 0 | Rootkit Shield | ✓ |
| **Properties** | | Web Threat Shield | ✓ |
| Policy | Unmanaged *(Site Policy)* | USB Shield | ✓ |
| Group | Default Group | Offline Shield | ✓ |
| Keycode | BBA3-ENTP-E412-0E7F-4B72 | Identity Shield | ✓ |
| Expiration Date | Jul 15 2017 | Phishing Shield | ✓ |
| Remediation | Yes | Firewall | ✓ |
| Scan Schedule | False | Webroot Infrared | ✓ |

# Viewing Device Summaries

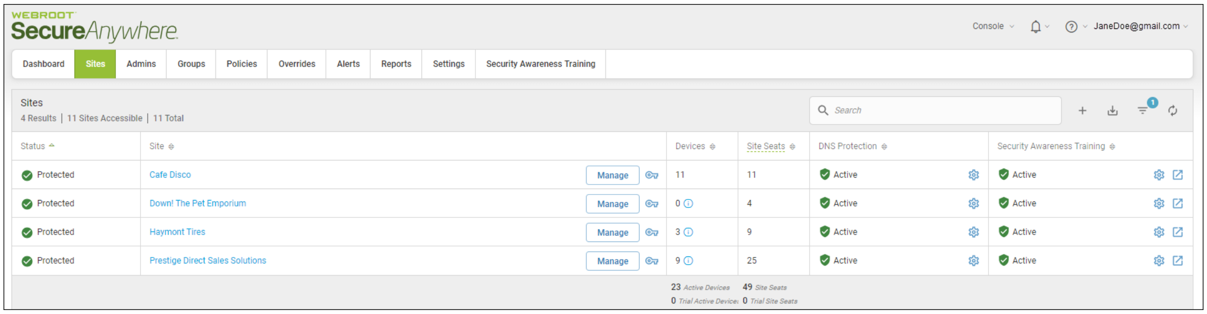
Within a group, you can have one or more endpoints. Within the panel, you can quickly view the Name, Status, Policies Applied, Last Seen, and Last Infected.

Follow this procedure to view additional information about a device such as a summary, infections encountered, and if there are any blocked URLs.

**To view device summaries:**

1. Log in to the management console.

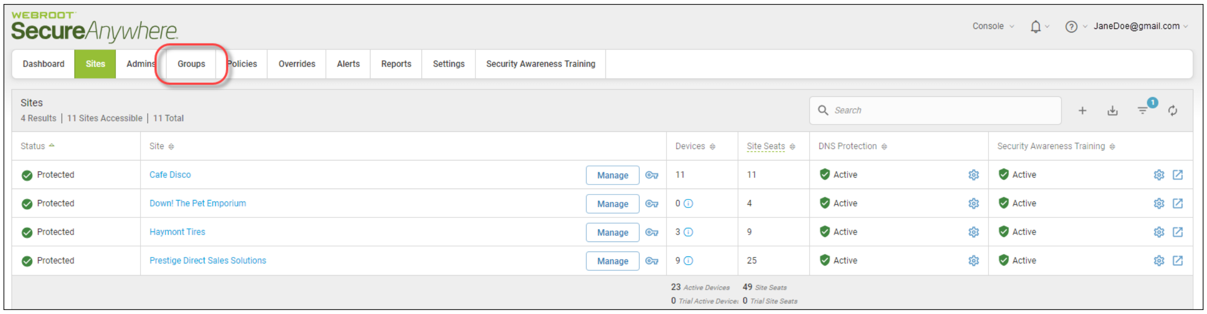
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

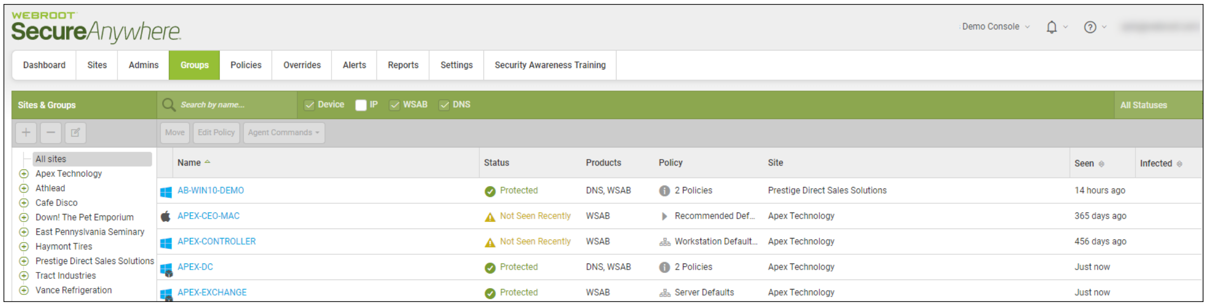
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

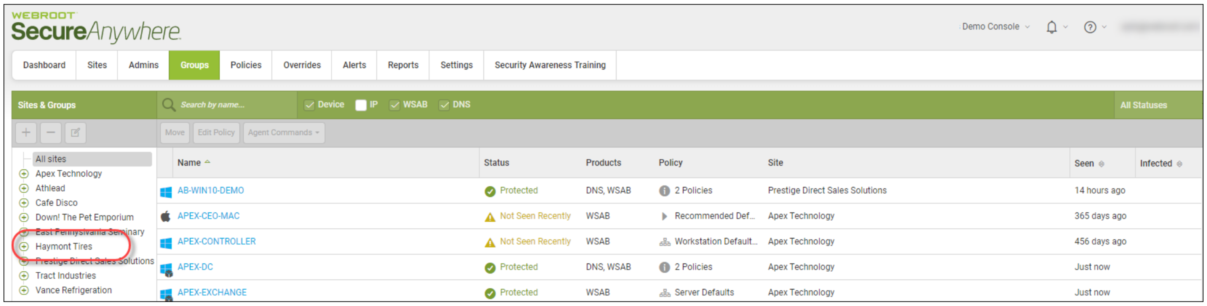
   The Groups tab displays.



All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennsylvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. In the left column, select the site that contains the group and device you want to view information about.

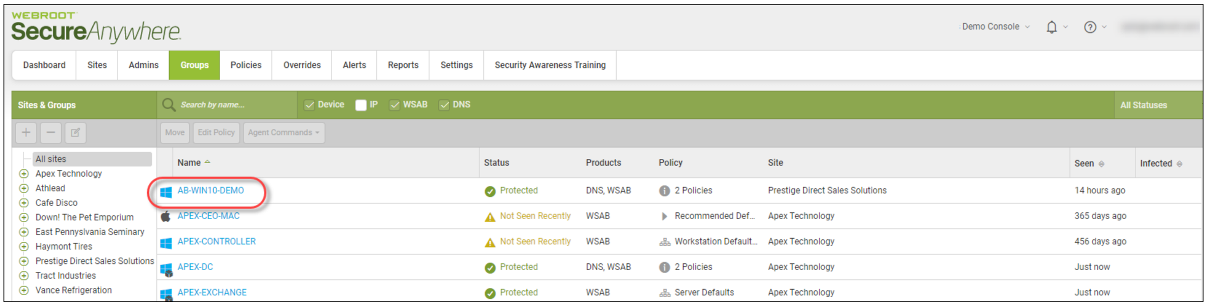


WEBROOT SecureAnywhere
Demo Console [redacted]
Dashboard | Sites | Admins | Groups | Policies | Overrides | Alerts | Reports | Settings | Security Awareness Training
Sites & Groups | Search by name... | ☑ Device □ IP ☑ WSAB ☑ DNS | All Statuses
Move | Edit Policy | Agent Commands

All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennsylvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

4. In the Devices panel, select the device that you want to view information about.



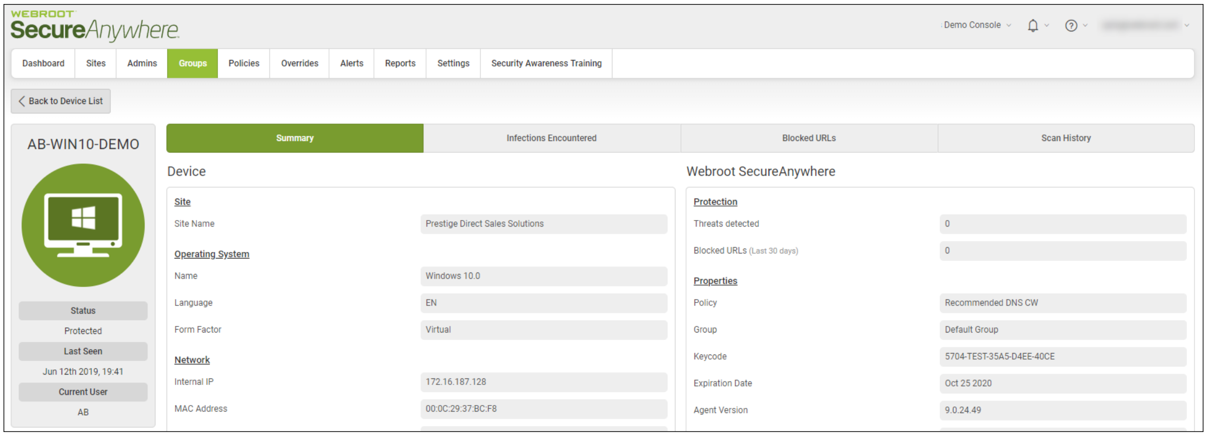
WEBROOT SecureAnywhere
Demo Console [redacted]
Dashboard | Sites | Admins | Groups | Policies | Overrides | Alerts | Reports | Settings | Security Awareness Training
Sites & Groups | Search by name... | ☑ Device □ IP ☑ WSAB ☑ DNS | All Statuses
Move | Edit Policy | Agent Commands

All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennsylvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The Summary panel displays the following information:

- Status and Last Seen
- Summary
- Infections Encountered
- Blocked URLs
- Scan History



AB-WIN10-DEMO

Status
Protected

Last Seen
Jun 12th 2019, 19:41

Current User
AB

Device

| | |
|---|---|
| **Site** | |
| Site Name | Prestige Direct Sales Solutions |
| **Operating System** | |
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Virtual |
| **Network** | |
| Internal IP | 172.16.187.128 |
| MAC Address | 00:0C:29:37:BC:F8 |

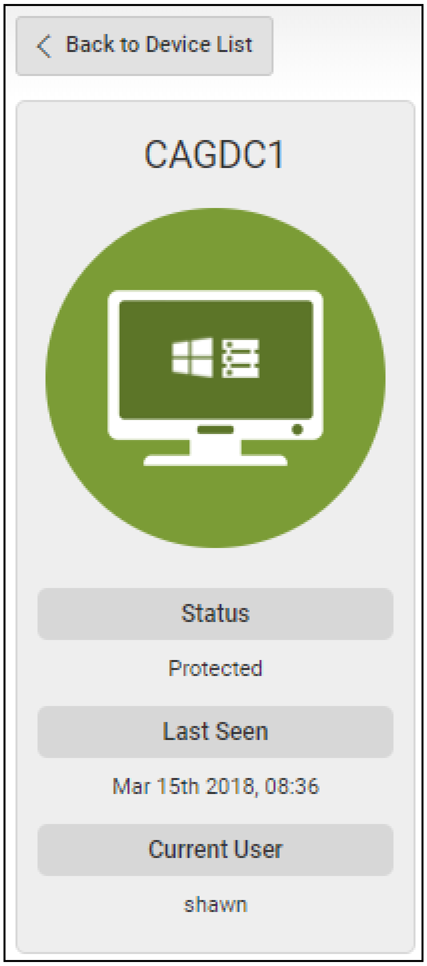
Webroot SecureAnywhere

| | |
|---|---|
| **Protection** | |
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |
| **Properties** | |
| Policy | Recommended DNS CW |
| Group | Default Group |
| Keycode | 5704-TEST-35A5-D4EE-40CE |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |

## Status and Last Seen

The Device Info column on the left displays the name of the device, as well as the following information:

- Displays an icon that indicates, by color, the status of the endpoint.
  - **Status** — The status of the endpoint.
  - **Last Seen** — The date the endpoint last checked in with the system.



CAGDC1

Status

Protected

Last Seen

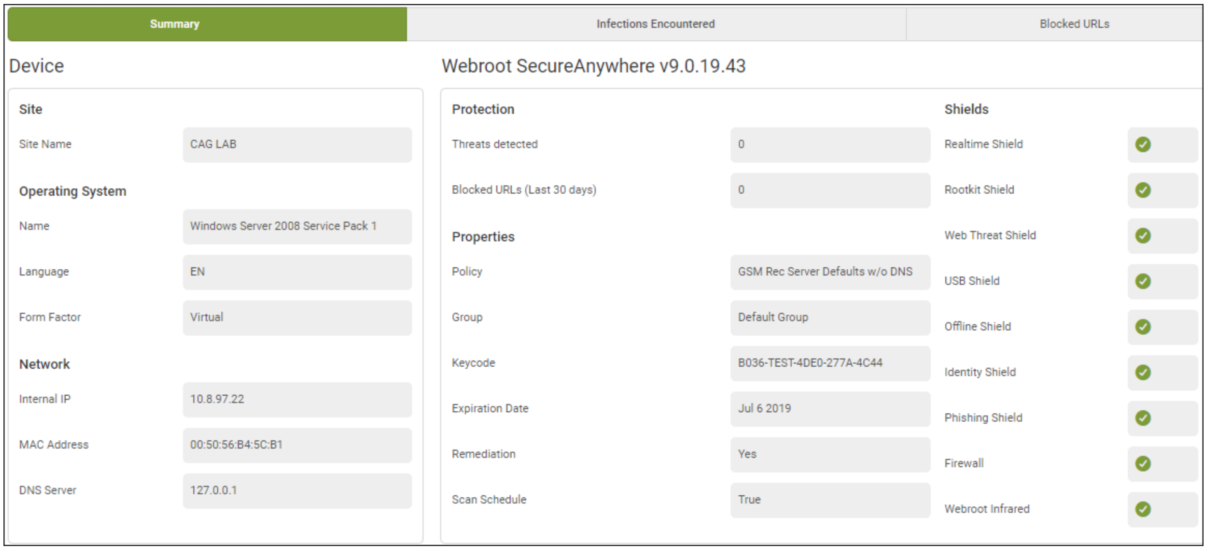
Mar 15th 2018, 08:36

Current User

shawn

## Summary Tab

- The version number
- Site Information
- Operating System
- Network Information
- Protection
- Properties
- Shields



Device

Site

| | |
|---|---|
| Site Name | CAG LAB |

Operating System

| | |
|---|---|
| Name | Windows Server 2008 Service Pack 1 |
| Language | EN |
| Form Factor | Virtual |

Network

| | |
|---|---|
| Internal IP | 10.8.97.22 |
| MAC Address | 00:50:56:B4:5C:B1 |
| DNS Server | 127.0.0.1 |

Webroot SecureAnywhere v9.0.19.43

Protection

| | |
|---|---|
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |

Properties

| | |
|---|---|
| Policy | GSM Rec Server Defaults w/o DNS |
| Group | Default Group |
| Keycode | B036-TEST-4DE0-277A-4C44 |
| Expiration Date | Jul 6 2019 |
| Remediation | Yes |
| Scan Schedule | True |

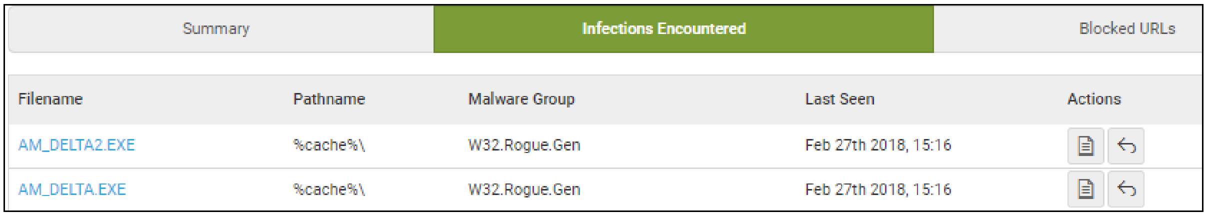
Shields

| | |
|---|---|
| Realtime Shield | ✓ |
| Rootkit Shield | ✓ |
| Web Threat Shield | ✓ |
| USB Shield | ✓ |
| Offline Shield | ✓ |
| Identity Shield | ✓ |
| Phishing Shield | ✓ |
| Firewall | ✓ |
| Webroot Infrared | ✓ |

## Infections Encountered Tab

Click the **Infections Encountered** tab to display information about infections that the device encountered:

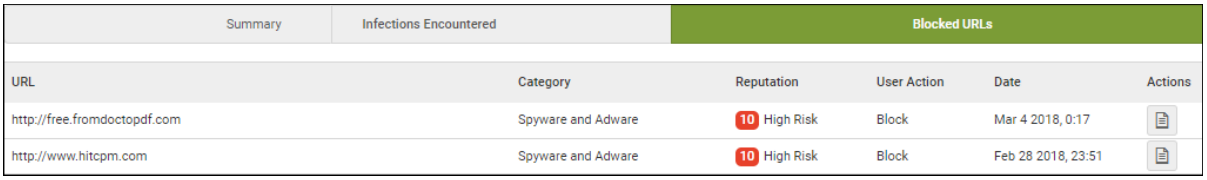
- Filename
- Pathname
- Malware Group
- Last Seen
- Actions



| Filename | Pathname | Malware Group | Last Seen | Actions |
|---|---|---|---|---|
| AM_DELTA2.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↶ |
| AM_DELTA.EXE | %cache%\ | W32.Rogue.Gen | Feb 27th 2018, 15:16 | 🗎 ↶ |

## Blocked URLs Tab

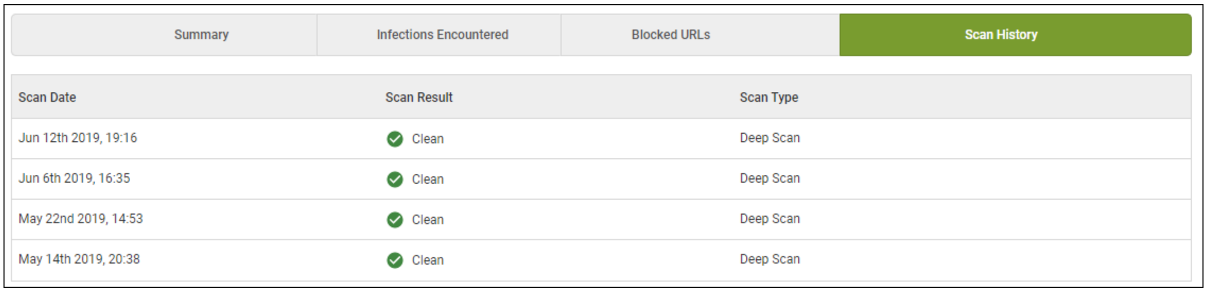
Contains a list of URLs that have been blocked from that endpoint.



| URL | Category | Reputation | User Action | Date | Actions |
|---|---|---|---|---|---|
| http://free.fromdoctopdf.com | Spyware and Adware | 10 High Risk | Block | Mar 4 2018, 0:17 | 🗎 |
| http://www.hitcpm.com | Spyware and Adware | 10 High Risk | Block | Feb 28 2018, 23:51 | 🗎 |

## Scan History Tab

Displays information about all the scans that have taken place, including any threats that have been found during the scan. For more information, see *Displaying Scan Histories on page 277*.



| Scan Date | Scan Result | Scan Type |
|---|---|---|
| Jun 12th 2019, 19:16 | ✓ Clean | Deep Scan |
| Jun 6th 2019, 16:35 | ✓ Clean | Deep Scan |
| May 22nd 2019, 14:53 | ✓ Clean | Deep Scan |
| May 14th 2019, 20:38 | ✓ Clean | Deep Scan |

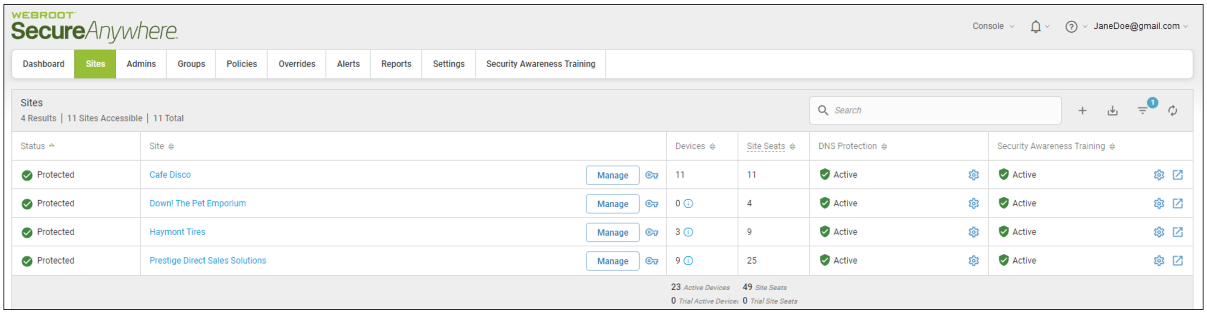
# Searching for Devices

Follow this procedure to search for a device.

### To search for a device:

1. Log in to the management console.

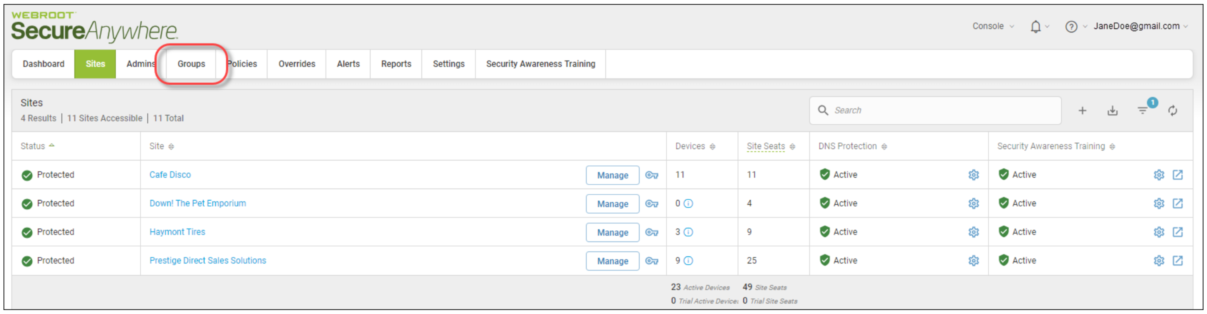
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

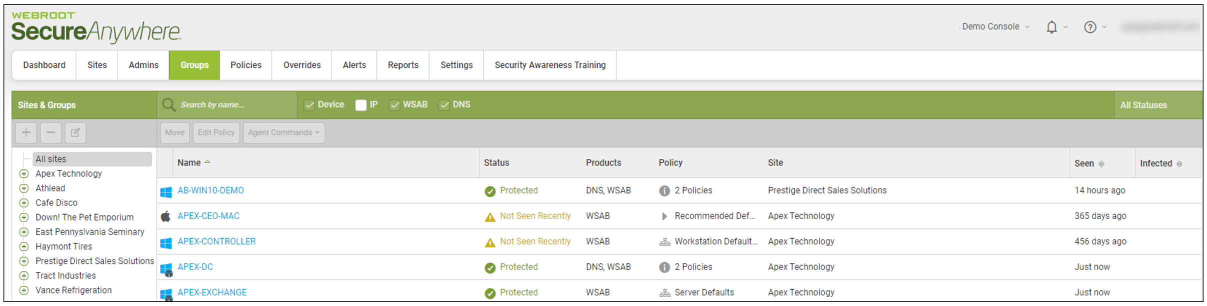
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

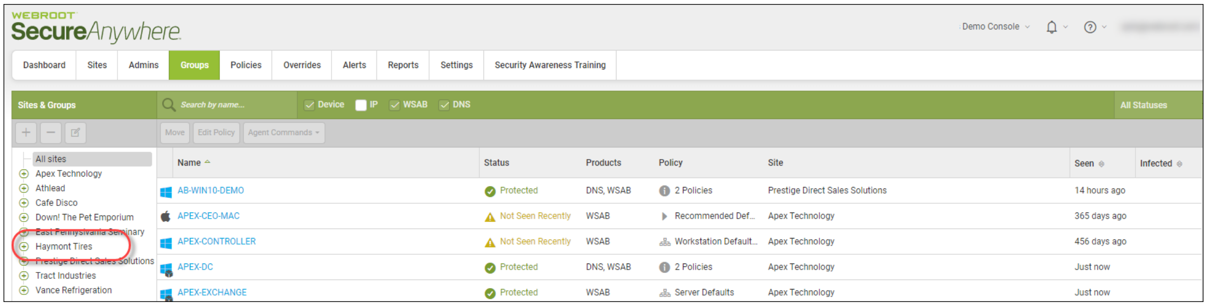
The Groups tab displays.



All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

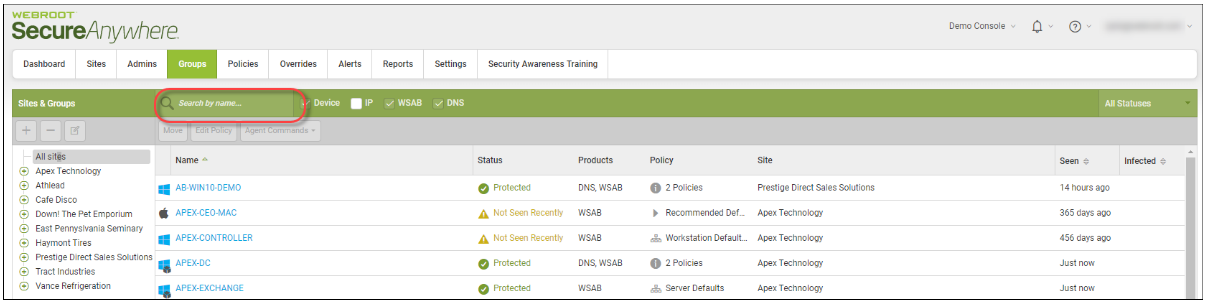
3. In the left column, select the site that contains the device you want to find.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

**Note:** You can search for a device at both the site and group level.

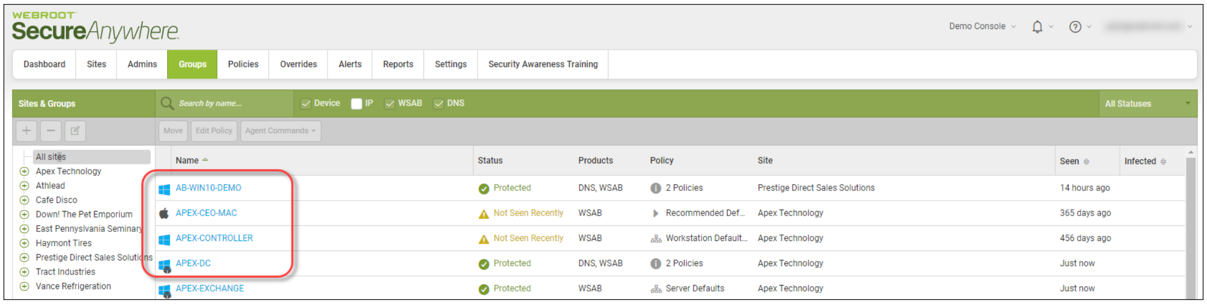
4. In the Search field, enter the name of the device you want to find.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

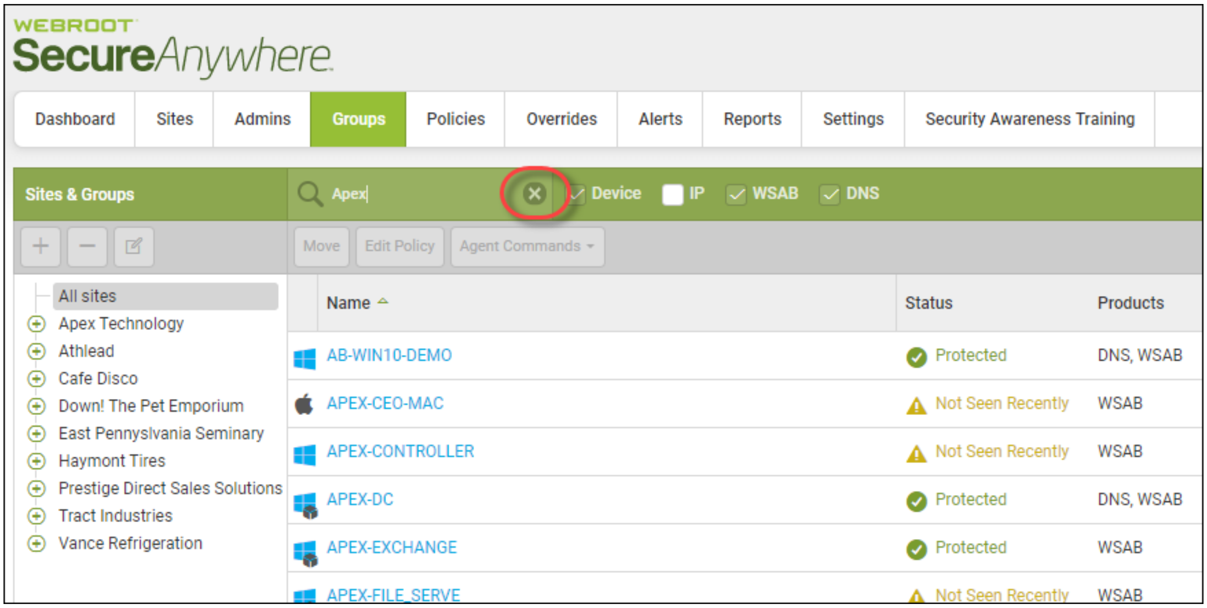
If needed, you can enter a partial name, and the system will display all devices that fit that criteria. For example, if you remember that part of the device name was "Brown" but don't remember the rest of the name, enter *Brown*.

A list of devices that match the search criteria you entered displays.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

5. To clear the Search field, click the **X**.



| Name | Status | Products |
|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB |
| APEX-CEO-MAC | Not Seen Recently | WSAB |
| APEX-CONTROLLER | Not Seen Recently | WSAB |
| APEX-DC | Protected | DNS, WSAB |
| APEX-EXCHANGE | Protected | WSAB |
| APEX-FILE_SERVE | Not Seen Recently | WSAB |

All devices within that site display.

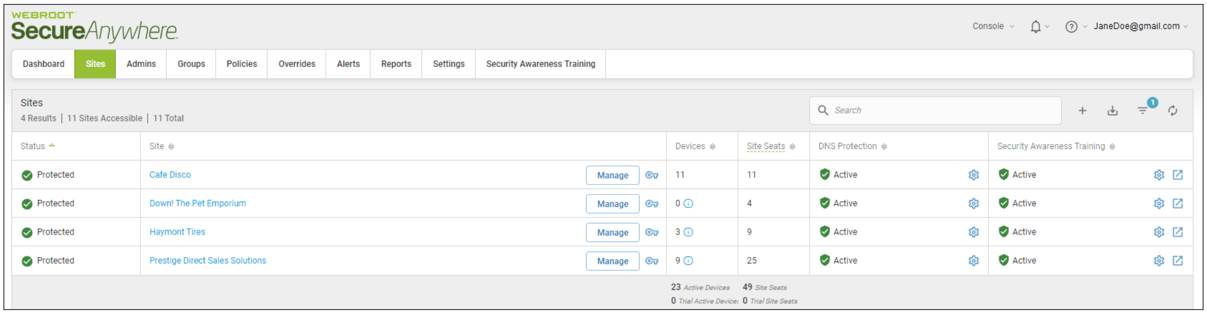
# Filtering Devices By Site Names

Follow this procedure to sort devices by the name of the site to which they belong.

### To filter by a site name:

1. Log in to the management console.

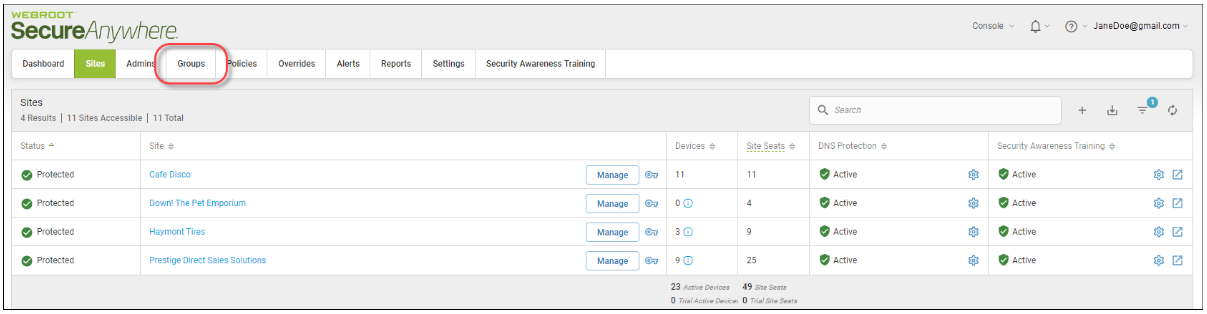
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats |  |  |

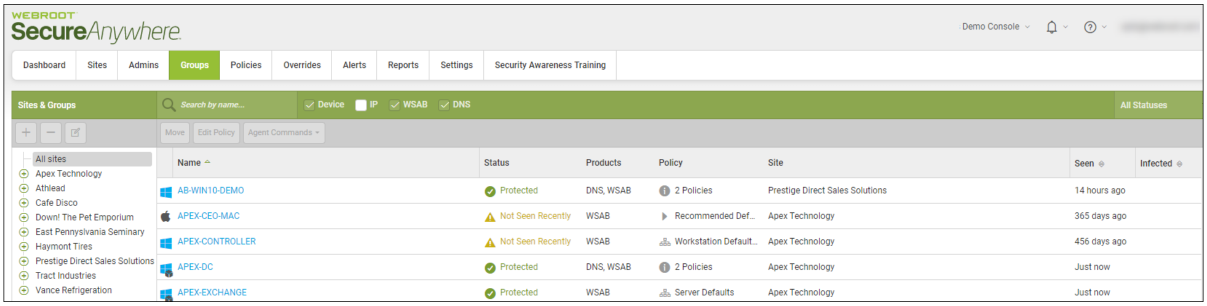
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats |  |  |

   The Groups tab displays.

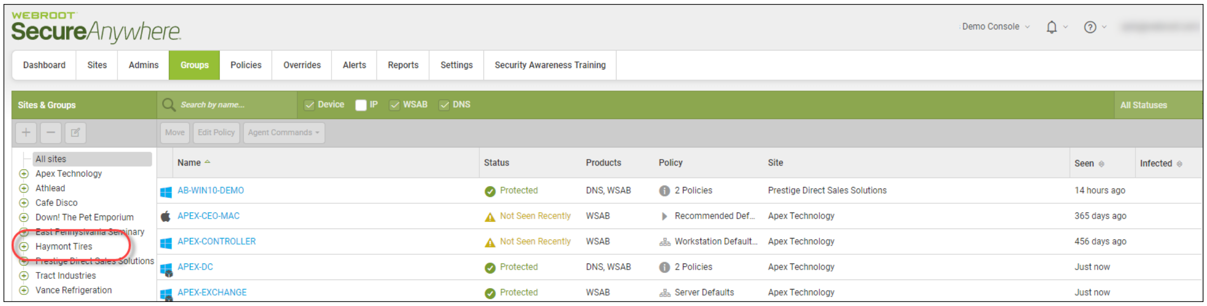


[redacted]

All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

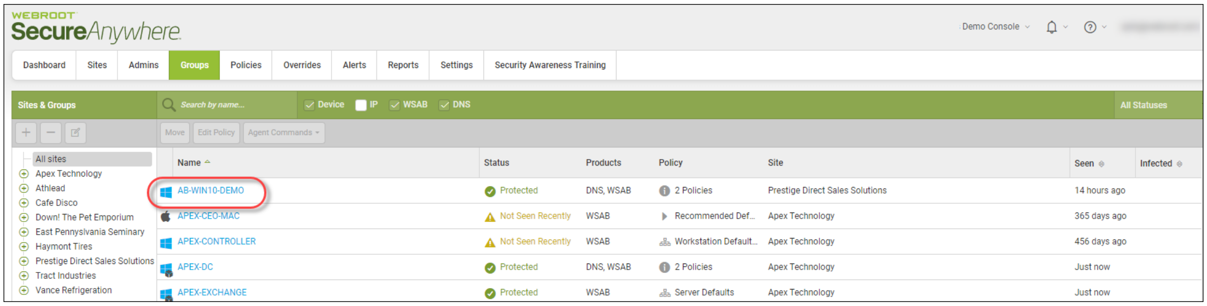
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago |  |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago |  |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago |  |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now |  |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now |  |

3. From the All sites drop-down menu, select the site you'd like to filter on.



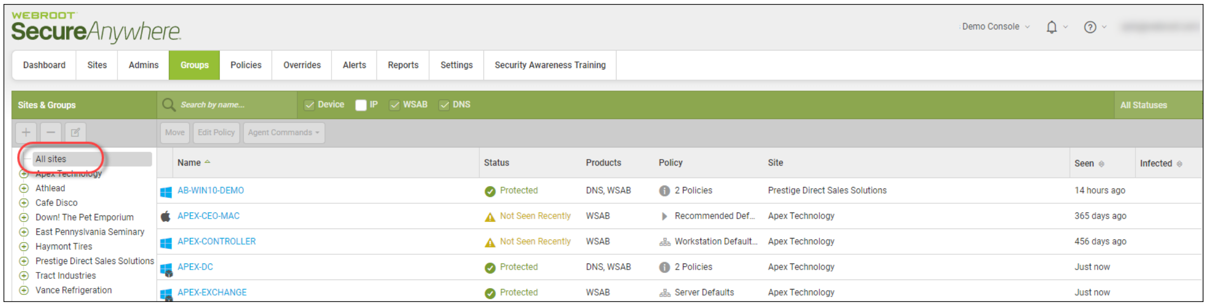
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The system displays the device you filtered on for.



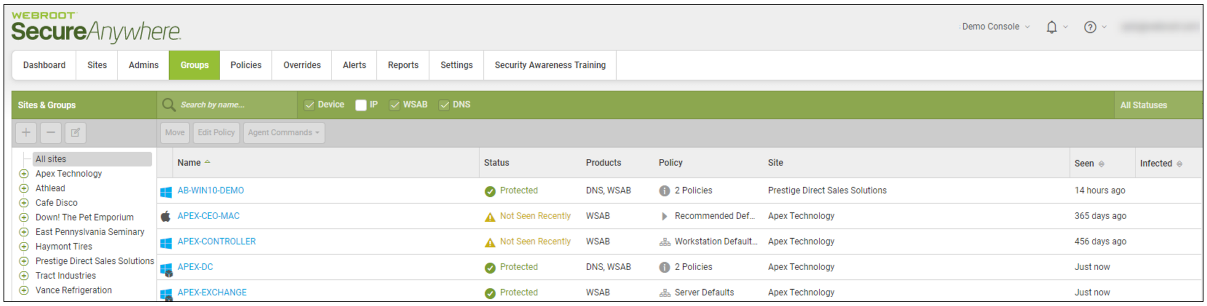
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

4. To display all devices again, from the All sites drop-down menu, select **All Site**s.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The complete list of devices displays.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

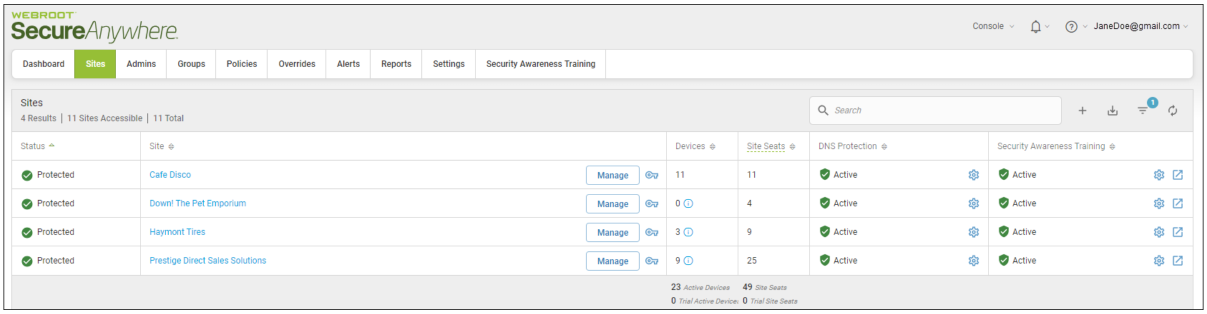
# Filtering Devices by Site Statuses

Follow this procedure to filter devices by their site statuses.

### To filter devices by status:

1. Log in to the management console.

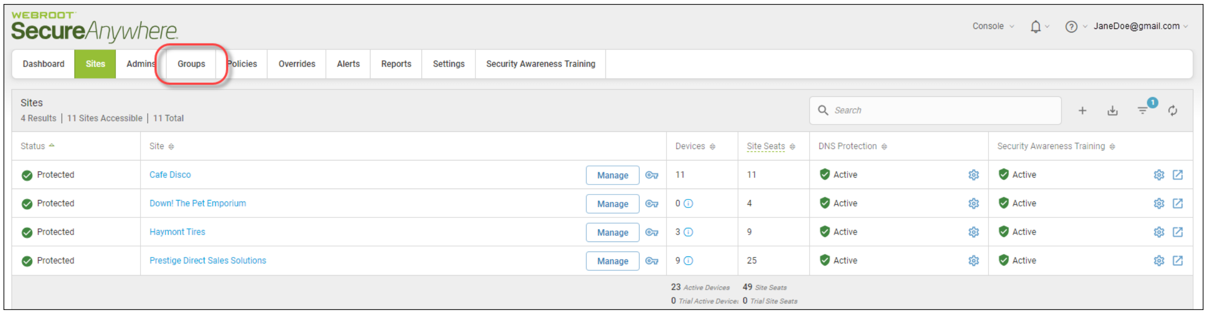
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats |  |  |

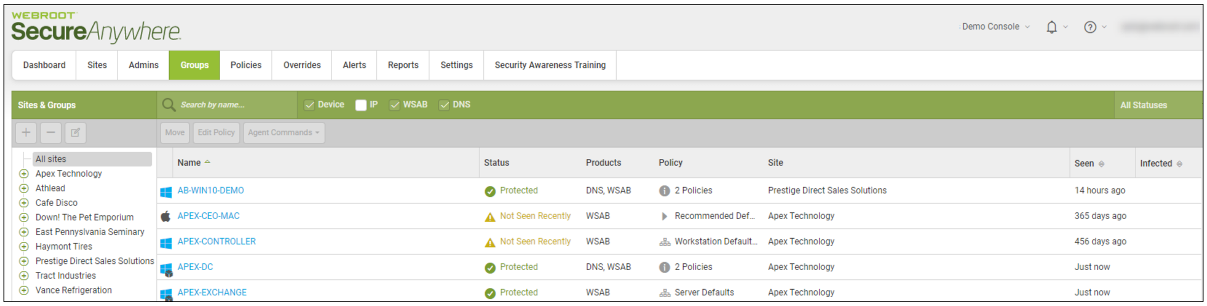
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
|  |  | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats |  |  |

The Groups tab displays.

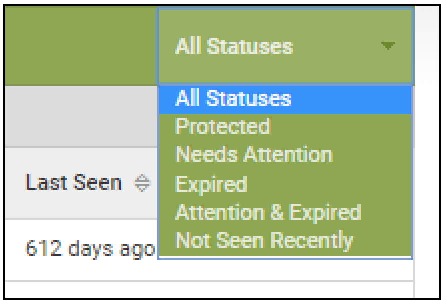


| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago |  |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago |  |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago |  |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now |  |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now |  |

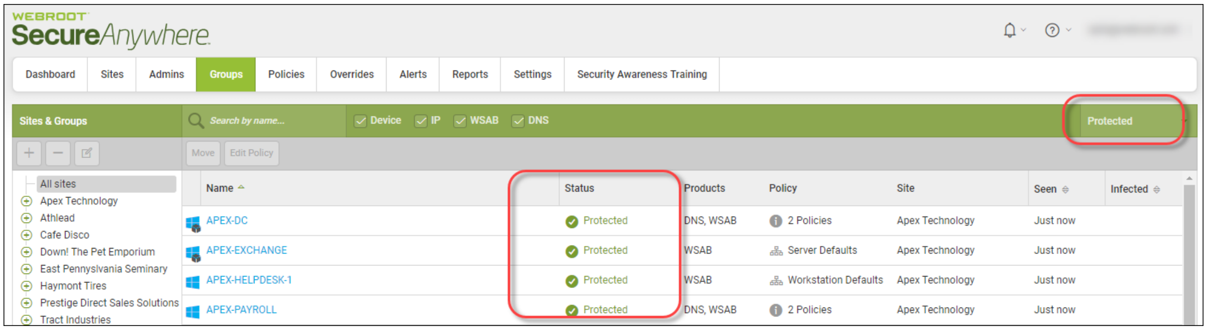
3. From the All Statuses drop-down menu, select the status that you want to filter on.

   The available statuses are:

   - **Protected** — Device is being protected by Webroot SecureAnywhere.
   - **Needs Attention** — Device needs attention.
   - **Expired** — Device's license has expired and is no longer being protected by Webroot SecureAnywhere.
   - **Attention & Expired** — Device needs attention, and the device's license has expired and is no longer being protected by Webroot SecureAnywhere.
   - **Not Seen Recently** — Device has not been seen recently by Webroot SecureAnywhere.

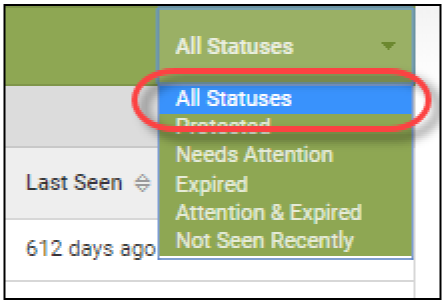


   The devices with the status that you filtered on displays.

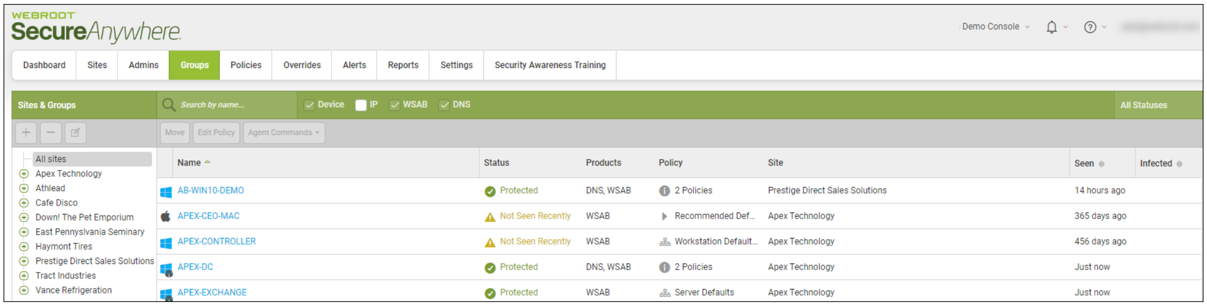


| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |
| APEX-HELPDESK-1 | Protected | WSAB | Workstation Defaults | Apex Technology | Just now | |
| APEX-PAYROLL | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |

4. To display all devices again, from the All Statuses drop-down menu, select **All Statuses**.



The complete list of devices displays.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

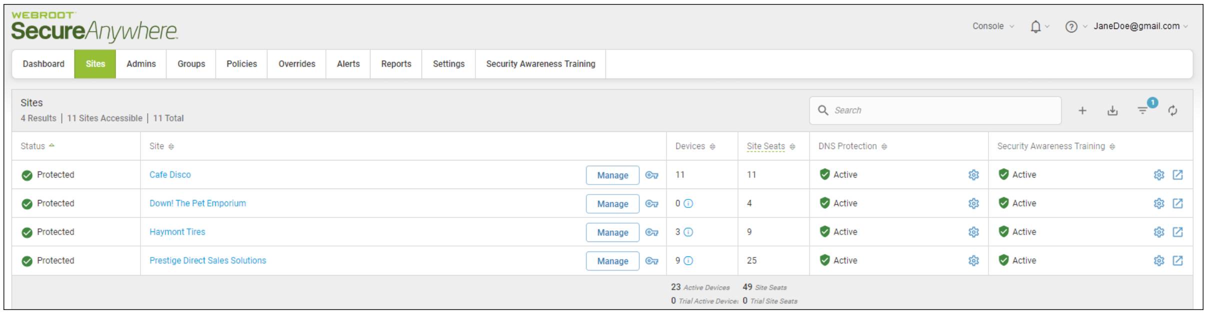
# Filtering Devices Within Groups

Follow this procedure to filter devices within groups based on their statuses.

### To filter endpoints:

1. Log in to the management console.

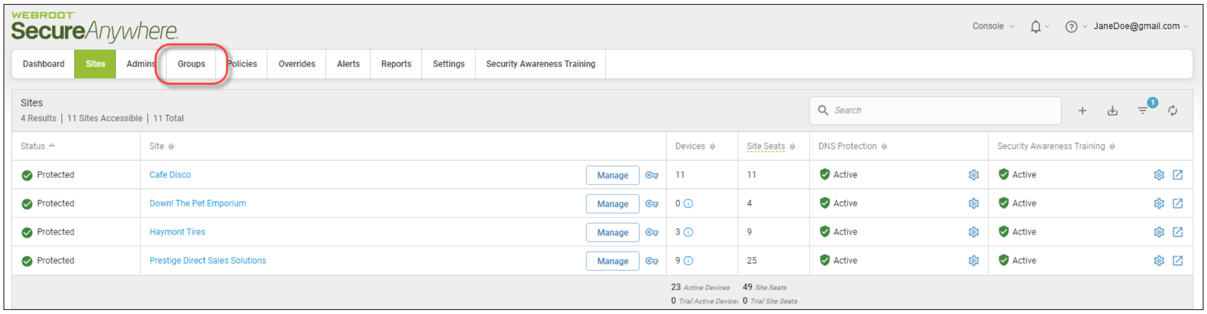
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

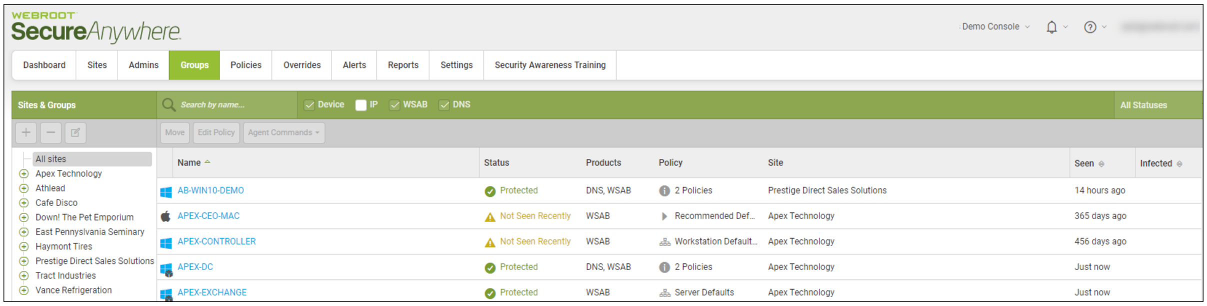
2. Click the **Groups** tab.


WEBROOT SecureAnywhere
Console
JaneDoe@gmail.com
Dashboard Sites Admins Groups Policies Overrides Alerts Reports Settings Security Awareness Training

Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

The Groups tab displays.

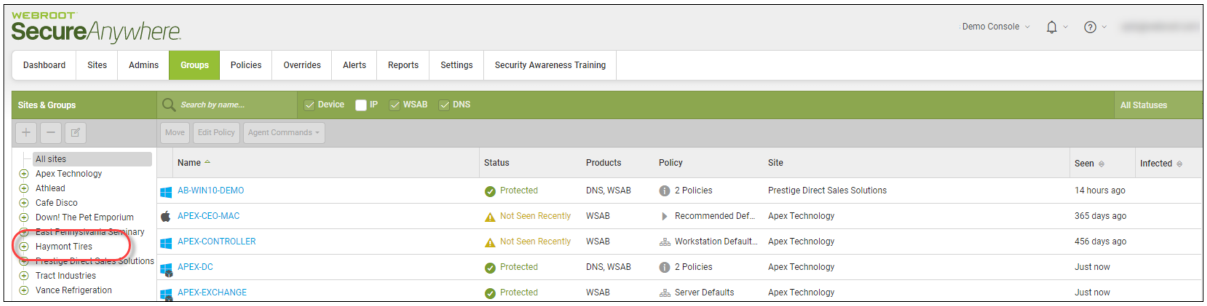


[redacted]

All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

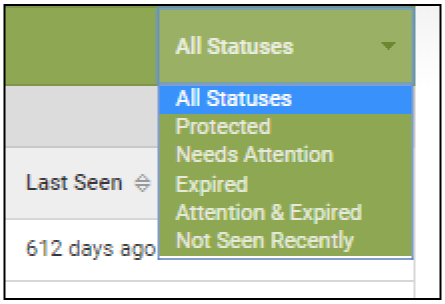
3. In the left column, select the site that contains the group you want to filter



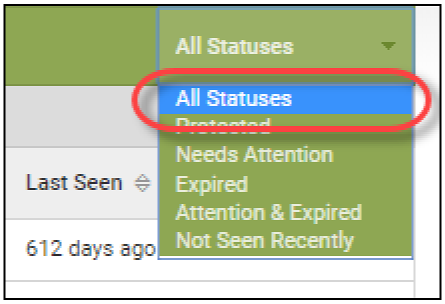
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

4. From the All Statuses drop-down menu, select one of the following statuses to filter on:

- **Protected** — Device is being protected by Webroot SecureAnywhere.
- **Needs Attention** — Device needs attention.
- **Expired** — Device's license has expired and is no longer being protected by Webroot SecureAnywhere.
- **Attention & Expired** — Device needs attention, and the device's license has expired and is no longer being protected by Webroot SecureAnywhere.
- **Not Seen Recently** — Device has not been seen recently by Webroot SecureAnywhere. The devices with the status that you filtered on displays.



5. To display all devices again, from the All Statuses drop-down menu, select **All Statuses**.



The complete list of devices displays.

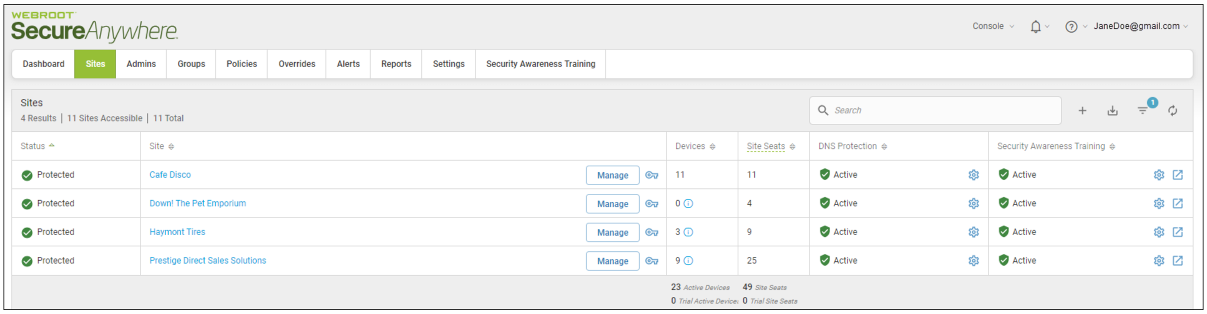
# Moving Devices Between Groups

Follow this procedure to move devices between groups.

### To move a device:

1. Log in to the management console.

   The management console displays, with the Sites tab active.

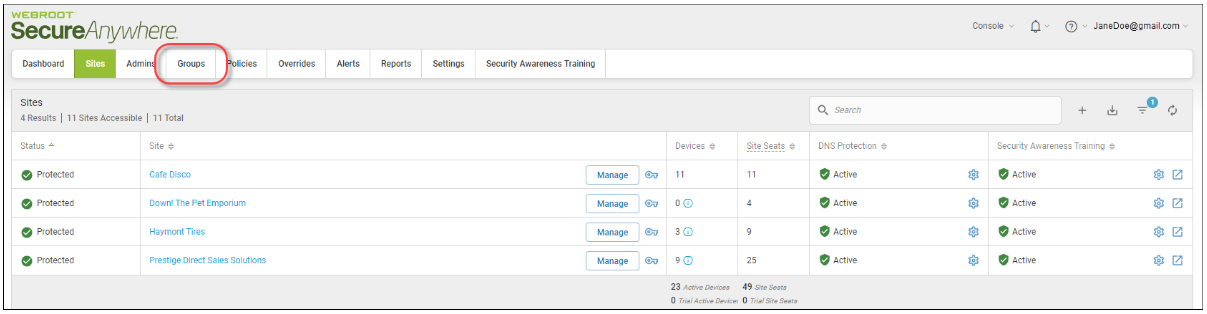


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |

23 Active Devices 49 Site Seats
0 Trial Active Device: 0 Trial Site Seats

2. Click the **Groups** tab.

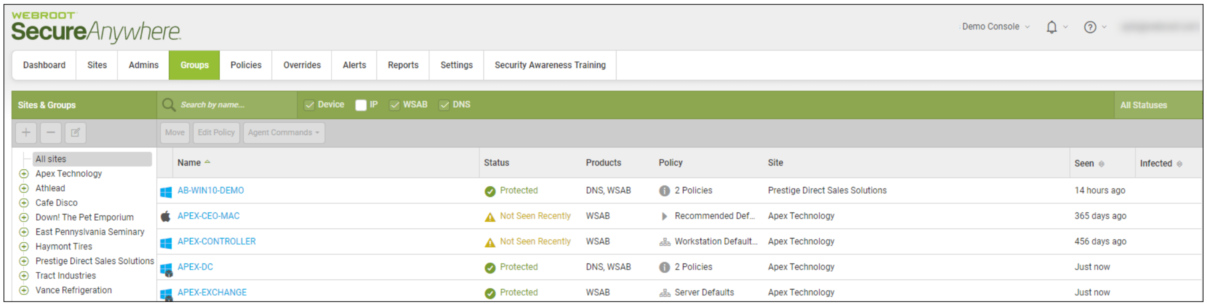


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |

23 Active Devices 49 Site Seats
0 Trial Active Device: 0 Trial Site Seats

The Groups tab displays.

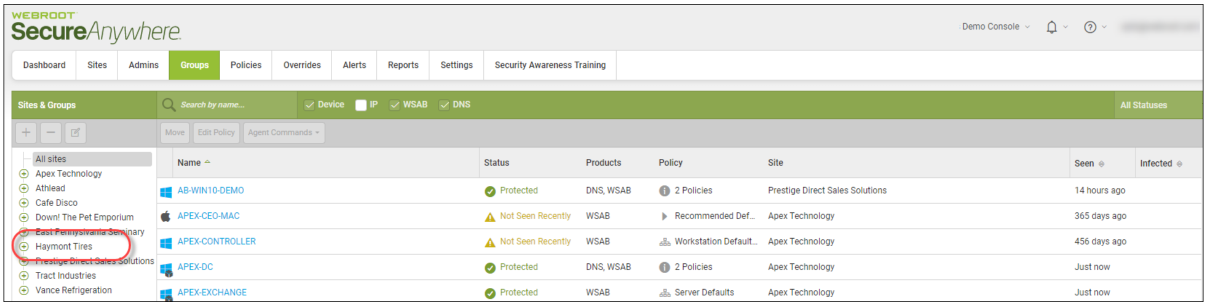


☑ Device □ IP ☑ WSAB ☑ DNS

- All sites
- Apex Technology
- Athlead
- Cafe Disco
- Down! The Pet Emporium
- East Pennyslvania Seminary
- Haymont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

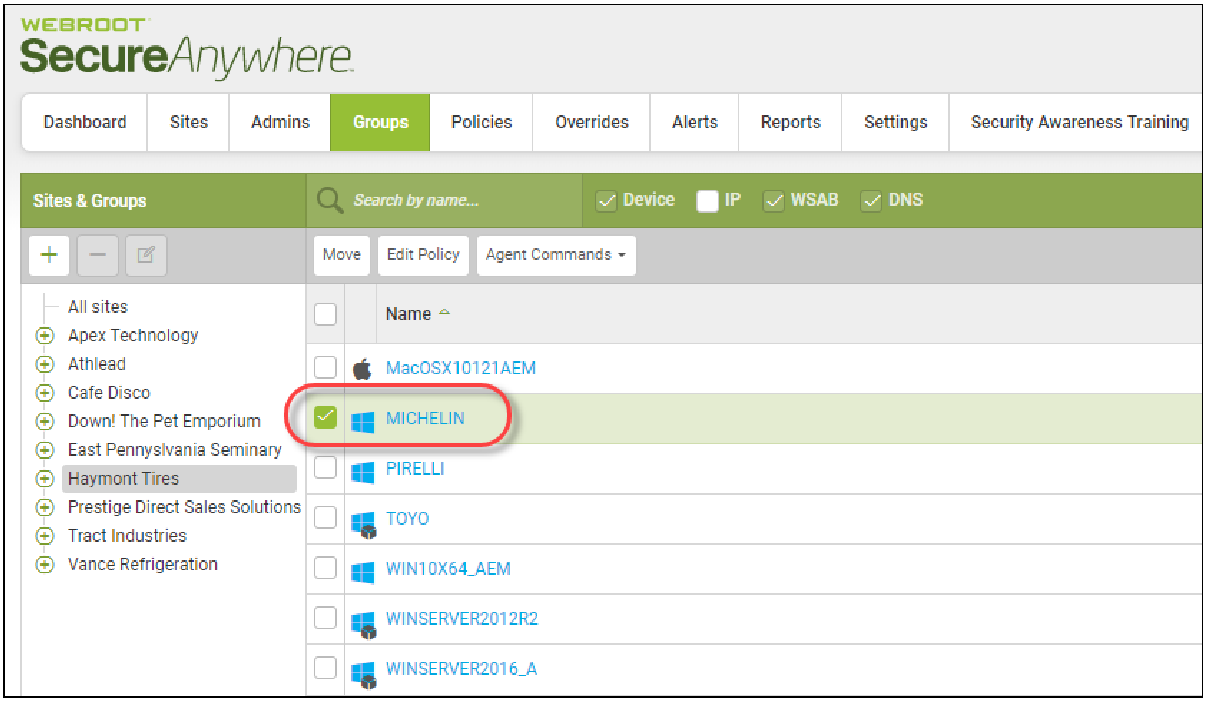
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. In the left column, select the site that contains the group you want to move.



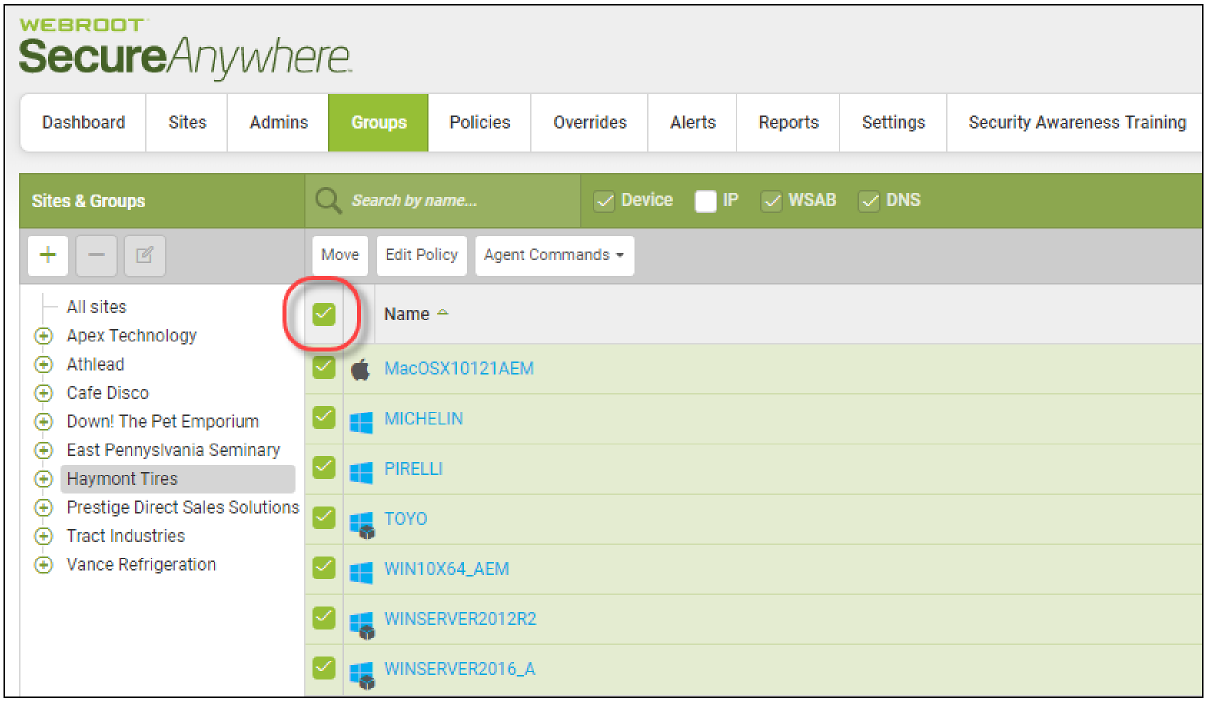
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

4. Select one or more devices from the Devices panel on the right.



| ☐ | Name |
|---|---|
| ☐ | MacOSX10121AEM |
| ☑ | MICHELIN |
| ☐ | PIRELLI |
| ☐ | TOYO |
| ☐ | WIN10X64_AEM |
| ☐ | WINSERVER2012R2 |
| ☐ | WINSERVER2016_A |

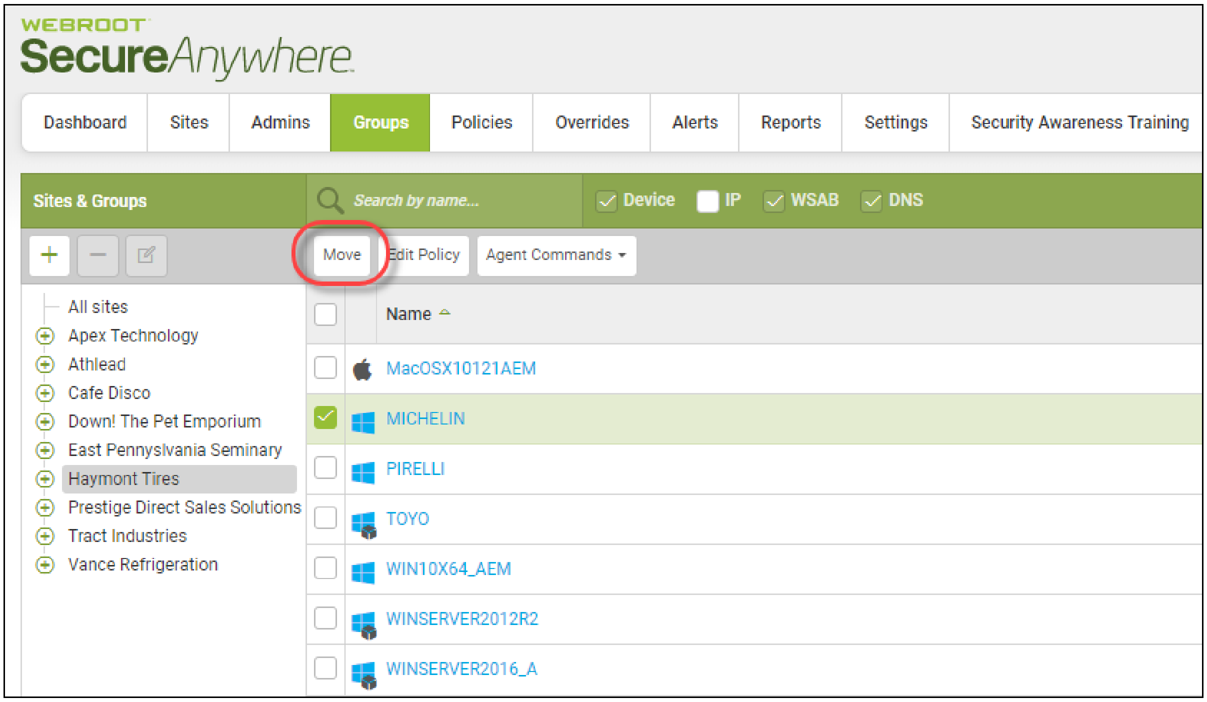
To select all devices, select the checkbox at the top of the column.



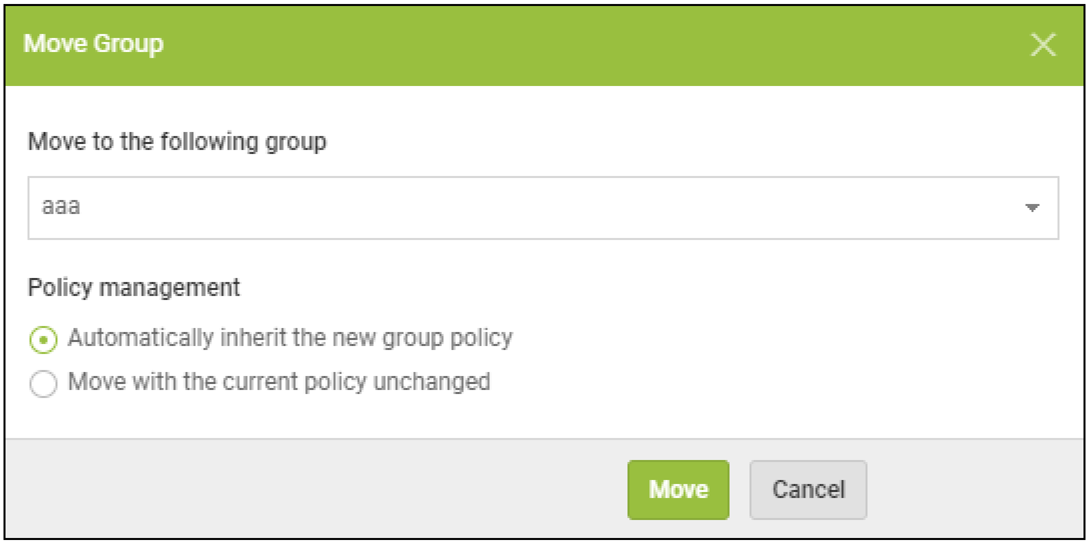
All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| ☑ | Name |
|---|---|
| ☑ | MacOSX10121AEM |
| ☑ | MICHELIN |
| ☑ | PIRELLI |
| ☑ | TOYO |
| ☑ | WIN10X64_AEM |
| ☑ | WINSERVER2012R2 |
| ☑ | WINSERVER2016_A |

5. Click the **Move** button.



The Move Group window displays.



Move to the following group

aaa

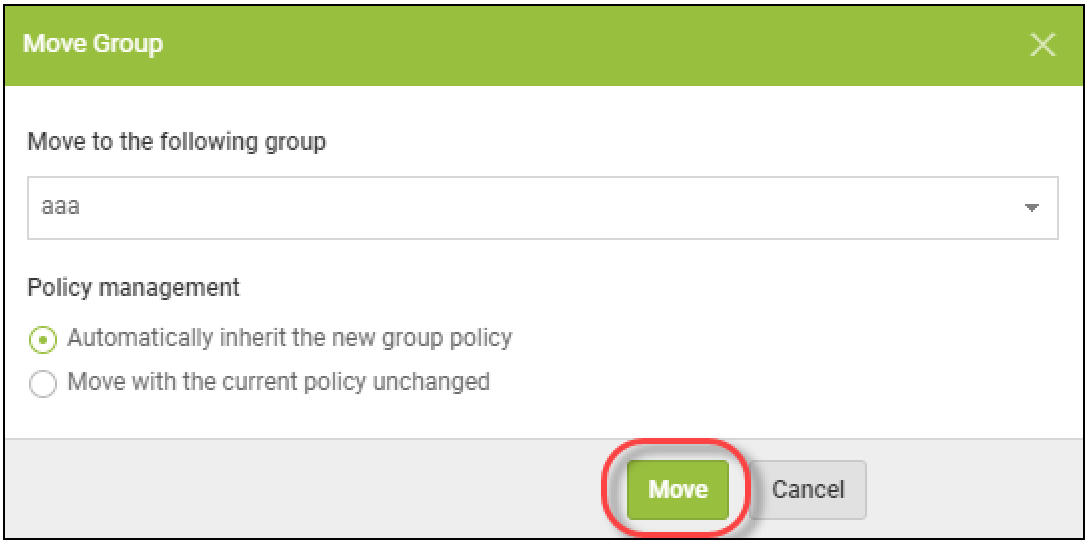
Policy management

● Automatically inherit the new group policy

○ Move with the current policy unchanged

6. From the Move to the following group drop-down menu, select the group you want to move the device to.

7. Select one of the following Policy management radio buttons:
   - **Automatically inherit the new group policy**
   - **Move with the current policy unchanged**
8. Click the **Move** button.



Move Group

Move to the following group

aaa

Policy management

● Automatically inherit the new group policy

○ Move with the current policy unchanged

The group has been moved to the new group.

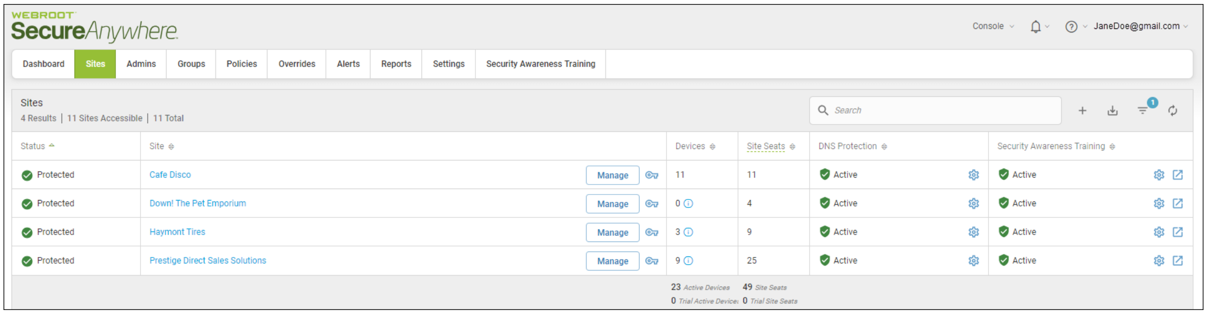
# Sorting Devices Within Groups

Follow this procedure to sort devices within a group.

**To sort devices:**

1. Log in to the [management console](management console).

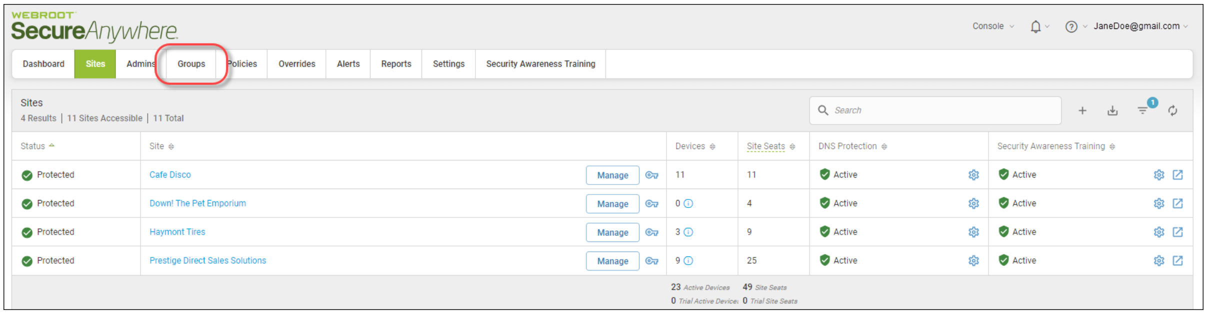
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

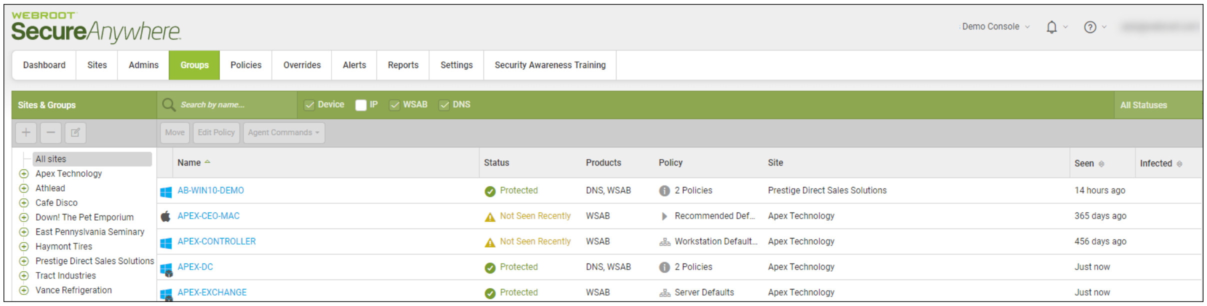
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

The Groups tab displays.



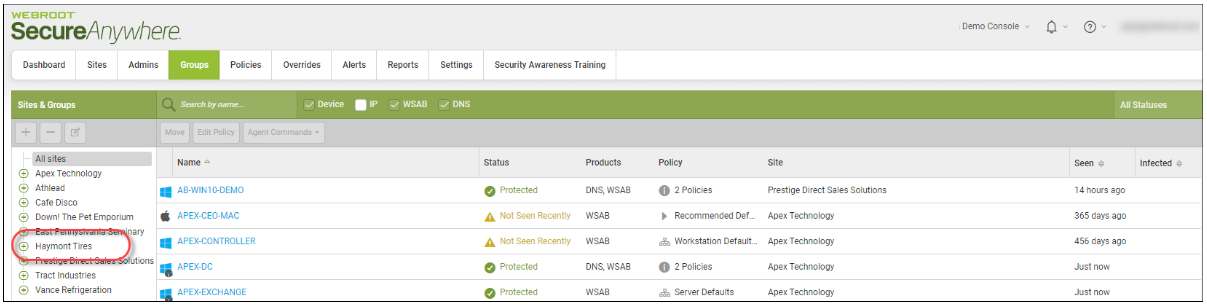
[redacted]

☑ Device ☐ IP ☑ WSAB ☑ DNS

All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

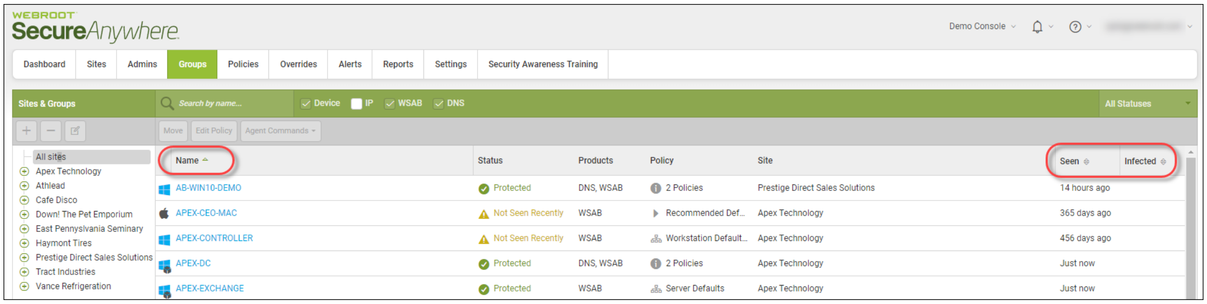
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. In the left column, select the site that contains the group you want to sort.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

4. In the Device panel, click the **Up** or **Down** arrow to the right of each heading to sort on the following columns:
   - **Name**
   - **Seen**
   - **Infected**



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The system sorts in ascending or descending order, based on the type of information in each column, for example, lowest to highest number, or alphabetical.

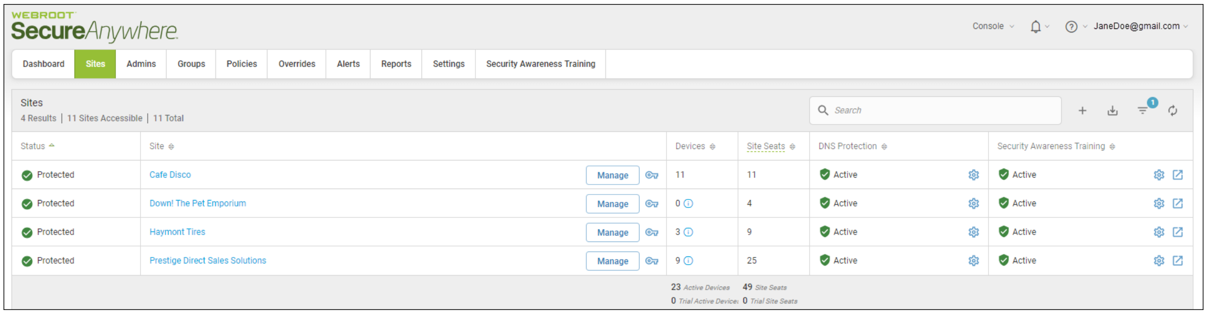
# Displaying Scan Histories

Follow this procedure to display a list of every scan that has taken place for a particular device, including any threats that have been found during the scan.

**To display a scan history:**

1. Log in to the management console.

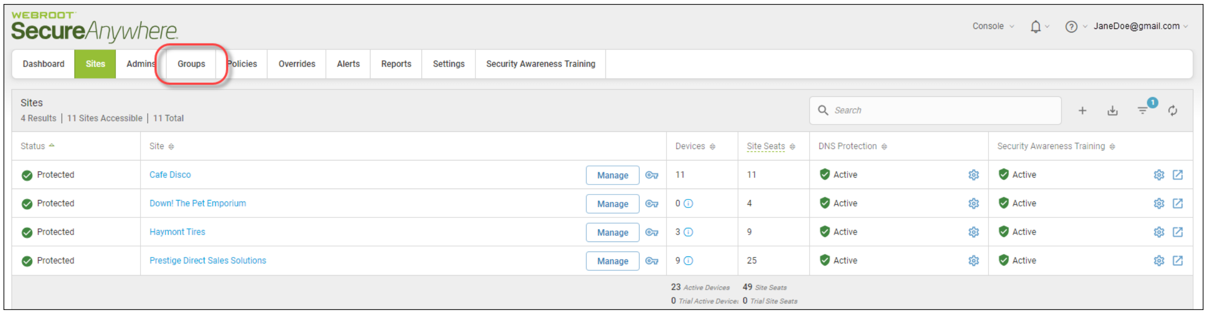
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

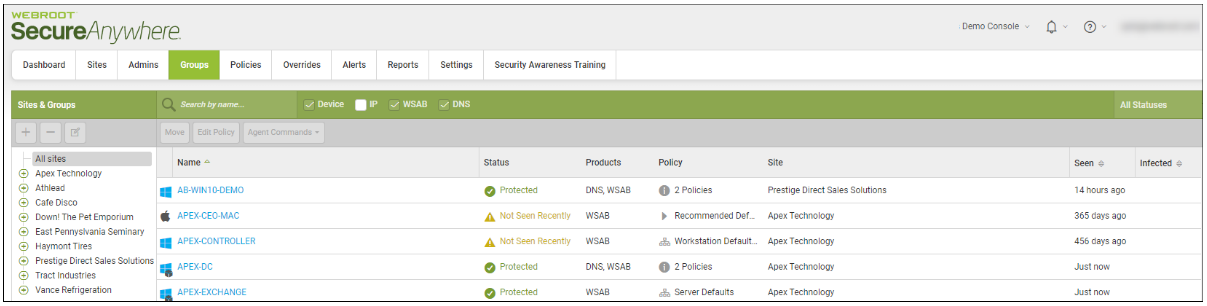
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

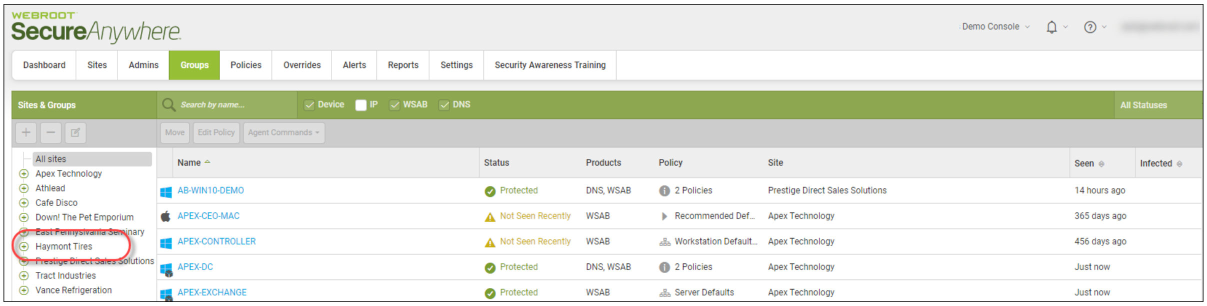
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



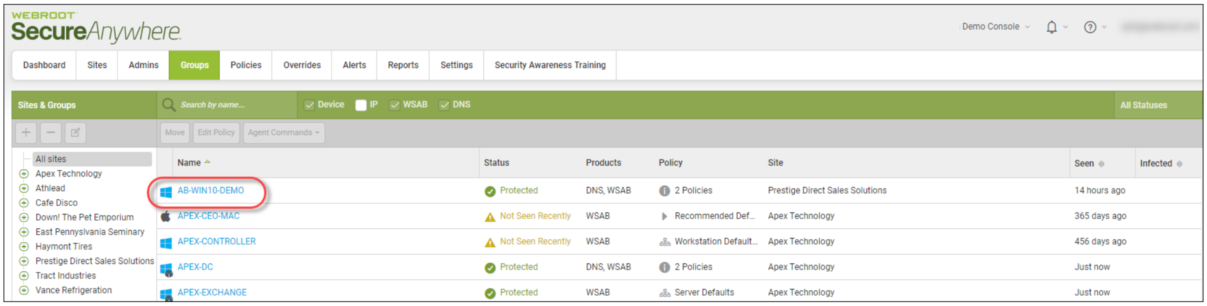
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. From the All sites drop-down menu, select the site you'd like to filter on.



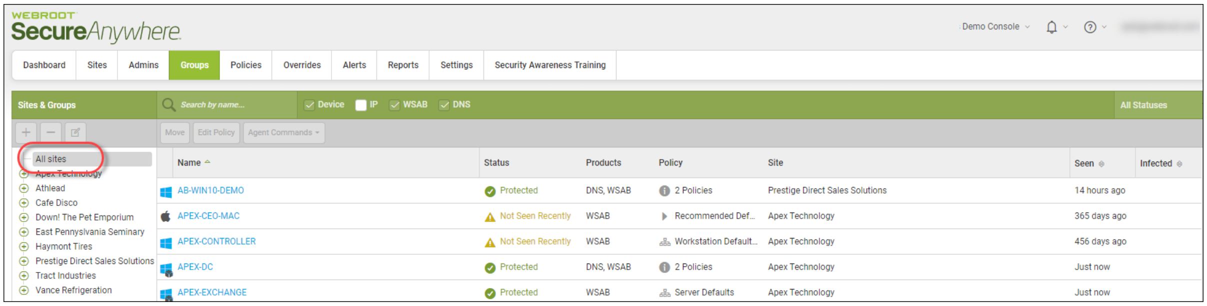
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The system displays the device you filtered on for.



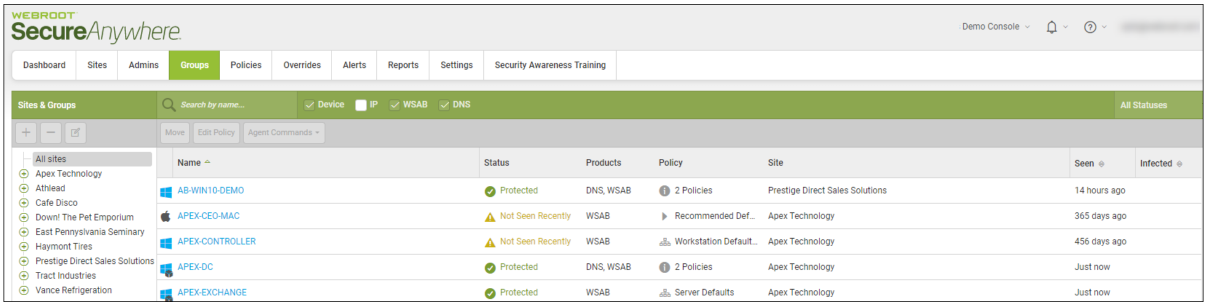
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

4. To display all devices again, from the All sites drop-down menu, select **All Sites**.



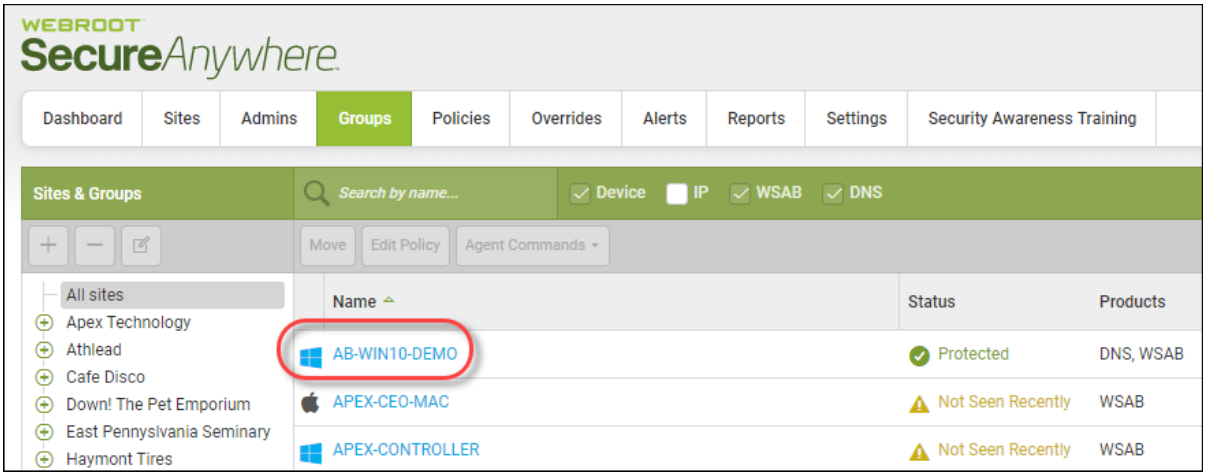
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

The complete list of devices displays.



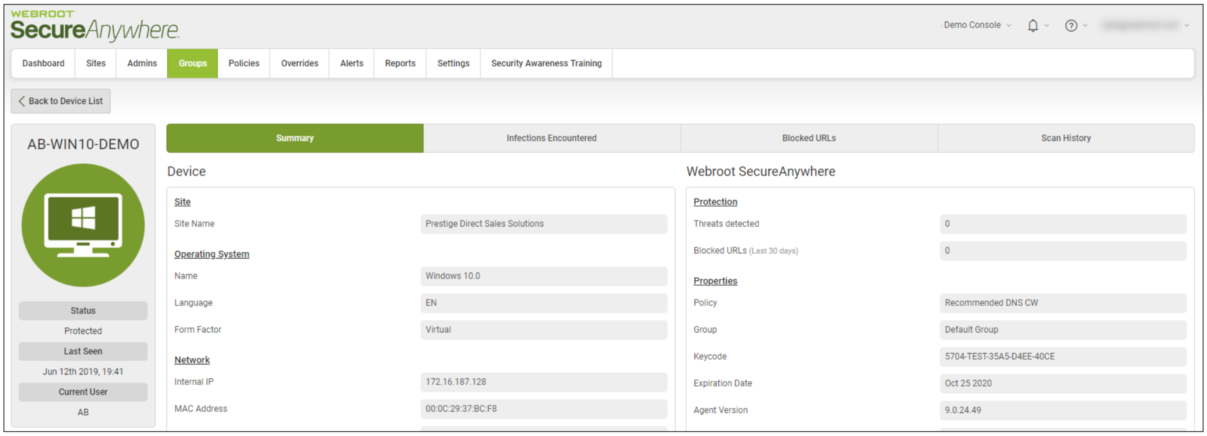
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

5. Click on a device you want to display a scan history for.



| Name | Status | Products |
|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB |
| APEX-CEO-MAC | Not Seen Recently | WSAB |
| APEX-CONTROLLER | Not Seen Recently | WSAB |

The Summary panel displays with the Summary tab active.



AB-WIN10-DEMO

| | |
|---|---|
| Status | Protected |
| Last Seen | Jun 12th 2019, 19:41 |
| Current User | AB |

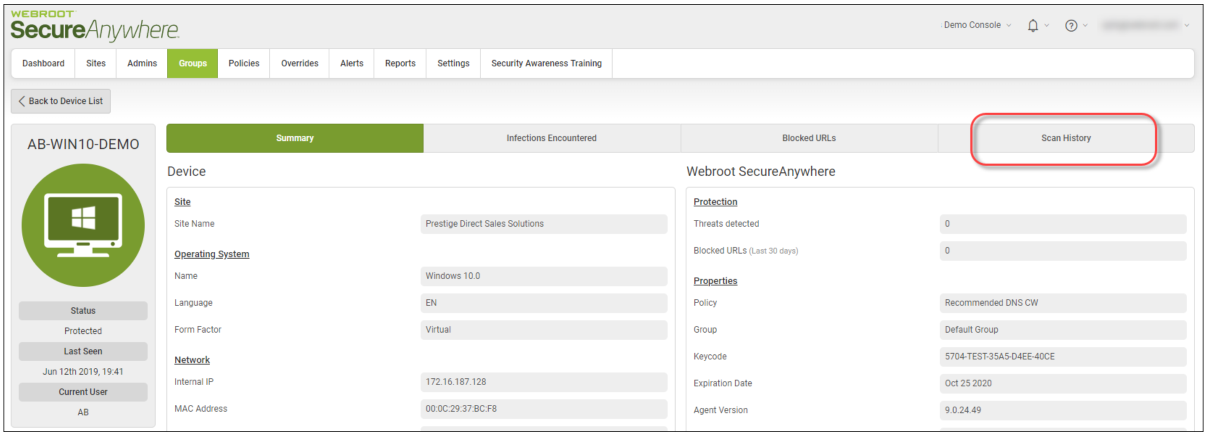
Device

| | |
|---|---|
| **Site** | |
| Site Name | Prestige Direct Sales Solutions |
| **Operating System** | |
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Virtual |
| **Network** | |
| Internal IP | 172.16.187.128 |
| MAC Address | 00:0C:29:37:BC:F8 |

Webroot SecureAnywhere

| | |
|---|---|
| **Protection** | |
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |
| **Properties** | |
| Policy | Recommended DNS CW |
| Group | Default Group |
| Keycode | 5704-TEST-35A5-D4EE-40CE |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |

6. Click the **Scan History** tab.



AB-WIN10-DEMO

| | |
|---|---|
| Status | Protected |
| Last Seen | Jun 12th 2019, 19:41 |
| Current User | AB |

Device

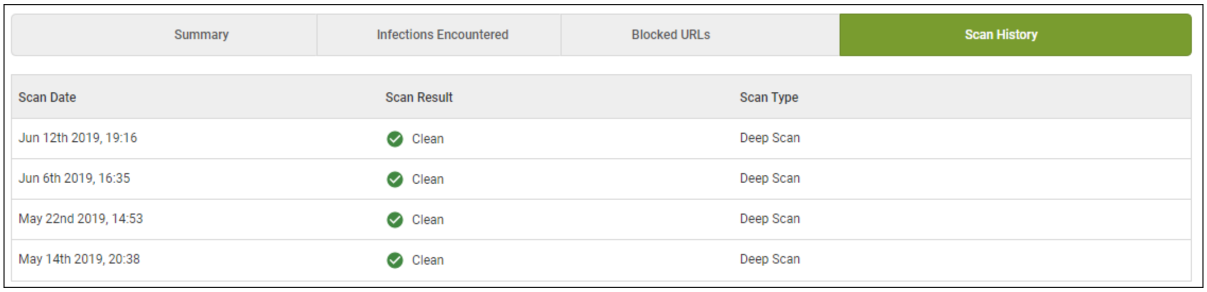
| | |
|---|---|
| **Site** | |
| Site Name | Prestige Direct Sales Solutions |
| **Operating System** | |
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Virtual |
| **Network** | |
| Internal IP | 172.16.187.128 |
| MAC Address | 00:0C:29:37:BC:F8 |

Webroot SecureAnywhere

| | |
|---|---|
| **Protection** | |
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |
| **Properties** | |
| Policy | Recommended DNS CW |
| Group | Default Group |
| Keycode | 5704-TEST-35A5-D4EE-40CE |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |

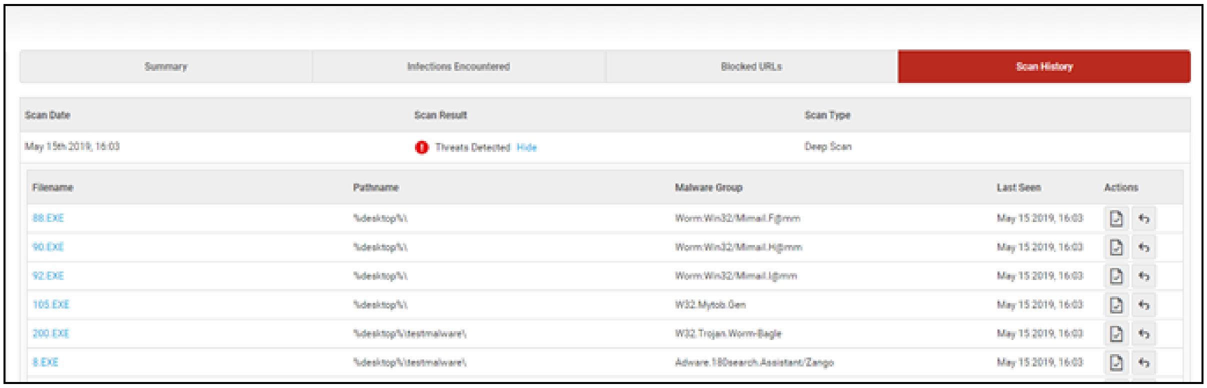
The scan history for that device displays, including the following information:

- Scan Date
- Scan Result
- Scan Type



| Scan Date | Scan Result | Scan Type |
|---|---|---|
| Jun 12th 2019, 19:16 | ✓ Clean | Deep Scan |
| Jun 6th 2019, 16:35 | ✓ Clean | Deep Scan |
| May 22nd 2019, 14:53 | ✓ Clean | Deep Scan |
| May 14th 2019, 20:38 | ✓ Clean | Deep Scan |

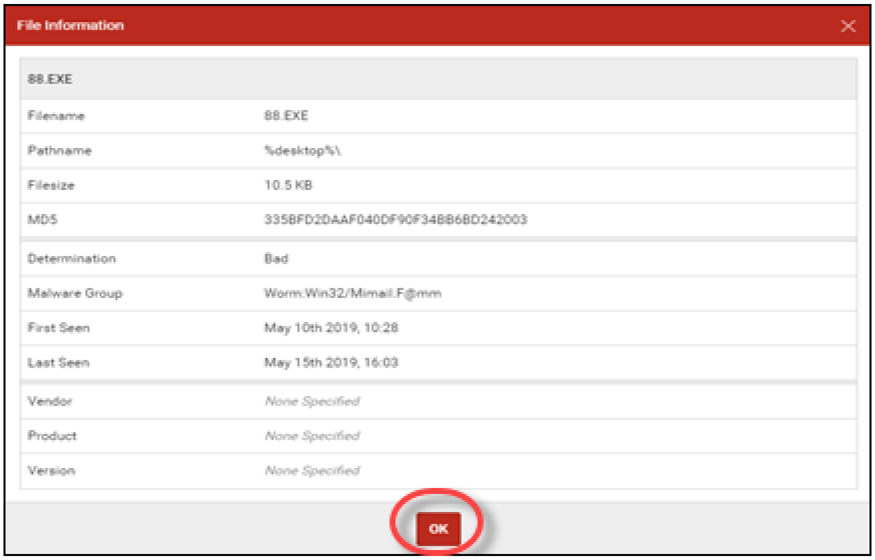
If any threats are detected, you can click on the file name to view information about the infection encountered.



| Scan Date | Scan Result | Scan Type |
|---|---|---|
| May 15th 2019, 16:03 | ! Threats Detected Hide | Deep Scan |

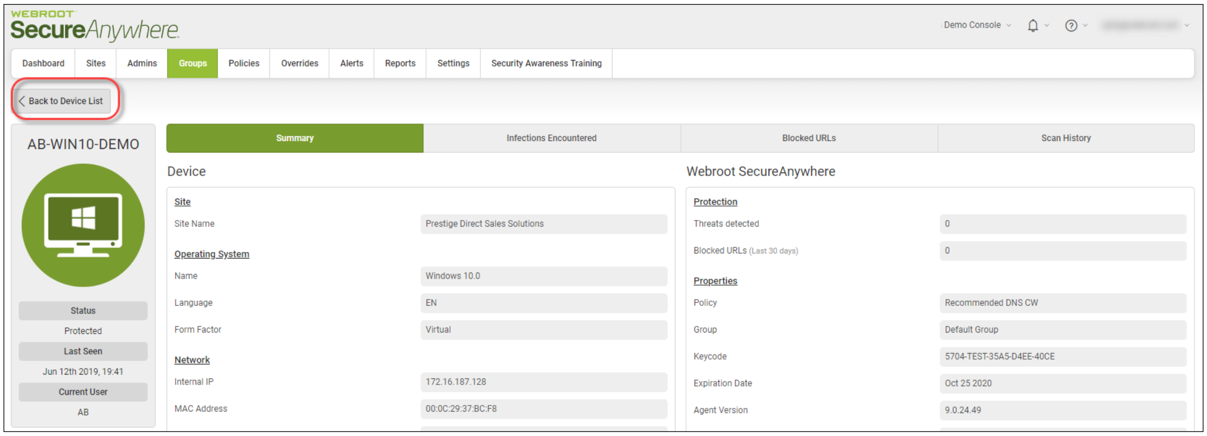
| Filename | Pathname | Malware Group | Last Seen | Actions |
|---|---|---|---|---|
| 88.EXE | %desktop%\ | Worm:Win32/Mimail.F@mm | May 15 2019, 16:03 | |
| 90.EXE | %desktop%\ | Worm:Win32/Mimail.H@mm | May 15 2019, 16:03 | |
| 92.EXE | %desktop%\ | Worm:Win32/Mimail.I@mm | May 15 2019, 16:03 | |
| 105.EXE | %desktop%\ | W32.Mytob.Gen | May 15 2019, 16:03 | |
| 200.EXE | %desktop%\testmalware\ | W32.Trojan.Worm-Bagle | May 15 2019, 16:03 | |
| 8.EXE | %desktop%\testmalware\ | Adware.180search.Assistant/Zango | May 15 2019, 16:03 | |

7. Click the **OK** button after you are done reviewing the information to return to the Scan History tab.



| 88.EXE | |
|---|---|
| Filename | 88.EXE |
| Pathname | %desktop%\ |
| Filesize | 10.5 KB |
| MD5 | 335BFD2DAAF040DF90F34BB6BD242003 |
| Determination | Bad |
| Malware Group | Worm:Win32/Mimail.F@mm |
| First Seen | May 10th 2019, 10:28 |
| Last Seen | May 15th 2019, 16:03 |
| Vendor | *None Specified* |
| Product | *None Specified* |
| Version | *None Specified* |

8. When you're done, click the **Back to Device List** button to return to the list of devices.



AB-WIN10-DEMO

Status: Protected
Last Seen: Jun 12th 2019, 19:41
Current User: AB

Device

Site

| | |
|---|---|
| Site Name | Prestige Direct Sales Solutions |

Operating System

| | |
|---|---|
| Name | Windows 10.0 |
| Language | EN |
| Form Factor | Virtual |

Network

| | |
|---|---|
| Internal IP | 172.16.187.128 |
| MAC Address | 00:0C:29:37:BC:F8 |

Webroot SecureAnywhere

Protection

| | |
|---|---|
| Threats detected | 0 |
| Blocked URLs (Last 30 days) | 0 |

Properties

| | |
|---|---|
| Policy | Recommended DNS CW |
| Group | Default Group |
| Keycode | 5704-TEST-35A5-D4EE-40CE |
| Expiration Date | Oct 25 2020 |
| Agent Version | 9.0.24.49 |

# Issuing Agent Commands

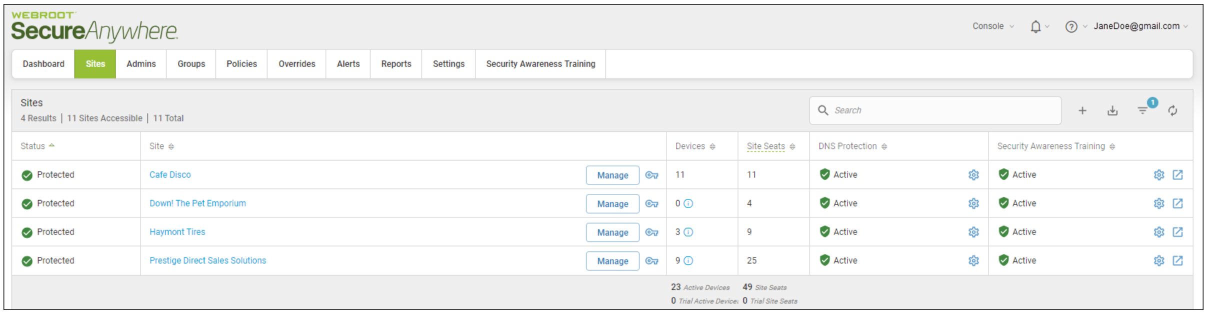
Follow this procedure to issue agent commands from the Groups tab.

> **Note:** The Agent Command drop-down menu only becomes active after you have selected one or more multiple devices from the list of devices.

**To issue an agent command:**

1. Log in to the management console.

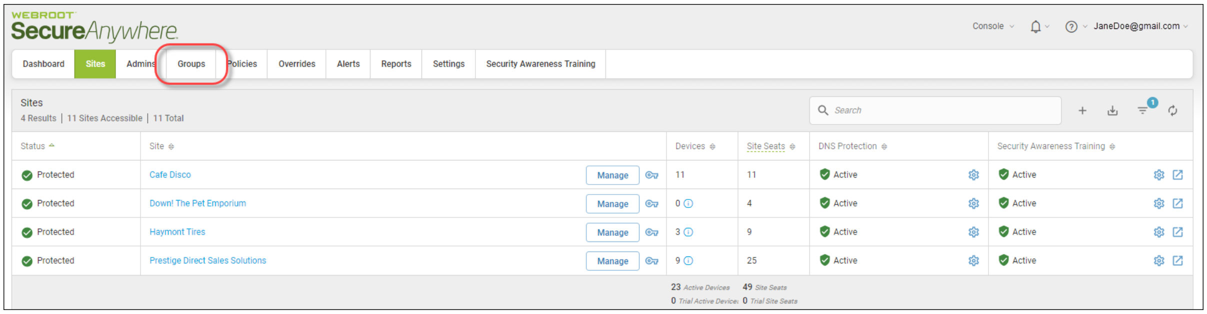
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

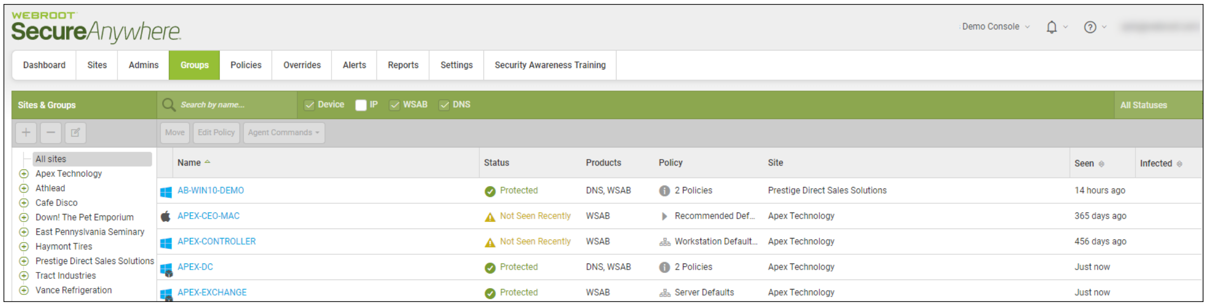
2. Click the **Groups** tab.


WEBROOT SecureAnywhere
Console
JaneDoe@gmail.com
Dashboard
Sites
Admins
Groups
Policies
Overrides
Alerts
Reports
Settings
Security Awareness Training
Search

Sites
4 Results | 11 Sites Accessible | 11 Total

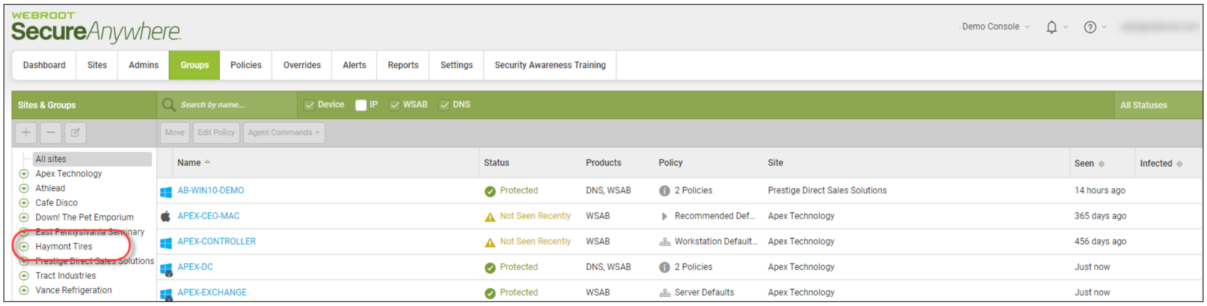
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



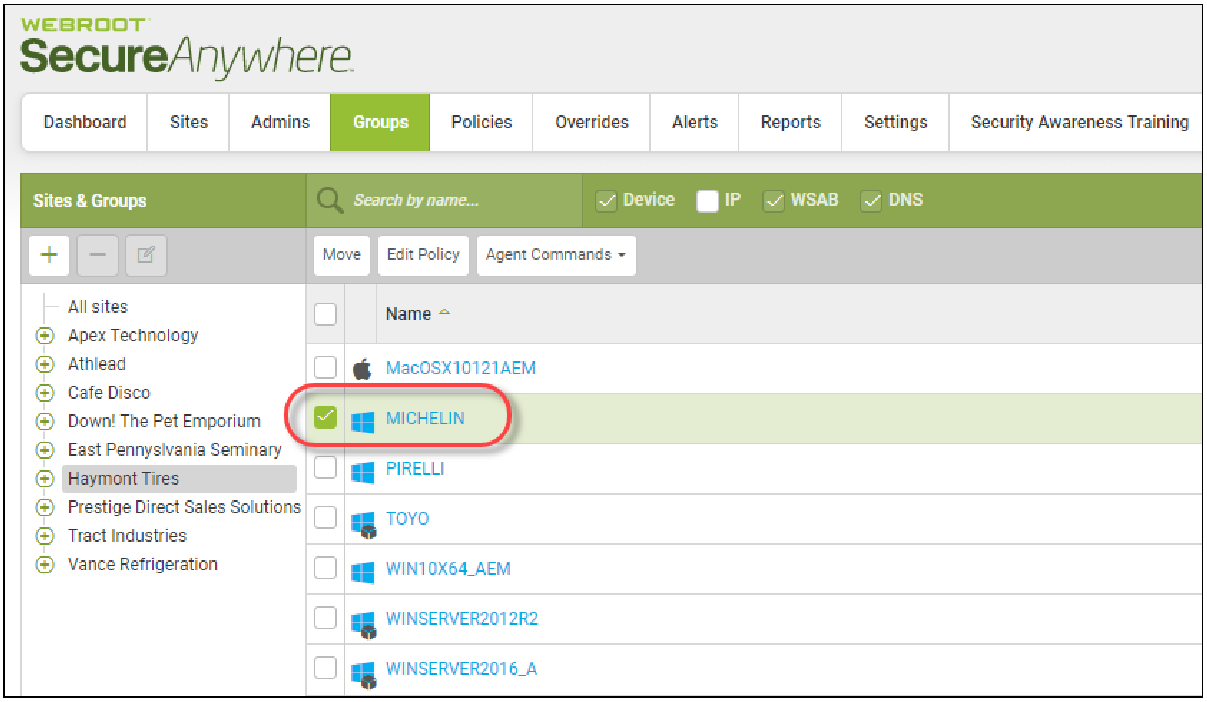
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

3. In the left column, select the site that contains the group and device you want to issue an agent command for.



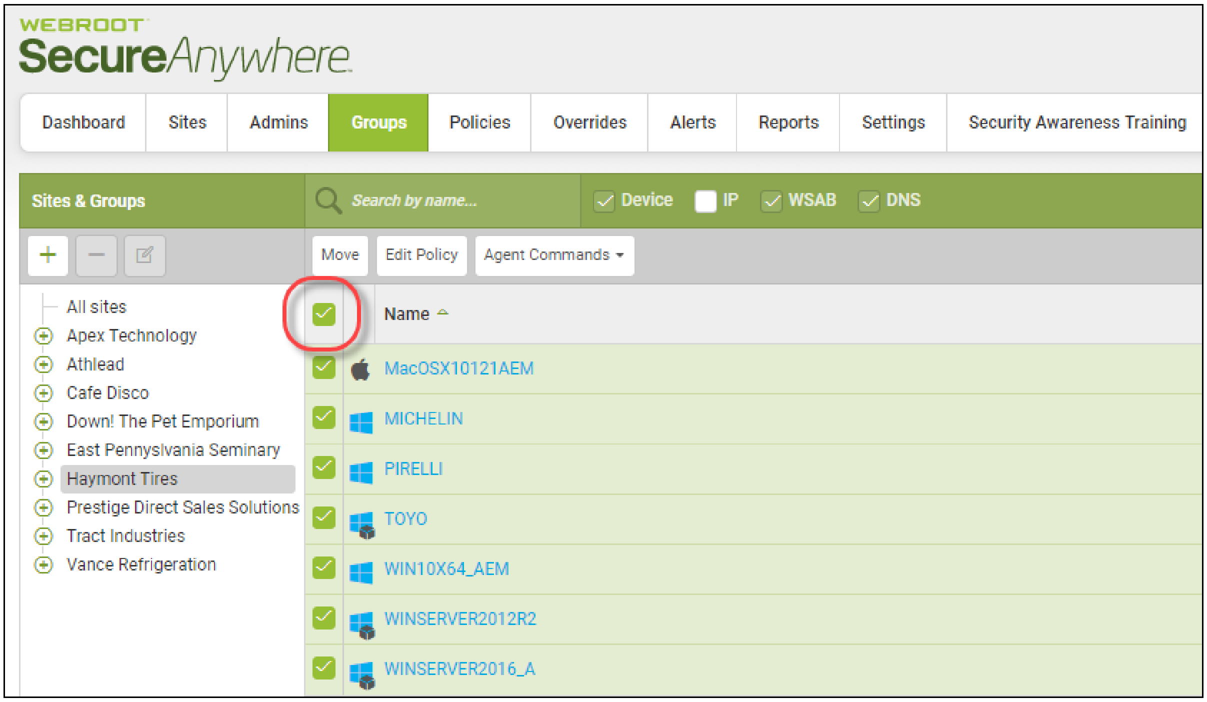
| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

4. In the Devices panel, select the device that you want to issue an agent command for.



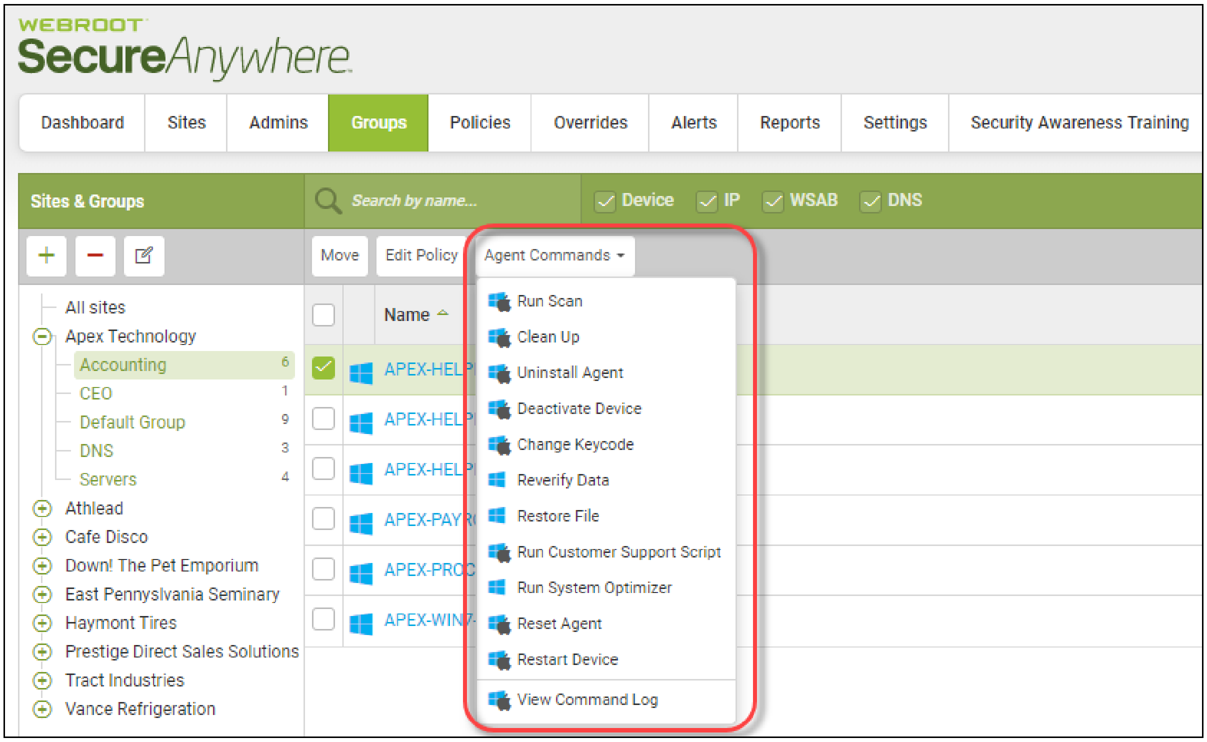
| ☐ | Name |
|---|---|
| ☐ | MacOSX10121AEM |
| ☑ | MICHELIN |
| ☐ | PIRELLI |
| ☐ | TOYO |
| ☐ | WIN10X64_AEM |
| ☐ | WINSERVER2012R2 |
| ☐ | WINSERVER2016_A |

To select all devices, select the checkbox at the top of the column.

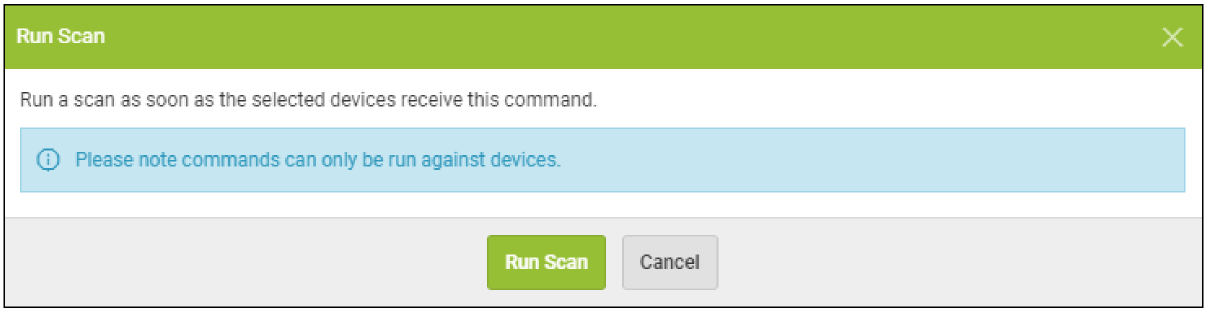


| ☑ | Name |
|---|---|
| ☑ | MacOSX10121AEM |
| ☑ | MICHELIN |
| ☑ | PIRELLI |
| ☑ | TOYO |
| ☑ | WIN10X64_AEM |
| ☑ | WINSERVER2012R2 |
| ☑ | WINSERVER2016_A |

5. Select a policy from the Agent Commands drop-down menu.



A confirmation window displays similar to the one displayed. Click **Run** or **Cancel**.


Run Scan

Run a scan as soon as the selected devices receive this command.

Please note commands can only be run against devices.

6. Additionally from the Agent Commands drop-down menu, you can select **View Command Log**. For more information, see *Viewing Agent Command Logs on page 288*.

# Viewing Agent Command Logs

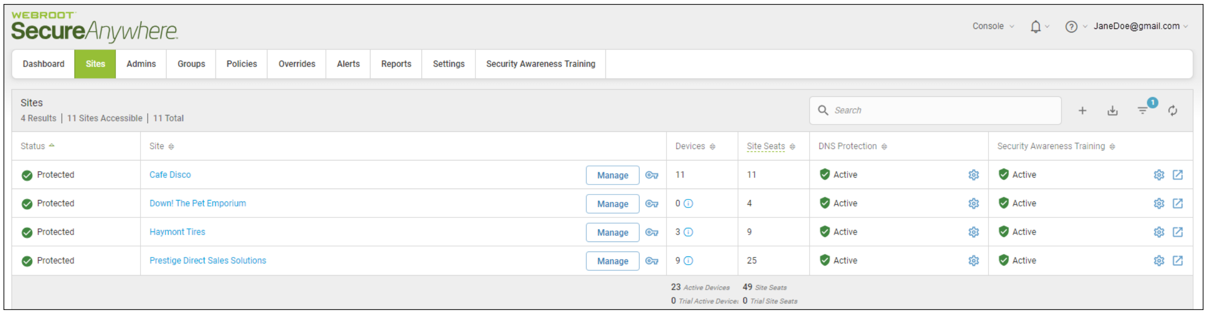
Follow this procedure to view information about commands that you have sent to devices.

> **Note:** The Agent Command drop-down menu only becomes active after you have selected one or more multiple devices from the list of devices.

**To view an agent command log:**

1. Log in to the management console.

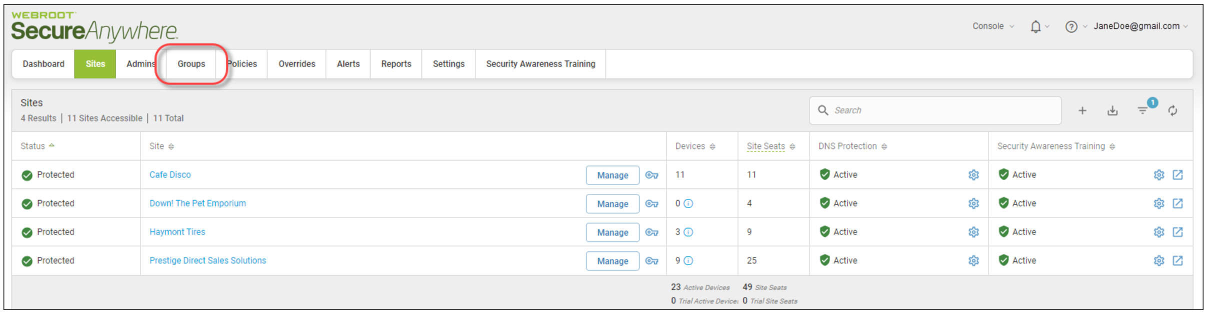
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

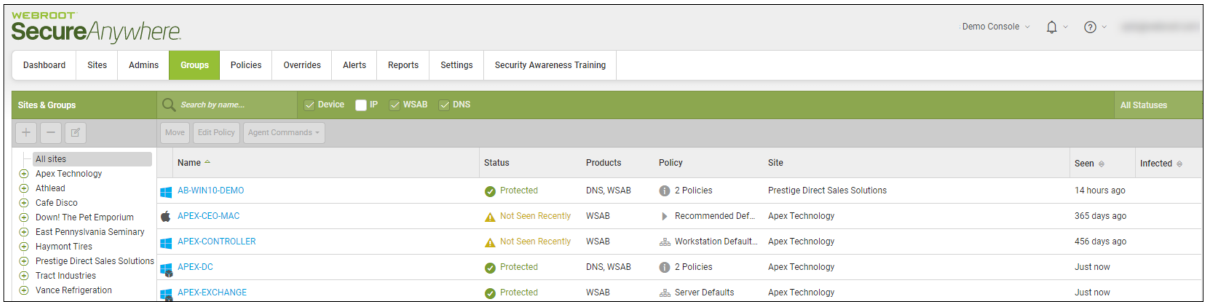
2. Click the **Groups** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

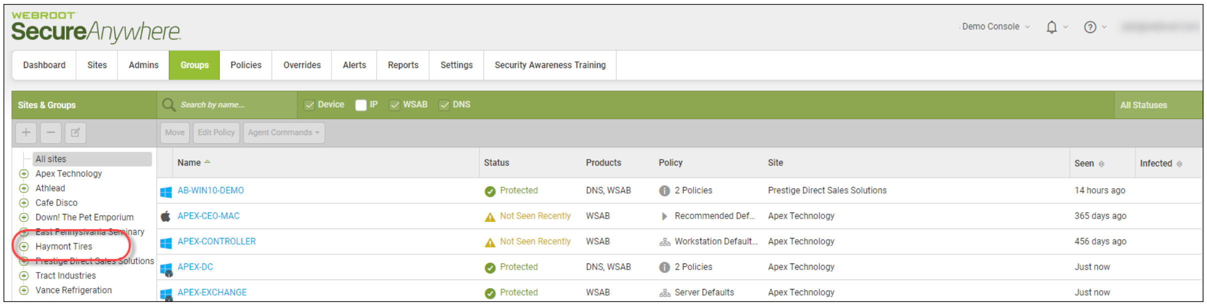
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Groups tab displays.



| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

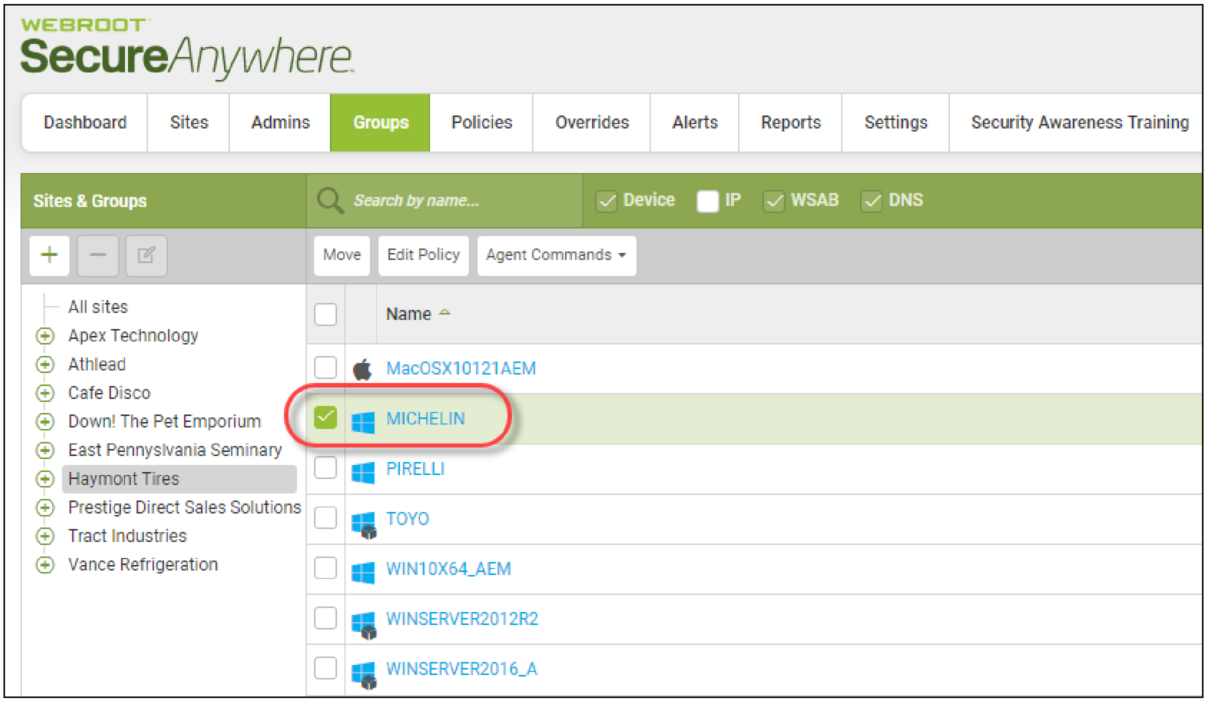
3. In the left column, select the site that contains the group and device you want to view an agent command log for.



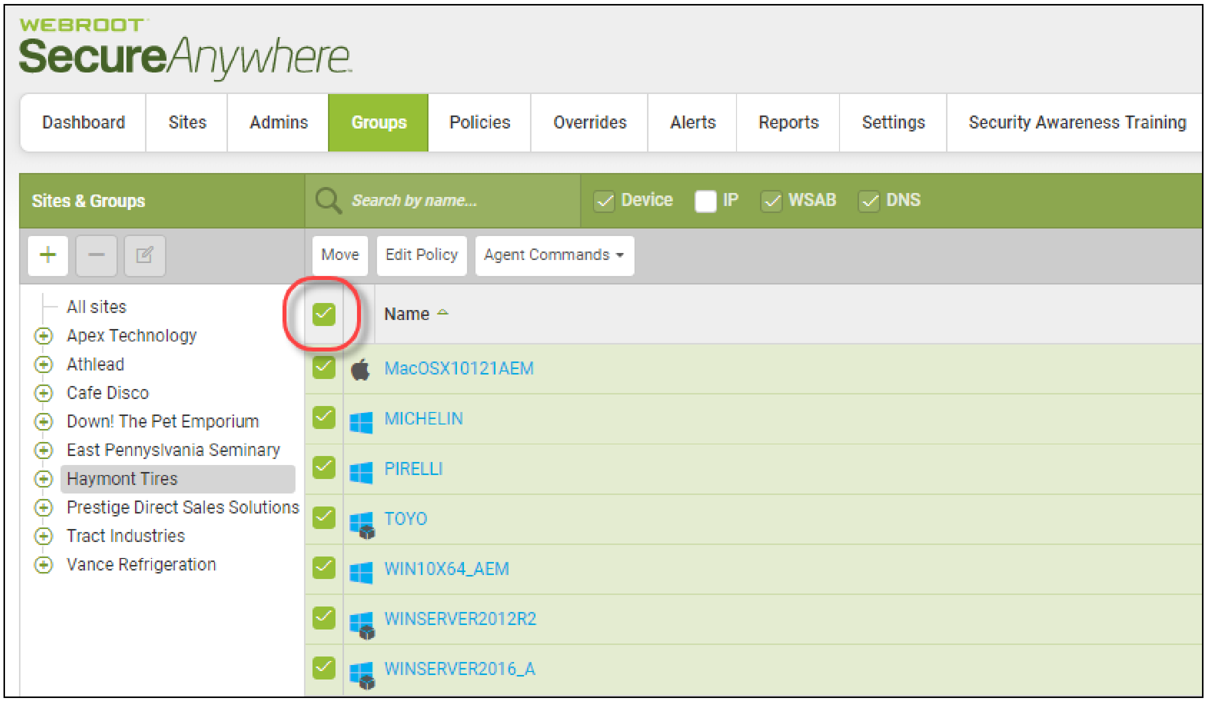
WEBROOT
SecureAnywhere
Demo Console
[redacted]
Dashboard
Sites
Admins
Groups
Policies
Overrides
Alerts
Reports
Settings
Security Awareness Training
Sites & Groups
Search by name...
☑ Device
☐ IP
☑ WSAB
☑ DNS
All Statuses
Move
Edit Policy
Agent Commands
All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennsylvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration

| Name | Status | Products | Policy | Site | Seen | Infected |
|---|---|---|---|---|---|---|
| AB-WIN10-DEMO | Protected | DNS, WSAB | 2 Policies | Prestige Direct Sales Solutions | 14 hours ago | |
| APEX-CEO-MAC | Not Seen Recently | WSAB | Recommended Def... | Apex Technology | 365 days ago | |
| APEX-CONTROLLER | Not Seen Recently | WSAB | Workstation Default... | Apex Technology | 456 days ago | |
| APEX-DC | Protected | DNS, WSAB | 2 Policies | Apex Technology | Just now | |
| APEX-EXCHANGE | Protected | WSAB | Server Defaults | Apex Technology | Just now | |

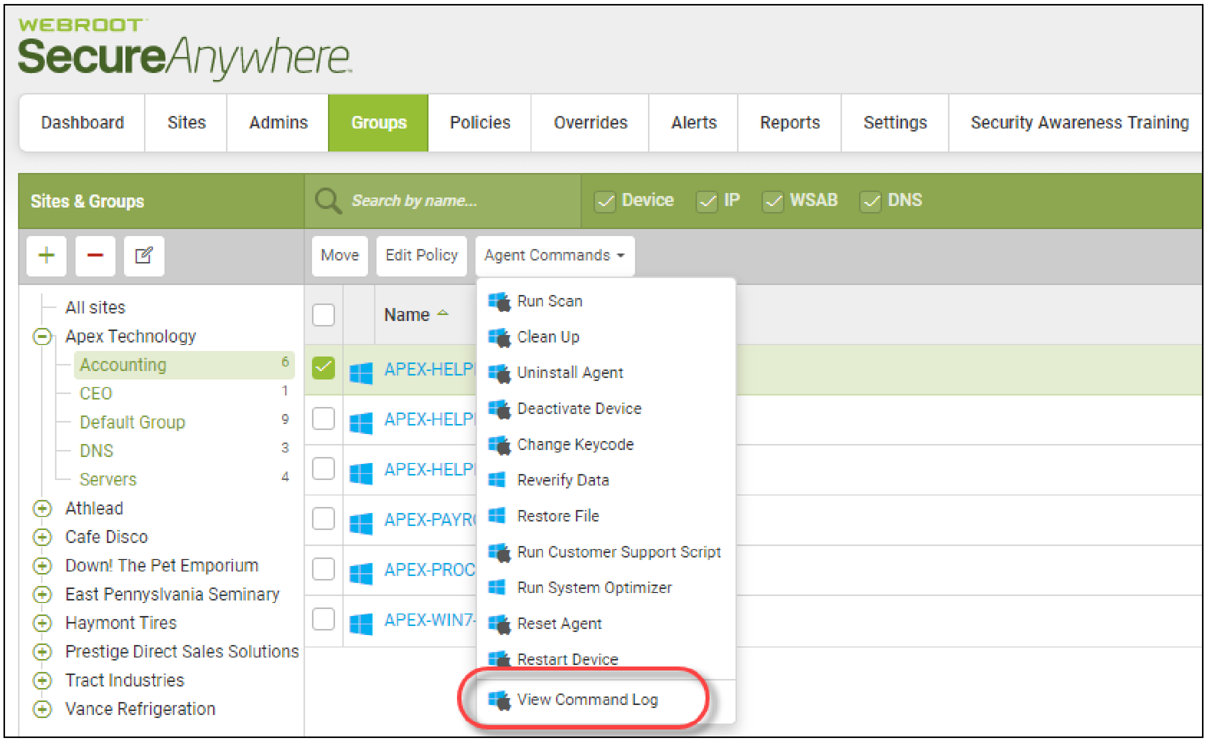
4. In the Devices panel, select the device that you want to view an agent command log for.



To select all devices, select the checkbox at the top of the column.


WEBROOT
SecureAnywhere
Dashboard
Sites
Admins
Groups
Policies
Overrides
Alerts
Reports
Settings
Security Awareness Training
Sites & Groups
Search by name...
☑ Device
□ IP
☑ WSAB
☑ DNS
Move
Edit Policy
Agent Commands
All sites
Apex Technology
Athlead
Cafe Disco
Down! The Pet Emporium
East Pennyslvania Seminary
Haymont Tires
Prestige Direct Sales Solutions
Tract Industries
Vance Refrigeration
Name
MacOSX10121AEM
MICHELIN
PIRELLI
TOYO
WIN10X64_AEM
WINSERVER2012R2
WINSERVER2016_A

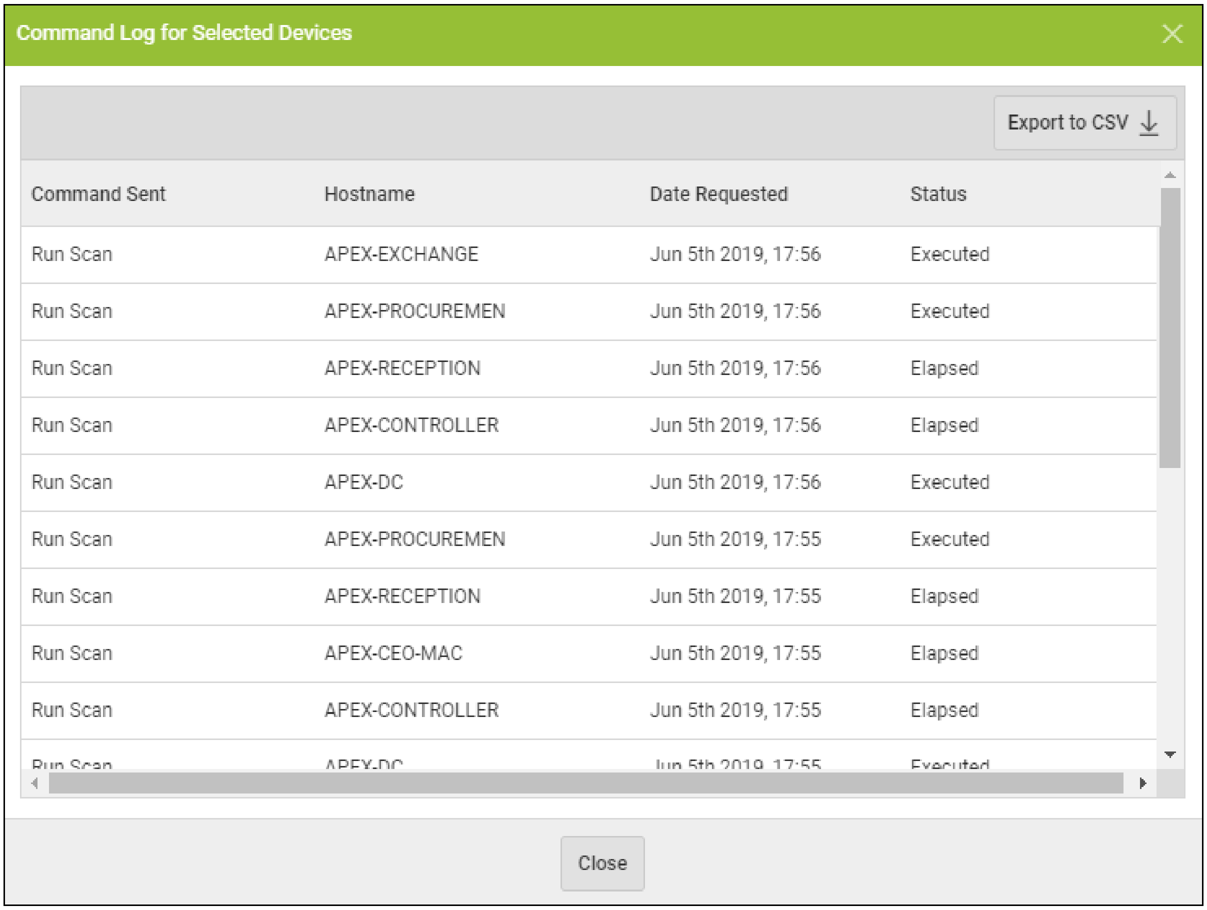
5. From the Agent Commands drop-down menu, select **View Command Log**.



A Command Log for Selected Devices window displays, and includes the following information:

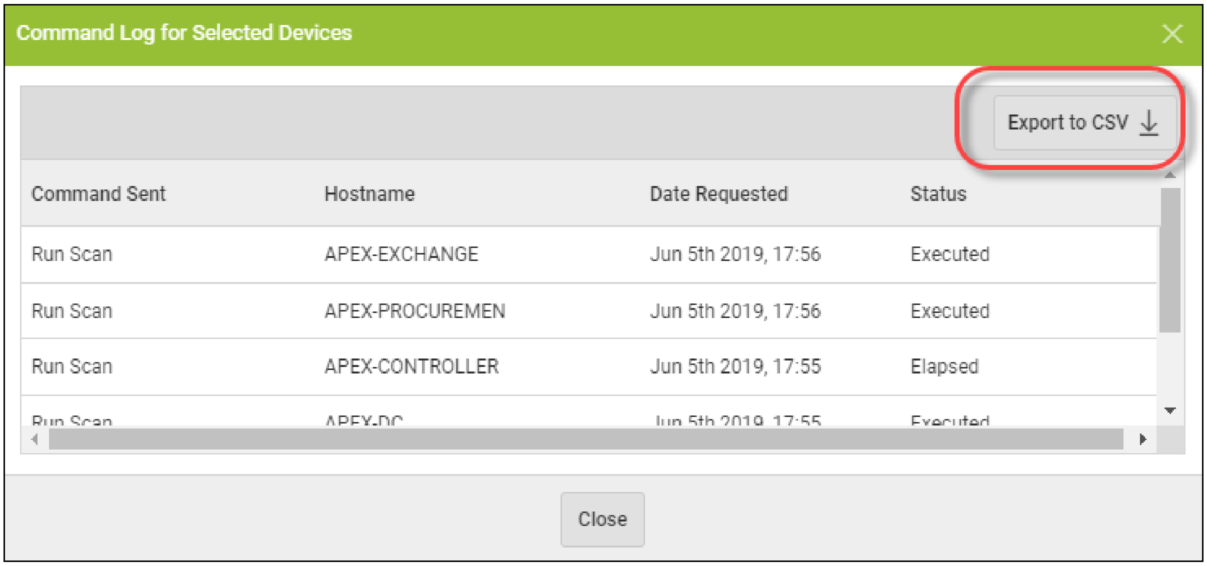
- Command Sent
- Hostname
- Date Requested

- Status



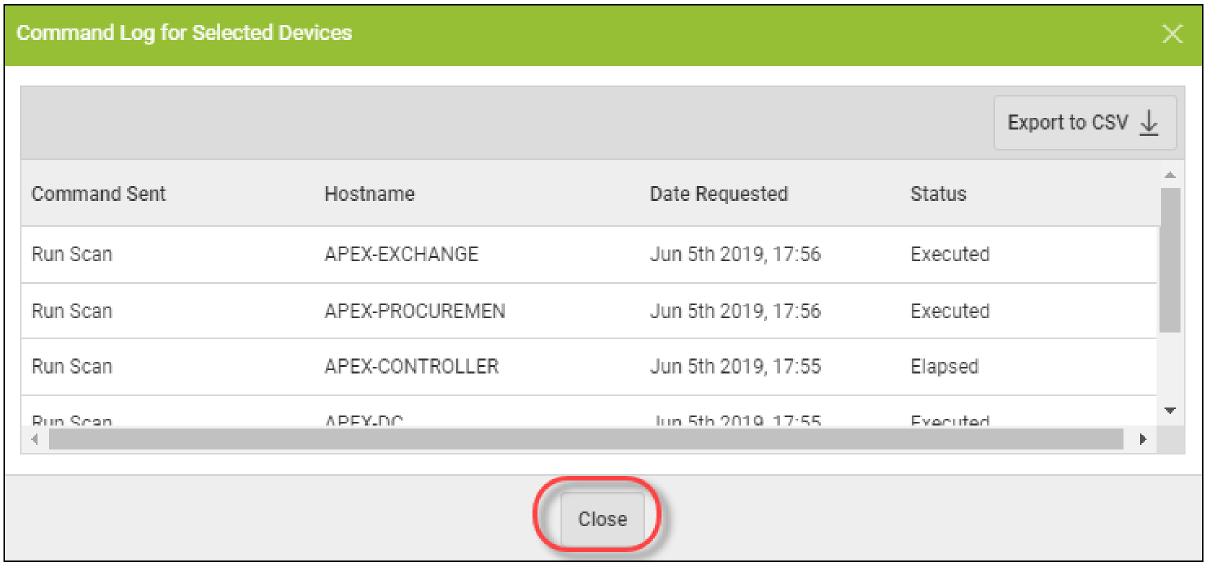
| Command Sent | Hostname | Date Requested | Status |
|---|---|---|---|
| Run Scan | APEX-EXCHANGE | Jun 5th 2019, 17:56 | Executed |
| Run Scan | APEX-PROCUREMEN | Jun 5th 2019, 17:56 | Executed |
| Run Scan | APEX-RECEPTION | Jun 5th 2019, 17:56 | Elapsed |
| Run Scan | APEX-CONTROLLER | Jun 5th 2019, 17:56 | Elapsed |
| Run Scan | APEX-DC | Jun 5th 2019, 17:56 | Executed |
| Run Scan | APEX-PROCUREMEN | Jun 5th 2019, 17:55 | Executed |
| Run Scan | APEX-RECEPTION | Jun 5th 2019, 17:55 | Elapsed |
| Run Scan | APEX-CEO-MAC | Jun 5th 2019, 17:55 | Elapsed |
| Run Scan | APEX-CONTROLLER | Jun 5th 2019, 17:55 | Elapsed |
| Run Scan | APEX-DC | Jun 5th 2019, 17:55 | Executed |

6. As needed, you can click the **Export to CSV** button to download a spreadsheet of the Agent Command Log.



| Command Sent | Hostname | Date Requested | Status |
|---|---|---|---|
| Run Scan | APEX-EXCHANGE | Jun 5th 2019, 17:56 | Executed |
| Run Scan | APEX-PROCUREMEN | Jun 5th 2019, 17:56 | Executed |
| Run Scan | APEX-CONTROLLER | Jun 5th 2019, 17:55 | Elapsed |
| Run Scan | APEX-DC | Jun 5th 2019, 17:55 | Executed |

7. When you are done, click the **Close** button.



| Command Sent | Hostname | Date Requested | Status |
|---|---|---|---|
| Run Scan | APEX-EXCHANGE | Jun 5th 2019, 17:56 | Executed |
| Run Scan | APEX-PROCUREMEN | Jun 5th 2019, 17:56 | Executed |
| Run Scan | APEX-CONTROLLER | Jun 5th 2019, 17:55 | Elapsed |
| Run Scan | APEX-DC | Jun 5th 2019, 17:55 | Executed |

# Chapter 7: Working With Policies

To work with policies, see the following topics:

# Creating Policies

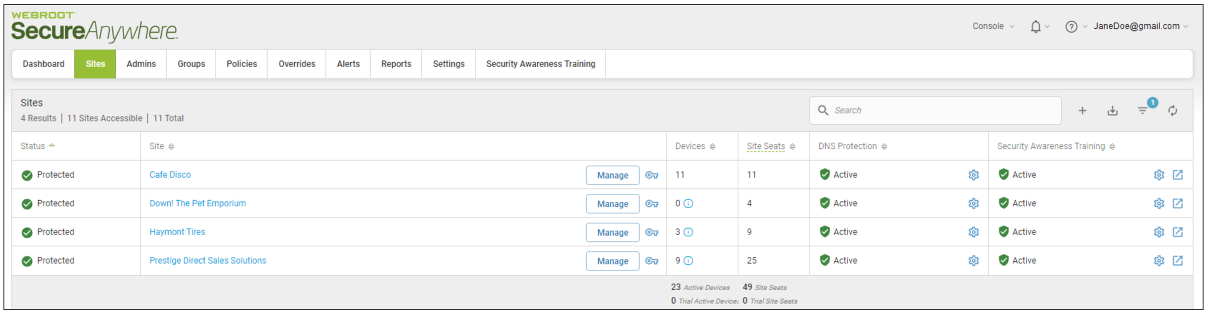
You can add policies in one of two ways, either by creating a new policy or by copying an existing policy as a starting point. Each method is described below. Once you have defined a policy name and given it a description, you can then determine the policy settings as described in . For information on deleting policies, see *Editing Policies on page 302*.

> **Note:**Policy names must be unique, so plan your policies in advance to avoid conflicts later. Once you give a policy a name, you cannot re-use that same name even after a policy has been deleted.

**To create a new policy:**

1. Log in to the management console.

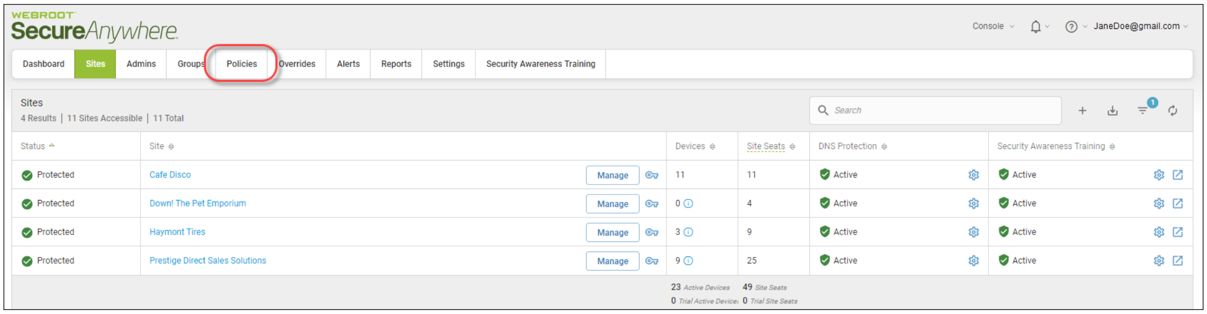
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

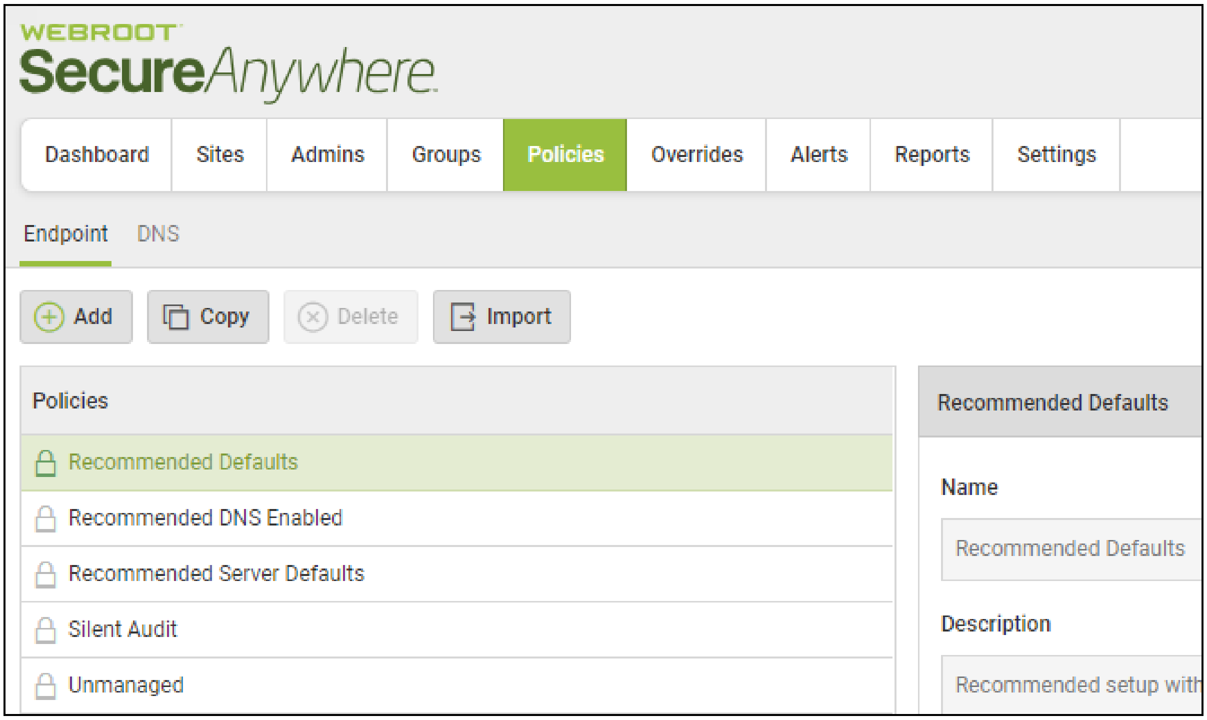
2. Click the **Policies** tab.



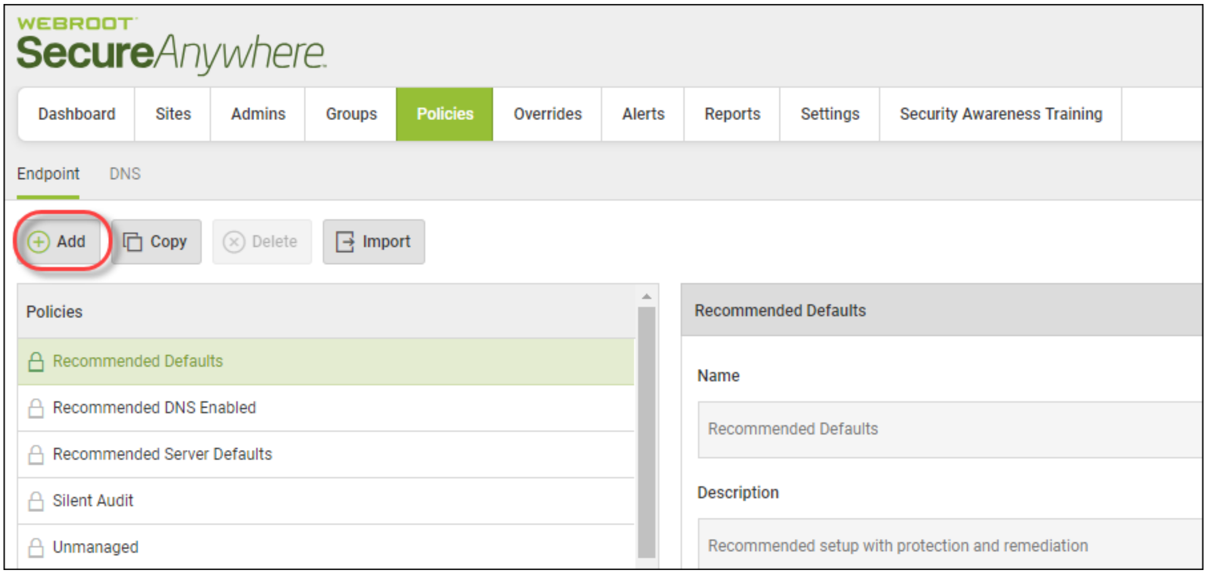
Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

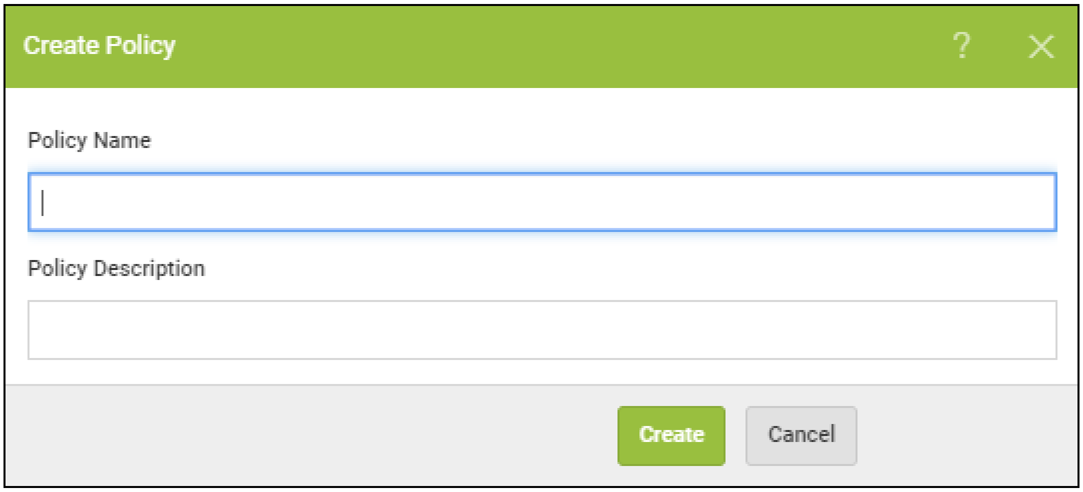
   The Policies tab displays.



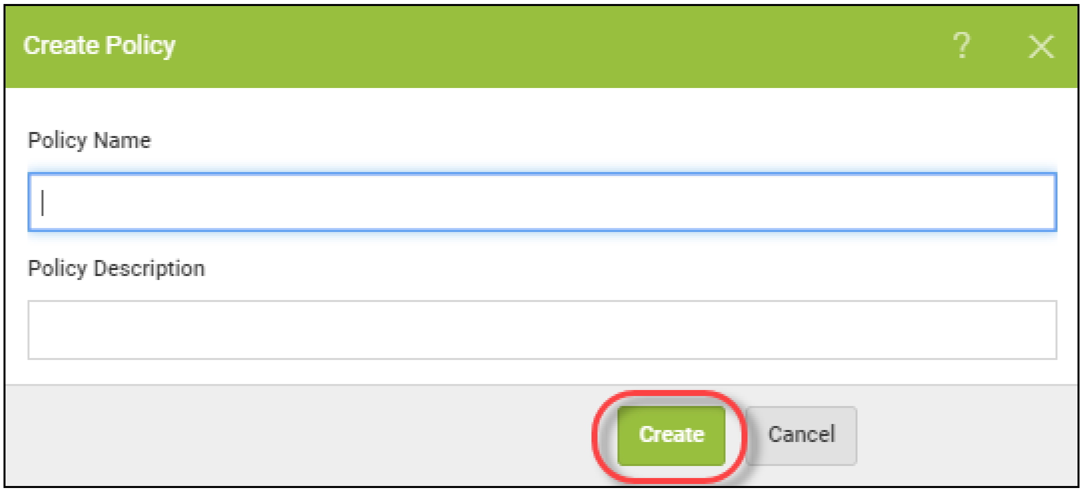
3. Click the **Add** button.



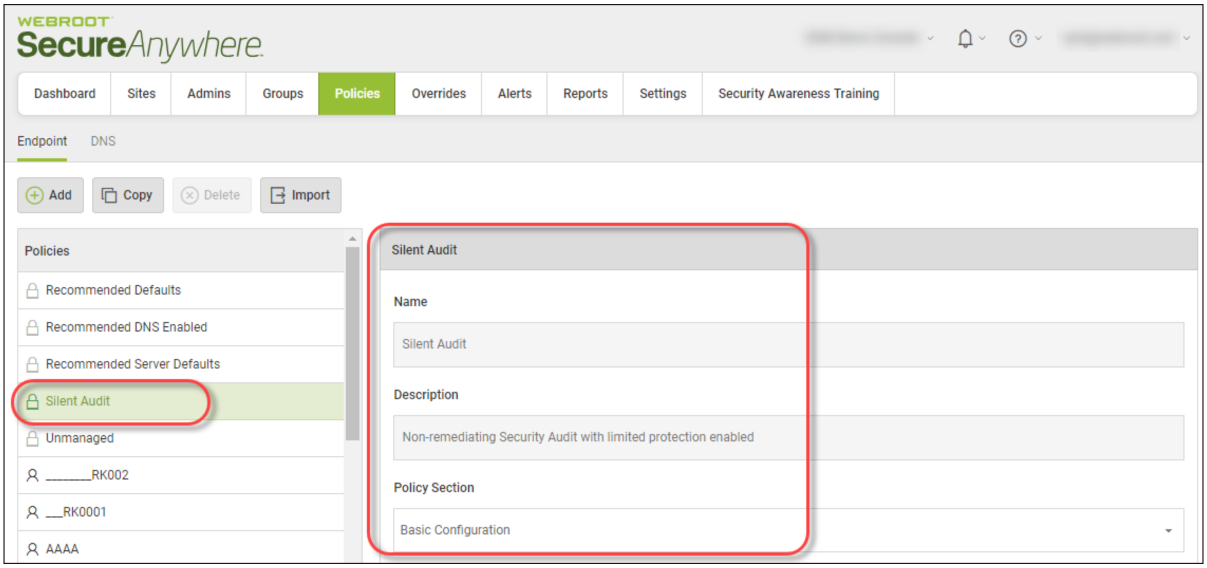
The Create Policy window displays.



4. In the Create Policy window, enter a policy name and description of up to 50 alphanumeric characters, then click the **Create Policy** button.



5. Locate your new policy in the Policy tab. Double-click the policy you just created to view and modify the settings.



Policies

- Recommended Defaults
- Recommended DNS Enabled
- Recommended Server Defaults
- Silent Audit
- Unmanaged
- ________RK002
- __RK0001
- AAAA

Silent Audit

Name

Silent Audit

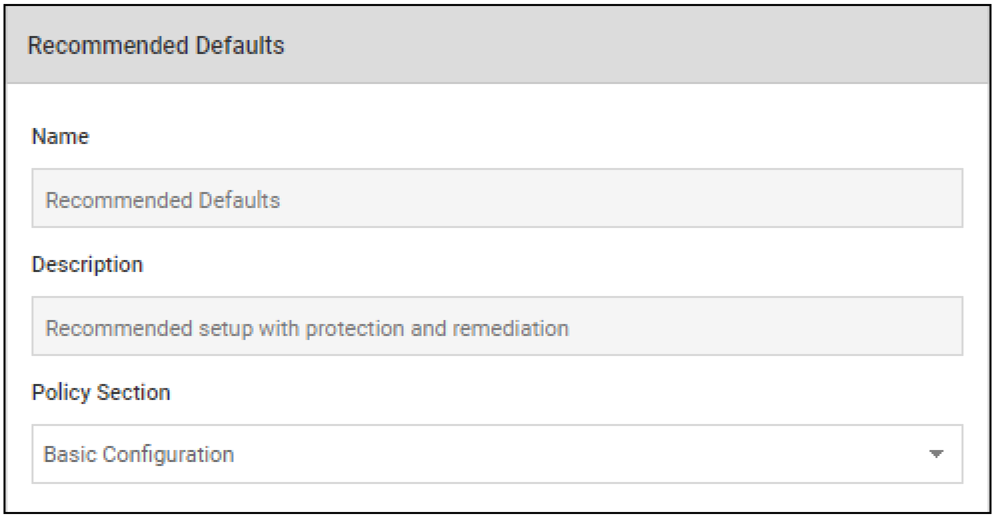
Description

Non-remediating Security Audit with limited protection enabled

Policy Section

Basic Configuration

The settings window for that policy displays, with the Recommended Defaults at the top.



Recommended Defaults

Name

Recommended Defaults

Description

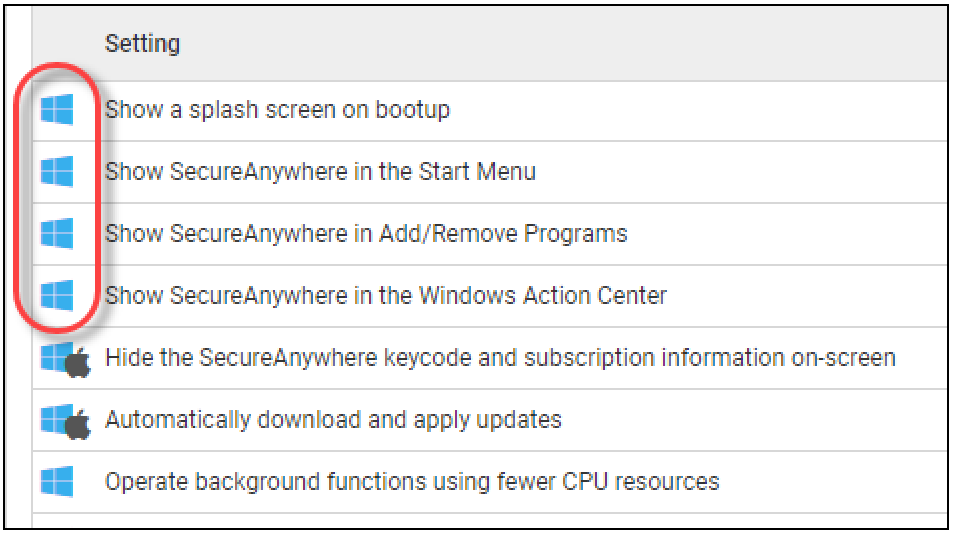
Recommended setup with protection and remediation

Policy Section

Basic Configuration

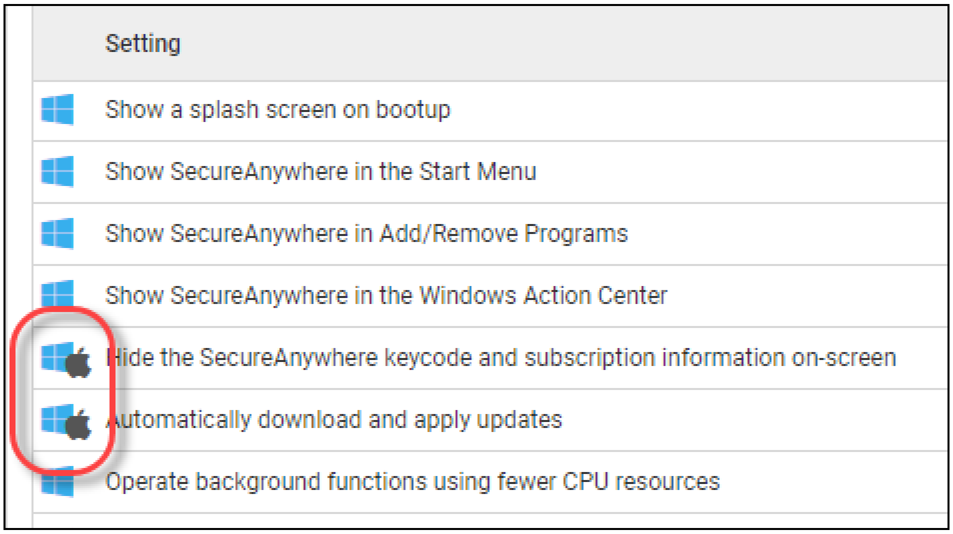
The Setting column displays the name of the policy, in addition to which:

- Settings that apply to PC only are indicated by the Windows icon.



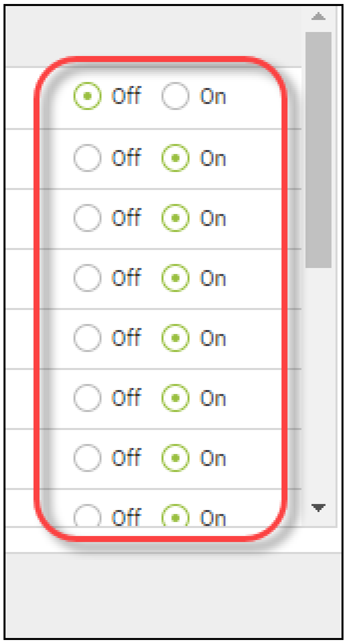
| Setting |
|---|
| Show a splash screen on bootup |
| Show SecureAnywhere in the Start Menu |
| Show SecureAnywhere in Add/Remove Programs |
| Show SecureAnywhere in the Windows Action Center |
| Hide the SecureAnywhere keycode and subscription information on-screen |
| Automatically download and apply updates |
| Operate background functions using fewer CPU resources |

- Settings that apply to PC and Mac are indicated by both the Windows icon and the Mac icon.



| Setting |
|---|
| Show a splash screen on bootup |
| Show SecureAnywhere in the Start Menu |
| Show SecureAnywhere in Add/Remove Programs |
| Show SecureAnywhere in the Windows Action Center |
| Hide the SecureAnywhere keycode and subscription information on-screen |
| Automatically download and apply updates |
| Operate background functions using fewer CPU resources |

The On/Off column displays how the setting is currently implemented on the endpoints.



● Off ○ On

○ Off ● On

○ Off ● On

○ Off ● On

○ Off ● On

○ Off ● On

○ Off ● On

○ Off ● On

# Editing Policies

Once you create a policy, you can edit its settings to suit your business purposes. For more information, see *Creating Policies on page 296*.

**Note:** You cannot change Webroot default policy settings.

The following policies control management console sites.

| SECTION | DESCRIPTION |
|---|---|
| Basic Configuration | General preferences that change the behavior of the SecureAnywhere program, such as whether the program icon displays in the endpoint's system tray and whether the user can shut down the program. |
| Scan Schedule | Allows you to run scans at different times, change the scanning behavior, or turn off automatic scanning. If you do not modify the scan schedule, SecureAnywhere launches scans automatically every day, at about the same time you installed the software. |
| Scan Settings | Provides more control over scans, such as performing a more thorough scan. |
| Self Protection | Provides additional protection that prevents malicious software from modifying the SecureAnywhere program settings and processes on the endpoint. If SecureAnywhere detects another product attempting to interfere with its functions, it launches a protective scan to look for threats. |

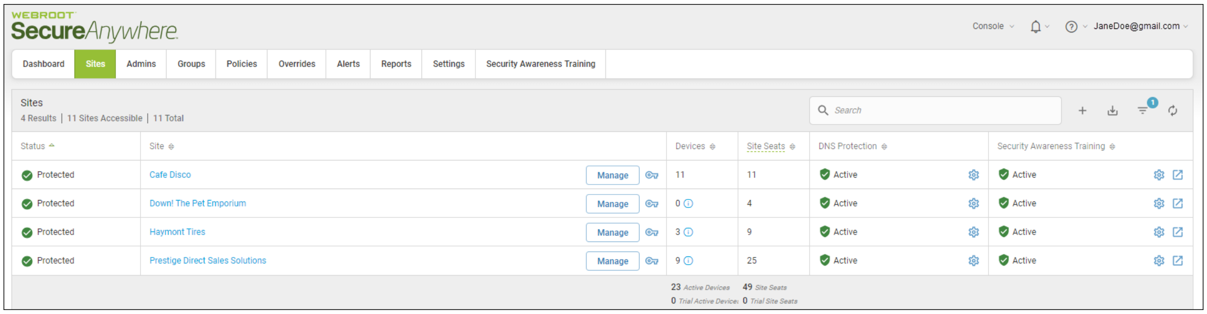
| SECTION | DESCRIPTION |
|---|---|
| Heuristics | Provides threat analysis that SecureAnywhere performs when scanning endpoints. Heuristics can be adjusted for separate areas of the endpoints, including the local drive, USB drives, the Internet, the network, CD/DVDs, and when the endpoint is offline. |
| Realtime Shield | Blocks known threats listed in Webroot's threat definitions and in Webroot's community database. |
| Behavior Shield | Analyzes applications and processes running on the endpoints. |
| Core System Shield | Monitors the computer system structures to ensure that malware has not tampered with them. |
| Web Threat Shield | Protects endpoints as users surf the Internet and click links in search results. |
| Identity Shield | Protects from identity theft and financial loss. It ensures that sensitive data is protected, while safe-guarding users from keyloggers, screen-grabbers, and other information-stealing techniques. |
| Firewall | Monitors data traffic traveling out of computer ports. It looks for untrusted processes that try to connect to the Internet and steal personal information. The Webroot firewall works in conjunction with the Windows firewall, which monitors data traffic coming into the endpoints. |

| SECTION | DESCRIPTION |
|---|---|
| User Interface | Provides user access to the SecureAnywhere program on the endpoint. |
| System Optimizer | Controls System Optimizer behavior, such as an automatic optimization schedule and what types of files and traces to remove from the endpoint. |
| Evasion Shield | Detects, blocks, and remediates (quarantines) evasive attacks, whether they are file-based, fileless, obfuscated, or encrypted, and prevents malicious behaviors from executing. |

**To edit a policy:**

1. Log in to the management console.

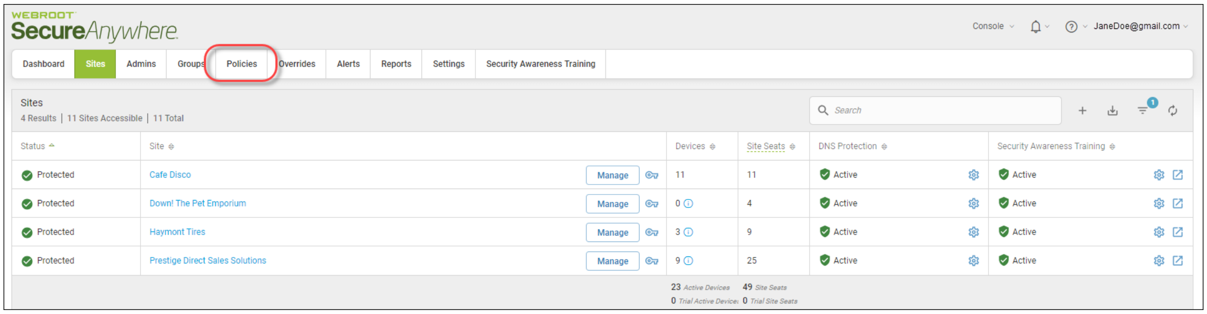
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

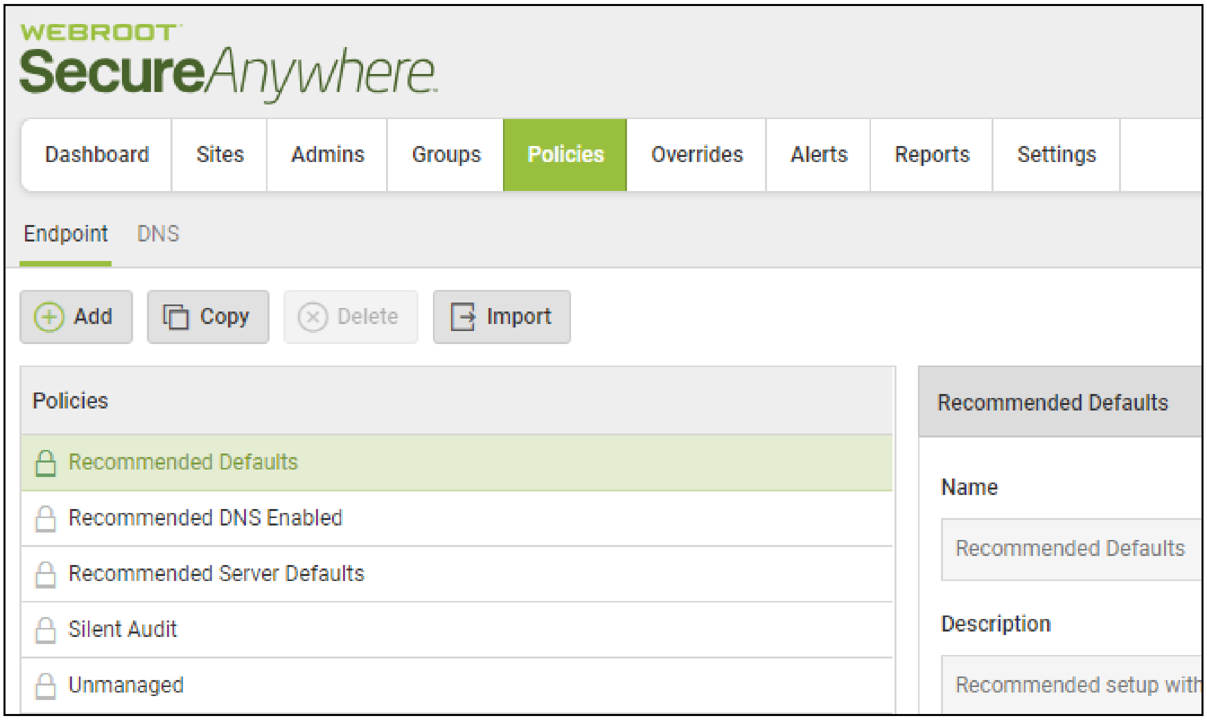
2. Click the **Policies** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

The Policies tab displays.



Policies

- Recommended Defaults
- Recommended DNS Enabled
- Recommended Server Defaults
- Silent Audit
- Unmanaged

Recommended Defaults

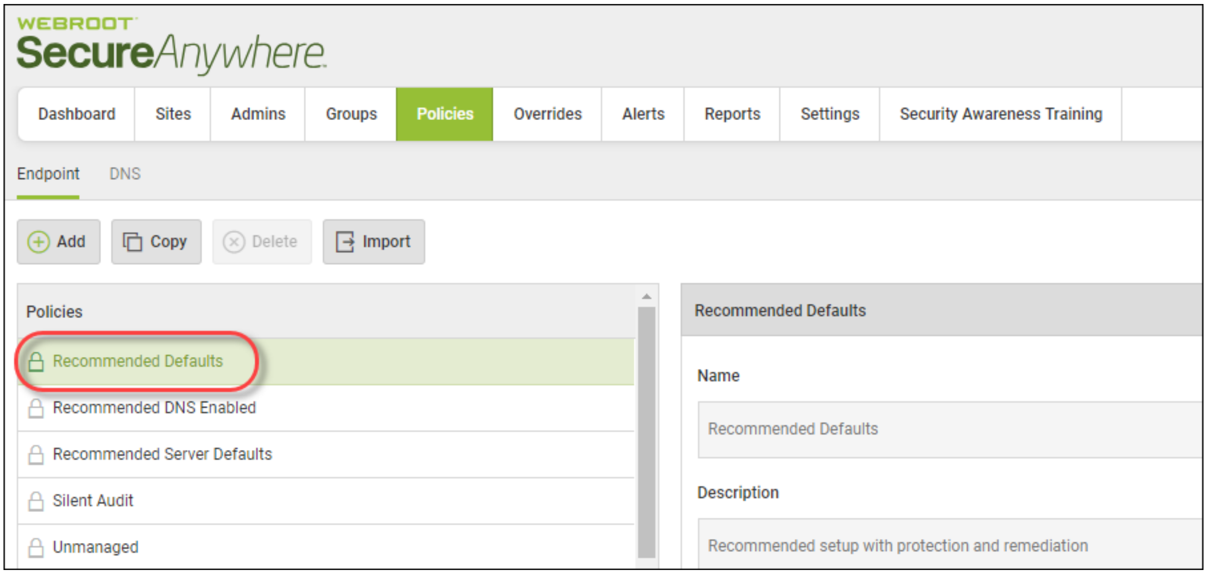
Name

Recommended Defaults

Description

Recommended setup with

3. In the Policies column, click a policy to display its settings.



Recommended Defaults

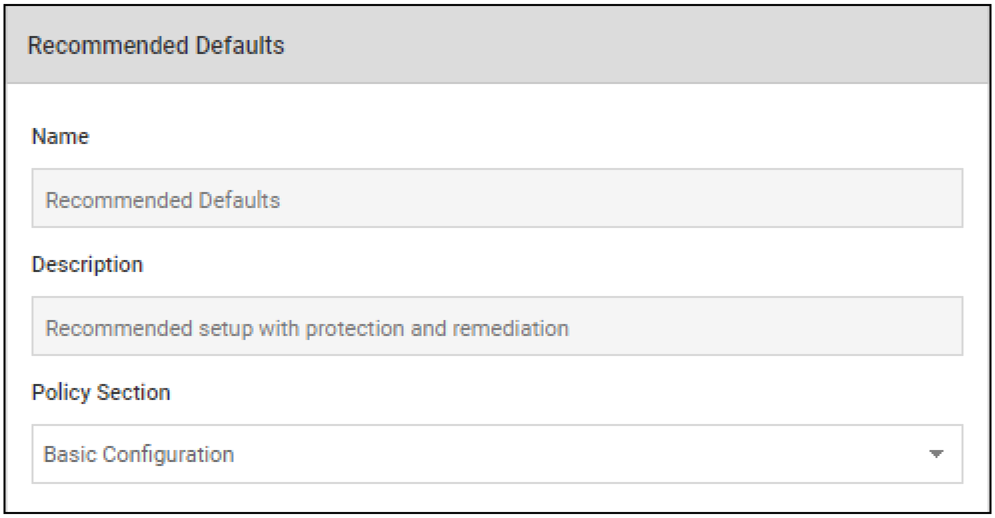
Name

Recommended Defaults

Description

Recommended setup with protection and remediation

The policy's settings window displays, with the Basic Configuration setting selected.



Recommended Defaults

Name

Recommended Defaults

Description

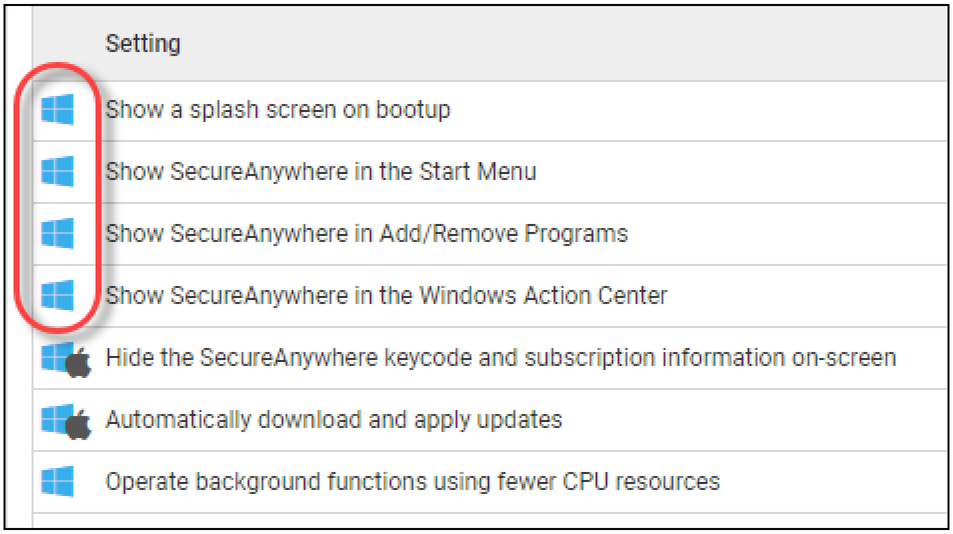
Recommended setup with protection and remediation

Policy Section

Basic Configuration

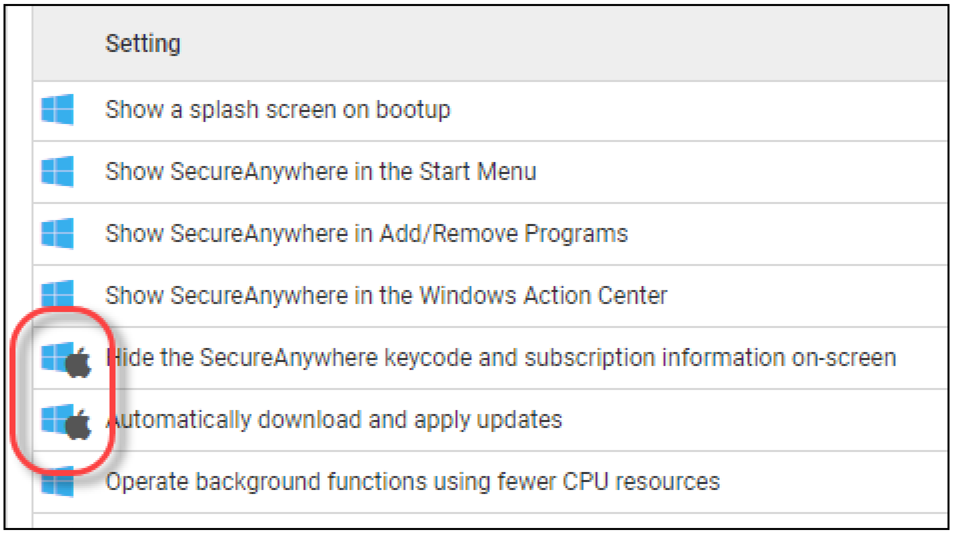
The Setting column displays the name of the policy, in addition to which:

- Settings that apply to PC only are indicated by the Windows icon.



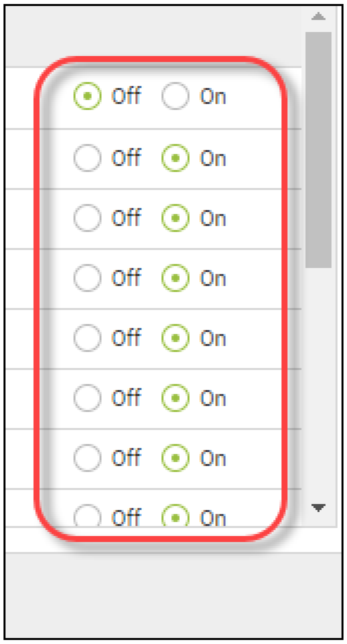
| | Setting |
|---|---|
| ⊞ | Show a splash screen on bootup |
| ⊞ | Show SecureAnywhere in the Start Menu |
| ⊞ | Show SecureAnywhere in Add/Remove Programs |
| ⊞ | Show SecureAnywhere in the Windows Action Center |
| ⊞  | Hide the SecureAnywhere keycode and subscription information on-screen |
| ⊞  | Automatically download and apply updates |
| ⊞ | Operate background functions using fewer CPU resources |

- Settings that apply to PC and Mac are indicated by both the Windows icon and the Mac icon.



| | Setting |
|---|---|
| ⊞ | Show a splash screen on bootup |
| ⊞ | Show SecureAnywhere in the Start Menu |
| ⊞ | Show SecureAnywhere in Add/Remove Programs |
| ⊞ | Show SecureAnywhere in the Windows Action Center |
| ⊞  | Hide the SecureAnywhere keycode and subscription information on-screen |
| ⊞  | Automatically download and apply updates |
| ⊞ | Operate background functions using fewer CPU resources |

The On/Off column displays how the setting is currently implemented on the endpoints.



● Off ○ On

○ Off ● On

○ Off ● On

○ Off ● On

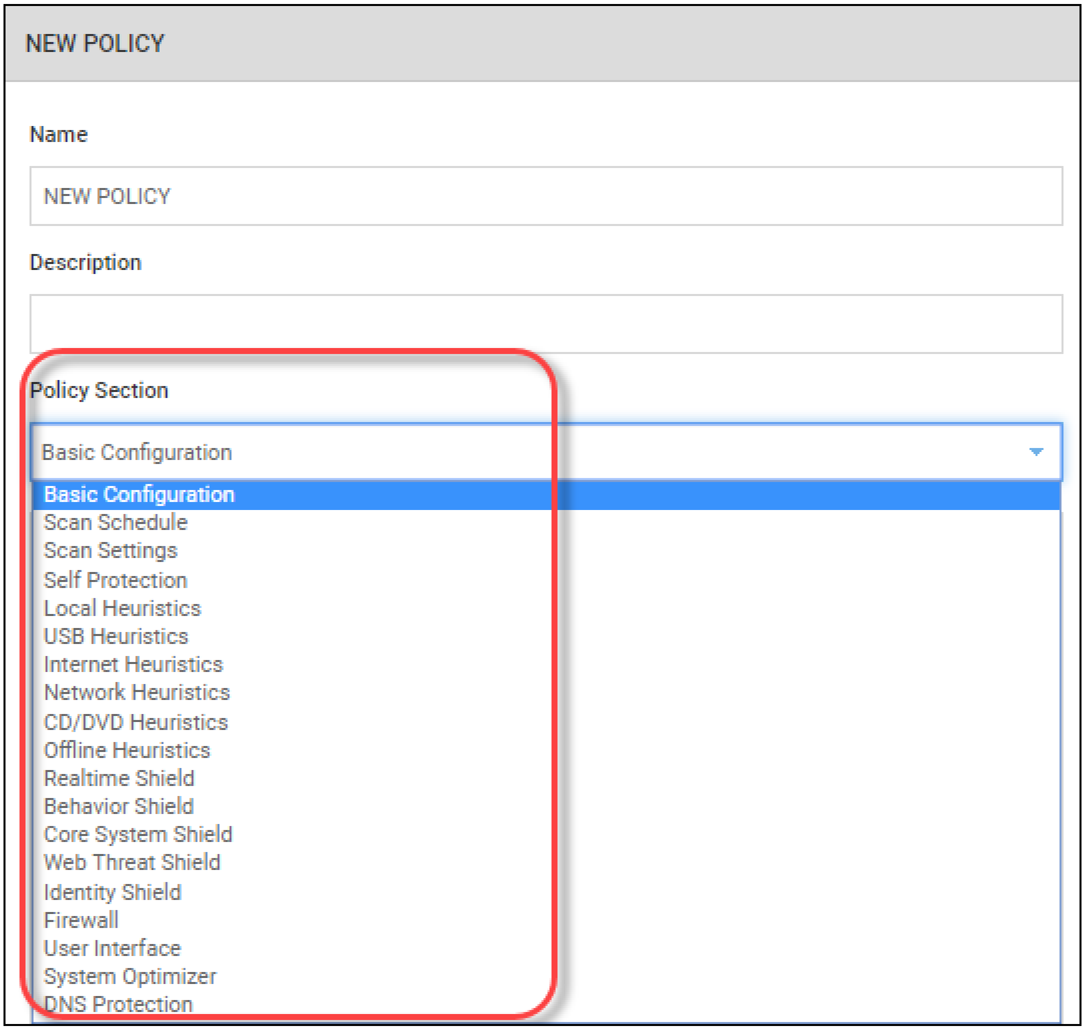
○ Off ● On

○ Off ● On

○ Off ● On

○ Off ● On

4. From the Policy Section drop-down menu, select the category you want to edit.



NEW POLICY

Name

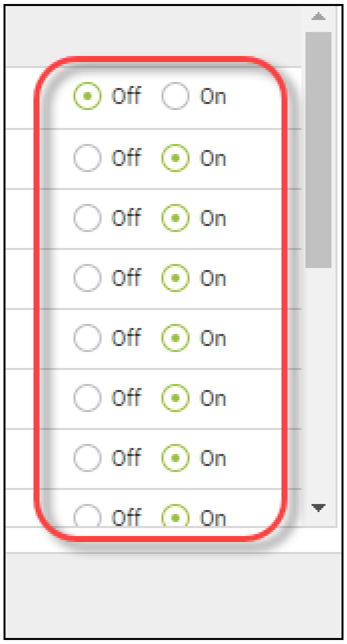
NEW POLICY

Description

Policy Section

Basic Configuration

5. Select either **On** or **Off** for that setting.



● Off ○ On

○ Off ● On

○ Off ● On

○ Off ● On

○ Off ● On

○ Off ● On

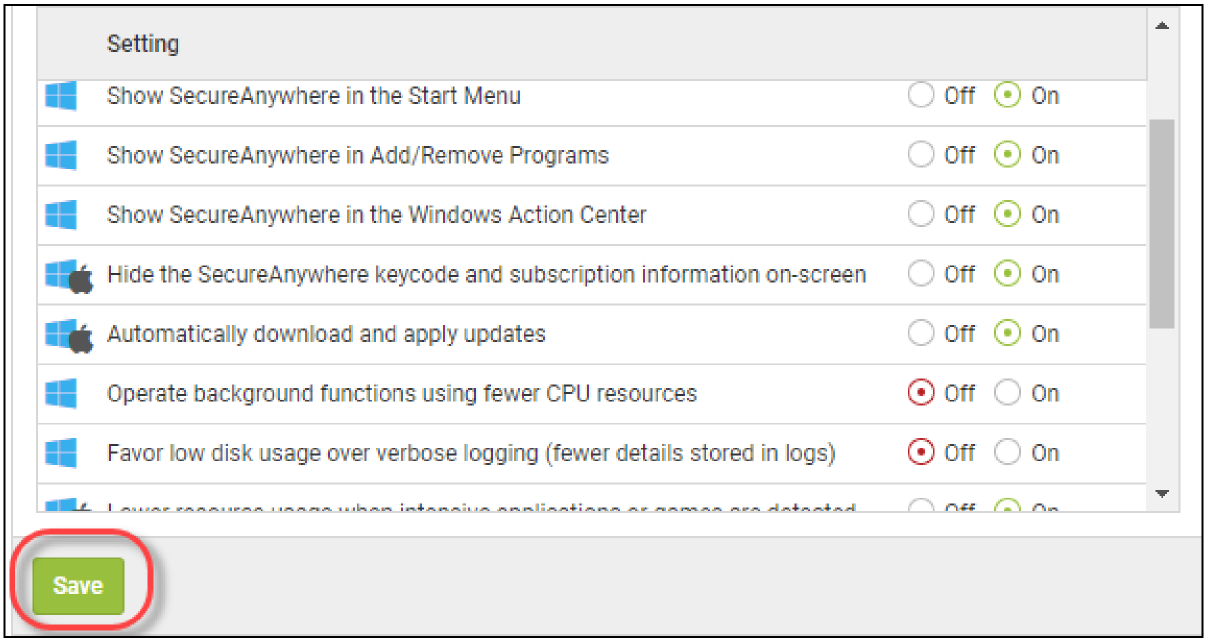
○ Off ● On

○ Off ● On

For a complete description of each setting, see the following tables in this procedure.

| | |
|---|---|
| • Basic Configuration | • Core System Shield |
| • Scan Schedule | • Web Threat Shield |
| • Scan Settings | • Identity Shield |
| • Self Protection | • Firewall |
| • Heuristics | • User Interface |
| • Realtime Shield | • System Optimizer |
| • Behavior Shield | • Evasion Shield |

6. When you're done making changes for a selection, click the **Save** button.



| Setting | | |
|---|---|---|
| Show SecureAnywhere in the Start Menu | ○ Off | ● On |
| Show SecureAnywhere in Add/Remove Programs | ○ Off | ● On |
| Show SecureAnywhere in the Windows Action Center | ○ Off | ● On |
| Hide the SecureAnywhere keycode and subscription information on-screen | ○ Off | ● On |
| Automatically download and apply updates | ○ Off | ● On |
| Operate background functions using fewer CPU resources | ● Off | ○ On |
| Favor low disk usage over verbose logging (fewer details stored in logs) | ● Off | ○ On |
| Lower resource usage when intensive applications or games are detected | ○ Off | ● On |

## Basic Configuration Settings

The Basic Configuration settings control the behavior of the SecureAnywhere software on sites.

| SETTING | DESCRIPTION |
|---|---|
| **Show a SecureAnywhere shortcut on the desktop** | Provides quick access to the main interface by placing the shortcut icon on the endpoint desktop.<br>This setting applies only to PC endpoints. |
| **Show a system tray icon** | Provides quick access to SecureAnywhere functions by placing the Webroot icon in the endpoint system tray.<br>This setting applies only to PC endpoints. |
| **Show a splash screen on bootup** | Opens the Webroot splash screen when the endpoint starts.<br>This setting applies only to PC endpoints. |
| **Show SecureAnywhere in the Start Menu** | Lists SecureAnywhere in the Windows Startup menu items.<br>This setting applies only to PC endpoints. |
| **Show SecureAnywhere in Add/Remove Programs** | Lists SecureAnywhere in the Windows Add/Remove Programs panel.<br>This setting applies only to PC endpoints. |
| **Show SecureAnywhere in Windows Action Center** | Lists SecureAnywhere in the Windows Action Center, under Virus Protection information.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Hide the SecureAnywhere keycode on-screen** | Hides the keycode on the endpoint's My Account panel. Asterisks replace the code, except for the first four digits.<br>This setting applies to both PC and Mac endpoints. |
| **Automatically download and apply updates** | Downloads product updates automatically without alerting the endpoint user.<br>This setting applies to both PC and Mac endpoints. |
| **Operate background functions using fewer CPU resources** | Saves CPU resources by running non-scan related functions in the background.<br>This setting applies to both PC and Mac endpoints. |
| **Favor low disk usage over verbose logging (fewer details stored in logs)** | Saves disk resources by saving only the last four log items.<br>This setting applies only to PC endpoints. |
| **Lower resource usage when intensive applications or games are detected** | Suppresses SecureAnywhere functions while the user is gaming, watching videos, or using other intensive applications.<br>This setting applies to both PC and Mac endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Allow SecureAnywhere to be shut down manually** | Displays a Shutdown command in the endpoint's system tray menu. Deselecting this option removes the Shutdown command from the menu.<br>This setting applies to both PC and Mac endpoints. |
| **Force non-critical notifications into the background** | Suppresses information-only messages from displaying in the system tray.<br>This setting applies only to PC endpoints. |
| **Fade out warning messages automatically** | Closes warning dialogs in the system tray after a few seconds. If you disable this option, the user must manually click on a message to close it.<br>This setting applies to both PC and Mac endpoints. |
| **Store Execution History details** | Stores data for the Execution History logs, available under Reports.<br>This setting applies only to PC endpoints. |
| **Poll interval** | Specifies how often the endpoint checks for updates. For example: 15 minutes, 30 minutes, 1 hour, or 2 hours.<br>This setting applies to both PC and Mac endpoints. |

## Scan Schedule

SecureAnywhere runs scans automatically every day, at about the same time you installed the software. You can use the Scan Schedule settings to change the schedules and run scans at different times.

| SETTING | DESCRIPTION |
|---|---|
| **Enable Scheduled Scans** | Allows scheduled scans to run on the endpoint.<br>This setting applies to both PC and Mac endpoints. |
| **Scan Frequency** | Determines how often to run the scan. You can set a day of the week or select on bootup.<br>This setting applies to both PC and Mac endpoints. |
| **Time** | Specifies the time to run the scan:<br>• Scan time options for when computer is idle are before 8:00 a.m., before noon, before 5:00 p.m., or before midnight.<br>• Scan time options for when resources are available are hourly, from 12:00 a.m. to 11:00 p.m.<br>This setting applies to both PC and Mac endpoints. |
| **Scan on bootup if the computer is off at the scheduled time** | Launches a scheduled scan within an hour after the user turns on the computer, if the scan did not run at the normally scheduled time. If this option is disabled, SecureAnywhere ignores missed scans.<br>This setting applies to both PC and Mac endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Hide the scan progress window during scheduled scans** | Runs scans silently in the background. If this option is disabled, a window opens and displays the scan progress.<br>This setting applies only to PC endpoints. |
| **Only notify me if an infection is found during a scheduled scan** | Opens an alert only if it finds a threat. If this option is disabled, a small status window opens when the scan completes, whether a threat was found or not.<br>This setting applies only to PC endpoints. |
| **Do not perform scheduled scans when on battery power** | Helps conserve battery power. If you want SecureAnywhere to launch scheduled scans when the endpoint is on battery power, deselect this option.<br>This setting applies to both PC and Mac endpoints. |
| **Do not perform scheduled scans when a full screen application or game is open** | Ignores scheduled scans when the user is viewing a full-screen application, such as a movie or a game. Deselect this option if you want scheduled scans to run anyway.<br>This setting applies to both PC and Mac endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Randomize the time of scheduled scans up to one hour for distributed scanning** | Determines the best time for scanning, based on available system resources, and runs the scan within an hour of the scheduled time. If you want to force the scan to run at the scheduled time, deselect this option.<br>This setting applies only to PC endpoints. |
| **Perform a scheduled Quick Scan instead of a Deep Scan** | Runs a quick scan of memory. We recommend that you keep this option deselected, so that deep scans run for all types of malware in all locations.<br>This setting applies only to PC endpoints. |

## Scan Settings

Scan settings give advanced control over scanning performance.

| SETTING | DESCRIPTION |
|---|---|
| **Enable Realtime Master Boot Record (MBR) Scanning** | Protects the endpoint against master boot record (MBR) infections. An MBR infection can modify core areas of the system so that they load before the operating system and can infect the computer. We recommend that you keep this option selected. It adds only a small amount of time to the scan.<br>This setting applies only to PC endpoints. |
| **Enable Enhanced Rootkit Detection** | Checks for rootkits and other malicious software hidden on disk or in protected areas. Spyware developers often use rootkits to avoid detection and removal. We recommend that you keep this option selected. It adds only a small amount of time to the scan.<br>This setting applies only to PC endpoints. |
| **Enable "right-click" scanning in Windows Explorer** | Enables an option for scanning the currently selected file or folder in the Windows Explorer right-click menu. This option is helpful if the user downloads a file and wants to scan it quickly.<br>This setting applies only to PC endpoints. |
| **Update the currently scanned folder immediately as scanned** | Displays a full list of files as SecureAnywhere scans each one. If you want to increase scan performance slightly, deselect this option so that file names only update once per second on the panel. SecureAnywhere will still scan all files, just not take the time to display each one on the screen.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Favor low memory usage over fast scanning** | Reduces RAM usage in the background by using less memory during scans, but scans will also run a bit slower. Deselect this option to run faster scans and use more memory.<br>This setting applies only to PC endpoints. |
| **Favor low CPU usage over fast scanning** | Reduces CPU usage during scans, but scans will also run a bit slower. Deselect this option to run faster scans.<br>This setting applies only to PC endpoints. |
| **Save non-executable file details to scan logs** | Saves all file data to the scan log, resulting in a much larger log file. Leave this option deselected to save only executable file details to the log.<br>This setting applies only to PC endpoints. |
| **Show the "Authenticating Files" popup when a new file is scanned on-execution** | Opens a small dialog whenever the user runs a program for the first time. Leave this option deselected if you do not want users to see this dialog.<br>This setting applies only to PC endpoints. |
| **Scan archived files** | Scans compressed files in zip, rar, cab, and 7-zip archives.<br>This setting applies to both PC and Mac endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Automatically reboot during cleanup without prompting** | Restarts the computer after running a clean-up, which is the process of removing all traces of a malware file.<br>This setting applies only to PC endpoints. |
| **Never reboot during malware cleanup** | Prevents the endpoint from restarting during cleanup, which is the process of removing all traces of a malware file.<br>This setting applies only to PC endpoints. |
| **Automatically remove threats found during background scans** | Removes threats during scans that run in the endpoint's background and sends them to quarantine.<br>This setting applies only to PC endpoints. |
| **Automatically remove threats found on the learning scan** | Removes threats during the first scan on the endpoint and sends them to quarantine.<br>This setting applies only to PC endpoints. |
| **Enable Enhanced Support** | Allows logs to be sent to Webroot customer support.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Show Infected Scan Results** | Displays scan results. If not enabled, the endpoint does not display scan results even if malware is detected.<br>This setting applies only to PC endpoints. |
| **Detect Possibly Unwanted Applications (PUAs) as malicious** | Detects PUAs and blocks them from installing.<br>Potentially unwanted applications (PUAs) are programs that aren't necessarily malicious but contain adware, toolbars, or other unwanted additions to your system. Generally, PUAs are not malicious but may be unsuitable for use in a business environment, and may create security concerns.<br>If a PUA is already on the system Webroot SecureAnywhere will detect the main program but may not be able to fully remove all aspects of it.<br>This setting applies only to PC endpoints. |
| **Allow Files to be Submitted for Threat Research** | Allows you to submit files for threat research.<br>This setting applies only to PC endpoints. |

## Self Protection Settings

Self Protection prevents malicious software from modifying the SecureAnywhere program settings and processes. If SecureAnywhere detects that another product is attempting to interfere with its functions, it launches a protective scan to look for threats. It will also update the internal self protection status to prevent incompatibilities with other software.

**Note:** We recommend that you leave Self Protection at the Maximum settings, unless you use other security software in addition to SecureAnywhere. If you use additional security software, adjust Self Protection to Medium or Minimum. The Maximum setting might interfere with other security software.

| SETTING | DESCRIPTION |
|---|---|
| **Enable self-protection response cloaking** | Turns self-protection on and off.<br>This setting applies only to PC endpoints. |
| **Self-protection level** | Sets the detection level to:<br>• **Minimum** — Protects the integrity of the SecureAnywhere settings and databases. Recommended if the endpoint has several other security products installed.<br>• **Medium** — Prevents other programs from disabling protection. Provides maximum possible compatibility with other security software.<br>• **Maximum** — Provides the highest protection of the SecureAnywhere processes. We recommend that you use this setting.<br>This setting applies only to PC endpoints. |

## Heuristics

With heuristics, you can set the level of threat analysis that SecureAnywhere performs when scanning managed endpoints. SecureAnywhere includes three types of heuristics: advanced, age, and popularity.

You can adjust these types of heuristics for several areas:

- **Local Heuristics** — Local drive
- **USB Heuristics** — USB drives
- **Internet Heuristics** — Internet

- **Network Heuristics** — Network
- **CD/DVD Heuristics** — CD/DVD
- **Offline Heuristics** — When your computer is offline

For each of these areas, you can set the following options:

- **Disable Heuristics** — Turns off heuristic analysis for the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline. Not recommended.
- **Apply advanced heuristics before Age/Popularity heuristics** — Warns against new programs as well as old programs that exhibit suspicious behavior on the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline.
- **Apply advanced heuristics after Age/Popularity heuristics** — Warns against suspicious programs detected with Advanced Heuristics, based on Age/Popularity settings on the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline.
- **Warn when new programs execute that are not known good** — Warns when malicious, suspicious, or unknown programs try to execute on the local drive, USB drives, the Internet, the network, CD/DVDs, or when your computer is offline. Keep in mind that this setting may result in false detections.

| SETTING | DESCRIPTION |
|---|---|
| **Advanced Heuristics** | Analyzes new programs for suspicious actions that are typical of malware.<br>• **Disabled** — Turns off Advanced Heuristics, leaving it vulnerable to new threats; however, it will still be protected against known threats.<br>• **Low** — Detects programs with a high level of malicious activity. This setting ignores some suspicious behavior and allows most programs to run.<br>• **Medium** — Balances detection versus false alarms by using our tuned heuristics in the centralized community database.<br>• **High** — Protects against a wide range of new threats. Use this setting if you think your system is infected or at very high risk. This setting may result in false detections.<br>• **Maximum** — Provides the highest level of protection against new threats. Use this setting if you think that your system is infected or at very high risk. This setting may result in false detections.\<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Age Heuristics** | Analyzes new programs based on the amount of time the program has been in the community. Legitimate programs are generally used in a community for a long time, but malware often has a short life span.<br>• **Disabled** — Turns off Age Heuristics, leaving it vulnerable to new threats; however, it will still be protected against known threats.<br>• **Low** — Detects programs that have been created or modified very recently.<br>• **Medium** — Detects programs that are fairly new and not trusted, preventing zero-day or zero-hour attacks. We recommend using this setting if you do not allow unpopular programs to be installed on your managed endpoints and you want extra security to prevent mutating threats.<br>• **High** — Detects programs that have been created or modified in a relatively short time and are not trusted. This setting is recommended only if new programs are rarely installed on your managed endpoints, and if you feel that your systems are relatively constant. This setting might generate a higher level of false detections on more obscure or unpopular programs.<br>• **Maximum** — Detects all untrusted programs that have been created or modified fairly recently. Use this setting only if your managed endpoints are in a high-risk situation, or if you think that they are currently infected.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Popularity Heuristics** | Analyzes new programs based on statistics for how often the program is used in the community and how often it changes. Legitimate programs do not change quickly, but malware often mutates at a rapid pace. Malware may install as a unique copy on every computer, making it statistically unpopular.<br>• **Low** — Detects programs that are seen for the first time. This setting is recommended if new or beta programs are frequently installed on your managed endpoints, or if endpoint users are software developers who frequently create new programs.<br>• **Medium** — Detects unpopular and mutating programs, preventing zero-day and zero-hour attacks. We recommend using this setting if you do not allow new programs to be installed frequently on your managed endpoints and you want extra security over standard settings.<br>• **High** — Detects programs that a significant percentage of the community has seen. This setting is recommended if you do not allow new programs on your managed endpoints and you suspect that they are currently infected.<br>• **Maximum** —Detects programs that a large percentage of the community has seen. We recommend this setting if you think your managed endpoints are at very high risk, and you accept that you might receive false detections because of the strict heuristic rules.<br>This setting applies only to PC endpoints. |

## Realtime Shield Settings

The Realtime shield blocks known threats that are listed in Webroot's threat definitions and community database. If the shield detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to the endpoint or steals its information.

| SETTING | DESCRIPTION |
|---|---|
| **Realtime Shield Enabled** | Turns the Realtime shield on and off.<br>This setting applies to both PC and Mac endpoints. |
| **Enable Predictive Offline Protection from the central SecureAnywhere database** | Downloads a small threat definition file to your managed endpoints, protecting them even when they are offline. We recommend that you leave this setting on.<br>This setting applies only to PC endpoints. |
| **Remember actions on blocked files** | Remembers how the user responded to an alert, whether they allowed a file or blocked it, and will not prompt again when it encounters the same file. If this setting is deselected, SecureAnywhere opens an alert every time it encounters the file in the future.<br>This setting applies only to PC endpoints. |
| **Automatically quarantine previously blocked files** | Opens an alert when it encounters a threat and allows the user to block it and send it to quarantine. If this setting is off, the user must run a scan manually to remove a threat.<br>This setting applies to both PC and Mac endpoints. |
| **Automatically block files when detected on execution** | Blocks threats and sends them to quarantine. If this setting is off, the user must respond to lerts about detected threats.<br>This setting applies to both PC and Mac endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Scan files when written or modified** | Scans any new or modified files that are saved to disk. If this setting is off, it ignores new file installations; however, it still alerts the user if a threat tries to launch.<br>This setting applies to both PC and Mac endpoints. |
| **Block threats automatically if no user is logged in** | Stops threats from executing even when managed endpoints are logged off. Threats are sent to quarantine without notification.<br>This setting applies to both PC and Mac endpoints. |
| **Show realtime event warnings** | Opens an alert when suspicious activity occurs.<br>This setting applies only to PC endpoints. |
| **Show realtime block modal alerts** | Displays alerts when Heuristics detects malware, and prompts the user to allow or block the action.<br>If Heuristics is set to Warn when new programs execute that are not known good, then this setting must be set to On. Otherwise, users will not see the alert.<br>This setting applies only to PC endpoints. |
| **Show realtime block notifications** | Displays a tray notification if the Realtime shield detects malware. If this setting is off, there is no tray notification, but malware is blocked and the home page displays that threats were detected.<br>This setting applies only to PC endpoints. |

## Behavior Shield Settings

The Behavior shield analyzes the applications and processes running on your managed endpoints. If it detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to managed endpoints or steals information.

| SETTING | DESCRIPTION |
|---|---|
| **Behavior Shield Enabled** | Turns the Behavior shield on and off.<br>This setting applies only to PC endpoints. |
| **Assess the intent of new programs before allowing them to execute** | Watches the program's activity before allowing it to run. If it seems okay, SecureAnywhere allows it to launch and continues to monitor its activity.<br>This setting applies only to PC endpoints. |
| **Enable advanced behavior interpretation to identify complex threats** | Analyzes a program to examine its intent. For example, a malware program might perform suspicious activities like modifying a registry entry, then sending an email.<br>This setting applies only to PC endpoints. |
| **Track the behavior of untrusted programs for advanced threat removal** | Watches programs that have not yet been classified as legitimate or as malware.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Automatically perform the recommended action instead of showing warning messages** | Does not prompt the user to allow or block a potential threat. SecureAnywhere determines how to manage the item.<br>This setting applies only to PC endpoints. |
| **Warn if untrusted programs attempt low-level system modifications when offline** | Opens an alert if an unclassified program tries to make changes to your managed endpoints when they are offline. SecureAnywhere cannot check its online threat database if endpoints are disconnected from the Internet.<br>This setting applies only to PC endpoints. |

## Core System Shield

The Core System shield monitors system structures of your managed endpoints and makes sure malware has not tampered with them. If the shield detects a suspicious file trying to make changes, it opens an alert and prompts the user to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage or steals information.

| SETTING | DESCRIPTION |
|---|---|
| **Core System Shield Enabled** | Turns the Core System shield on and off.<br>This setting applies only to PC endpoints. |
| **Assess system modifications before they are allowed to take place** | Intercepts any activity that attempts to make system changes on your managed endpoints, such as a new service installation.<br>This setting applies only to PC endpoints. |
| **Detect and repair broken system components** | Locates corrupted components, such as a broken Layered Service Provider (LSP) chain or a virus-infected file, then restores the component or file to its original state.<br>This setting applies only to PC endpoints. |
| **Prevent untrusted programs from modifying kernel memory** | Stops unclassified programs from changing the kernel memory.<br>This setting applies only to PC endpoints. |
| **Prevent untrusted programs from modifying system processes** | Stops unclassified programs from changing system processes.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Verify the integrity of the LSP chain and other system structures** | Monitors the Layered Service Provider (LSP) chain and other system structures to make sure malware does not corrupt them.<br>This setting applies only to PC endpoints. |
| **Prevent any program from modifying the HOSTS file** | Stops spyware from attempting to add or change the IP address for a website in the Hosts file, and opens an alert for the user to block or allow the changes.<br>This setting applies to both PC and Mac endpoints. |

## Web Threat Shield

The Web Threat shield protects your endpoints as users surf the Internet. If it detects a website that might be a threat, it opens an alert for users to block the site or continue despite the warning. When they use a search engine, this shield analyzes all the links on the search results page, then displays an image next to each link that signifies whether it's a trusted site, displaying a green checkmark, or a potential risk, indicated by a red X.

| SETTING | DESCRIPTION |
|---|---|
| **Enable Web Threat Shield** | Turns the Web Threat shield on and off.<br>This setting is turned On by default, which is the setting we recommend.<br>This setting applies to both PC and Mac endpoints. |
| **Activate browser extension** | Browser extensions provide blocking protection against malicious websites, realtime anti-phishing protection, and safety ratings when using search engines. Each function can be enabled or disabled separately using the individual controls for each function described in this table.<br>To completely disable and remove extensions from each supported browser, change the setting to Off.<br>This setting is turned On by default, which is the setting we recommend.<br>This setting applies only to PC endpoints. |
| **Block malicious websites** | Any URLs and IPs you enter in a browser are checked and a block page displays for known malicious sites.<br>This setting is turned On by default, which is the setting we recommend.<br>This setting applies to both PC and Mac endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Enable real-time anti-phising** | Protects against zero-day phishing sites. Zero-day phishing sites are sites that have never been seen before, and their related viruses do not yet have a definition.<br>This setting is turned On by default, which is the setting we recommend.<br>This setting applies to both PC and Mac endpoints. |
| **Show safety ratings when using search engines** | Search result are annotated with an icon and tooltip, indicating the likelihood that a site is malicious.<br>This setting is turned On by default, which is the setting we recommend.<br>This setting applies to both PC and Mac endpoints. |
| **Enable web filtering driver** | Provides additional protection against malicious connections, and in cases where the browser extensions are disabled.<br>This setting is turned On by default, which is the setting we recommend. |

| SETTING | DESCRIPTION |
|---|---|
| **Suppress the user's ability to bypass blocked websites** | Prevents users from bypassing the block page presented when a malicious website is detected.<br>This setting is turned On by default, which is the setting we recommend.<br>This setting applies to both PC and Mac endpoints. |
| **Suppress the user's ability to request website review** | Prevents users from submitting website reviews from the block page when a malicious website is detected.<br>This setting is turned On by default, which is the setting we recommend.<br>This setting applies to both PC and Mac endpoints. |

## Identity Shield

The Identity shield protects sensitive data that might be exposed during online transactions. You can change the behavior of the Identity shield and control what it blocks.

| SETTING | DESCRIPTION |
|---|---|
| **Identity Shield Enabled** | Turns the Identity shield on and off.<br>This setting applies to both PC and Mac endpoints.<br>**Note:** On Mac, this controls the Secure Keyboard Entry Mode setting. |
| **Look for identity threats online** | Analyzes websites as users browse the Internet or open links. If the shield detects malicious content, it blocks the site and opens an alert.<br>This setting applies only to PC endpoints. |
| **Verify websites for phishing threats** | Analyzes websites for phishing threats as users browse the Internet or open links. If the shield detects a phishing threat, it blocks the site and opens an alert.<br>This setting applies only to PC endpoints. |
| **Verify websites when visited to determine legitimacy** | Analyzes the IP address of each website to determine if it has been redirected or is on our blacklist. If the shield detects an illegitimate website, it blocks the site and opens an alert.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks** | Looks for servers that could be redirecting users to a malicious website, such as a man-in-the-middle attack. If the shield detects a man-in-the-middle attack, it blocks the threat and opens an alert.<br>This setting applies only to PC endpoints. |
| **Block websites from creating high risk tracking information** | Blocks third-party cookies from installing on your managed endpoints if the cookies originate from malicious tracking websites.<br>This setting applies only to PC endpoints. |
| **Prevent programs from accessing protected credentials** | Blocks programs from accessing login credentials, for example, when you type your name and password or when you request a website to remember them.<br>This setting applies only to PC endpoints. |
| **Warn before blocking untrusted programs from accessing protected data** | Opens an alert any time malware attempts to access data, instead of blocking known malware automatically.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Allow trusted screen capture programs access to protected screen contents** | Allows screen capture programs, no matter what content is displayed on the screen.<br>This setting applies only to PC endpoints. |
| **Enable Identity Shield compatibility mode** | Allows certain applications to run that the Identity shield might block during normal operations. You can enable this option if you notice problems with an application's functions after SecureAnywhere was installed on the endpoint. With this compatibility mode enabled, the endpoint is still protected by the Identity shield's core functionality.<br>This setting applies only to PC endpoints. |
| **Enable keylogging protection in non-Latin systems** | Allows endpoints with non-Latin systems, such as Japanese and Chinese, to be protected from keyloggers.<br>This setting applies only to PC endpoints. |

## Firewall

The Webroot firewall monitors data traffic traveling out of endpoint ports. It looks for untrusted processes that try to connect to the Internet and steal personal information. It works with the Windows firewall, which monitors data traffic coming into your managed endpoints. With both the Webroot and Windows firewall turned on, network data has complete inbound and outbound protection.

The Webroot firewall is preconfigured to filter traffic on your managed endpoints. It works in the background without disrupting normal activities. If the firewall detects unrecognized traffic, it opens an alert. You can either block the traffic or allow it to proceed.

| SETTING | DESCRIPTION |
|---|---|
| **Enabled** | Turns the Firewall on and off.<br>This setting applies only to PC endpoints. |
| **Firewall level** | • **Default Allow** — Allows all processes to connect to the Internet, unless explicitly blocked.<br>• **Warn unknown and infected** — Warns if any new, untrusted processes connect to the Internet, if the endpoint is infected.<br>• **Warn unknown** — Warns if a new, untrusted process connects to the Internet.<br>• **Default Block** — Warns if any process connects to the Internet, unless explicitly blocked.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Show firewall management warnings** | Controls the alert displayed by SecureAnywhere when the Windows firewall is off:<br>• **On** — The user sees an alert when SecureAnywhere detects that the Windows firewall is off.<br>• **Off** — No alert displays when the Windows firewall is off.<br>This setting applies only to PC endpoints. |
| **Show firewall process warnings** | Controls the firewall alerts. If this is setting is Off, no firewall alerts display . This option works in conjunction with the Firewall Level settings.<br>For example:<br>• If Show firewall process warnings and Default Block options are both set to On, the endpoint user sees an alert if a new process tries to connect.<br>• If Show Firewall process warnings is set to Off, no alert displays to the endpoint user and the process is allowed.<br>This setting applies only to PC endpoints. |

## User Interface

Gives administrative control over the SecureAnywhere interface on the endpoints using this policy.

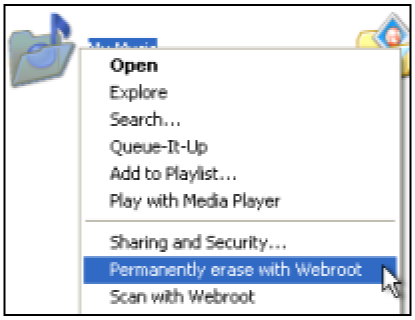
| SETTING | DESCRIPTION |
|---|---|
| **GUI** | Blocks or allows endpoint user access to the main SecureAnywhere interface. If users try to open SecureAnywhere when this option is set to Hide, a message tells them to contact the administrator to access the interface.<br>This setting applies to both PC and Mac endpoints.<br>**Note:** This option does not also hide the Webroot system tray icon on a PC. However, on a Mac, this option does hide the Webroot system tray icon. |

## System Optimizer

System Optimizer removes traces of the end user's web browsing history, files that display computer use, and unnecessary files that consume valuable disk space, such as files in the Recycle Bin or Windows temporary files. System Optimizer does not run automatically; you need to schedule cleanups and select the items you want removed.

**Note:** Optimization removes unnecessary files and traces, not malware threats. Malware are removed during scans. You can think of System Optimizer as the housekeeper for a computer, while the Scanner serves as the security guard.

| SETTING | DESCRIPTION |
|---|---|
| **Manage System Optimizer centrally** | Enables the administrator to change System Optimizer settings, as follows:<br>• **On** — System Optimizer settings display in the panel and are available to change.<br>• **Off** — No settings display in this panel.<br>This setting applies only to PC endpoints. |
| **Schedule** | |
| **Monday through Sunday** | Sets the days of the week, anything from one to seven, to automatically run System Optimizer.<br>This setting applies only to PC endpoints. |
| **Run at specific time of day - hour** | Sets the hour of the day System Optimizer runs on the endpoints.<br>This setting applies only to PC endpoints. |
| **Run at specific time of day - minute** | Sets the time in 15-minute increments that System Optimizer runs on the endpoints.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Run on bootup if the system was off at the scheduled time** | Launches a missed scheduled cleanup when the endpoint powers on. This is applicable only if the endpoint was off during a scheduled cleanup. Otherwise, skips the missed cleanup.<br>This setting applies only to PC endpoints. |
| **Enable Windows Explorer right click secure file erasing** | Includes an option for permanently erasing a file or folder in Windows Explorer on the endpoint. A menu item displays when the user right-clicks on a file or folder:<br><br> Open<br>Explore<br>Search...<br>Queue-It-Up<br>Add to Playlist...<br>Play with Media Player<br>Sharing and Security...<br>Permanently erase with Webroot<br>Scan with Webroot<br>This setting applies only to PC endpoints. |
| **Windows Desktop** | |
| **Recycle Bin** | Removes all files from the Recycle Bin in Windows Explorer.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Recent document history** | Clears the history of recently opened files, which is accessible from the Windows Start menu. The cleanup does not delete the actual files.<br>This setting applies only to PC endpoints. |
| **Start Menu click history** | Clears the history of shortcuts to programs that end users recently opened using the Start menu.<br>This setting applies only to PC endpoints. |
| **Run history** | Clears the history of commands recently entered into the Run dialog, which is accessible from the Start menu.<br>After the cleanup, the end user may need to restart the computer to completely remove items from the Run dialog.<br>This setting applies only to PC endpoints. |
| **Search history** | Clears the history of files or other information that the end user searched for on the computer. This history displays when the end user starts entering a new search that starts with the same characters. The cleanup does not delete the actual files.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Start Menu order history** | Reverts the list of programs and documents in the Start menu back to alphabetical order, which is the default setting. After the cleanup runs, the list reverts back to alphabetical order after a system re-boot.<br>This setting applies only to PC endpoints. |
| **Windows System** | |
| **Clipboard contents** | Clears the contents from the Clipboard, where Windows stores data used in either the Copy or Cut function from any Windows program.<br>This setting applies only to PC endpoints. |
| **Windows Temporary folder** | Deletes all files and folders in the Windows temporary folder, but not files that are in use by an open program. This folder is typically: C:\Windows\Temp.<br>This setting applies only to PC endpoints. |
| **System Temporary folder** | Deletes all files and folders in the system temporary folder, but not files that are in use by an open program. This folder is typically in: C:\Documents and Settings\[username]\Local Settings\Temp.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Windows Update Temporary folder** | Deletes all files and subfolders in this folder, but not files that are in use by an open program. Windows uses these files when a Windows Update runs. These files are typically in C:\Windows\Software\Distribution\Download.<br>This setting applies only to PC endpoints. |
| **Windows Registry Streams** | Clears the history of recent changes made to the Windows registry. This option does not delete the registry changes themselves.<br>This setting applies only to PC endpoints. |
| **Default logon user history** | Deletes the Windows registry entry that stores the last name used to log on to your computer. When the registry entry is deleted, end users must enter their user names each time they turn on or restart the computer. This cleanup option does not affect computers that use the default Welcome screen.<br>This setting applies only to PC endpoints. |
| **Memory dump files** | Deletes the memory dump file (memory.dmp) that Windows creates with certain Windows errors. The file contains information about what happened when the error occurred.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **CD burning storage folder** | Deletes the Windows project files, created when the Windows built-in function is used to copy files to a CD. These project files are typically stored in one of the following directories:<br>C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\CDBurning<br>or<br>C:\Users\[username]\AppData\Local\Microsoft\Windows\Burn\Burn<br>This setting applies only to PC endpoints. |
| **Flash cookies** | Deletes bits of data created by Adobe Flash, which can be a privacy concern because they track user preferences. Flash cookies are not actually cookies, and are not controlled through the cookie privacy controls in a browser.<br>This setting applies only to PC endpoints. |
| **Internet Explorer** | |
| **Address bar history** | Removes the list of recently visited websites, which is stored as part of Internet Explorer's AutoComplete feature. You see this list when you click the arrow on the right side of the Address drop-down list at the top of the Internet Explorer browser.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Cookies** | Deletes all cookies from the endpoint. Be aware that if you remove all cookie files, the end user must re-enter passwords, shopping cart items, and other entries that these cookies stored.<br>This setting applies only to PC endpoints. |
| **Temporary Internet Files** | Deletes copies of stored web pages that the end user visited recently. This cache improves performance by helping web pages open faster, but can consume a lot of space on the hard drive.<br>This setting applies only to PC endpoints. |
| **URL history** | Deletes the History list of recently visited websites of the Internet Explorer toolbar.<br>This setting applies only to PC endpoints. |
| **Setup Log** | Deletes log files created during Internet Explorer updates.<br>This setting applies only to PC endpoints. |
| **Microsoft Download Folder** | Deletes the contents in the folder that stores files last downloaded using Internet Explorer.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **MediaPlayer Bar History** | Removes the list of audio and video files recently opened with the media player in Internet Explorer. The cleanup does not delete the files themselves.<br>This setting applies only to PC endpoints. |
| **Autocomplete form information** | Deletes data that Internet Explorer stores when the end user entered information into fields on websites. This is part of Internet Explorer's AutoComplete feature.<br>This setting applies only to PC endpoints. |
| **Clean index.dat (cleaned on reboot)** | Marks files in the index.dat file for deletion, then clears those files after the system reboots. The index.dat file is a growing Windows repository of web addresses, search queries, and recently opened files. This option works when you also select one or more of the following options: Cookies, Temporary Internet Files, or URL History. Index.dat functions like an active database. It is only cleaned after you reboot Windows.<br>This setting applies only to PC endpoints. |

| SETTING | DESCRIPTION |
|---|---|
| **Secure File Removal** | |
| **Control the level of security to apply when removing files** | Removes files permanently in a shredding process, which overwrites them with random characters. This shredding feature is a convenient way to make sure no one can ever access the endpoint's files with a recovery tool.<br>By default, file removal is set to Normal, which means items are deleted permanently, bypassing the Recycle Bin. However, with the Normal setting, data recovery utilities could restore the files. If you want to make sure files can never be recovered, select Maximum. Medium overwrites files with three passes, whereas Maximum overwrites files with seven passes and cleans the space around the files. Also be aware that cleanup operations take longer when you select Medium or Maximum.<br>This setting applies only to PC endpoints. |

## Evasion Shield Settings

Evasion shield will detect and block malicious script files including JS, VBS, powershell, wscript, cscript, macros, and more. This shield includes file-based scripts as well as file-less scripts which often evade other malware detection software. On Windows 10, there is enhanced protection for file-less scripts, obfuscated scripts, and other sophisticated script attacks.

**Note:** You will also need to ensure that each device has upgraded to the latest Webroot Business Endpoint Protection agent version 9.0.28.00 or higher. Earlier agent versions will not fully support Evasion Shield protection.

| SETTING | DESCRIPTION |
|---|---|
| **Script Protection** | Sets the protection level to:<br>- **Off**<br>- **Detect and Report** — Threats will be detected, reported to the console and **not** quarantined.<br>- **Detect and Remediate** — Threats will be detected, reported to the console and quarantined.<br>This setting applies only to PC endpoints. |

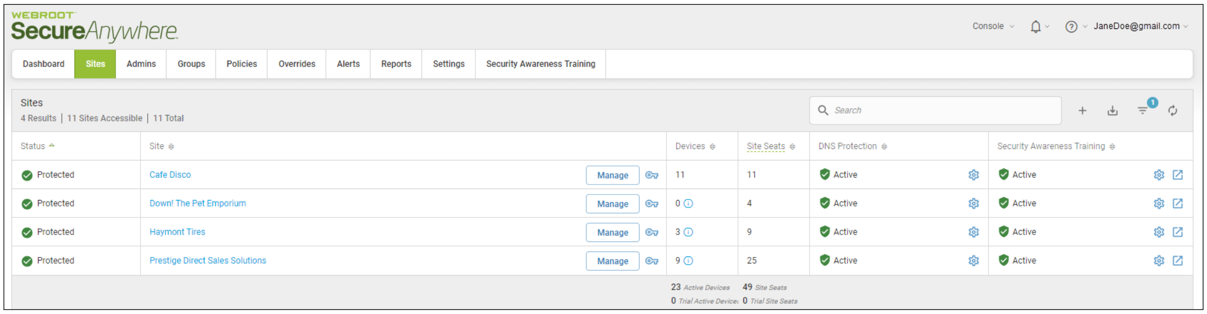
# Renaming Policies

Follow this procedure to rename a policy without having to edit any other section of your policy.

**To rename a policy:**

1. Log in to the management console.

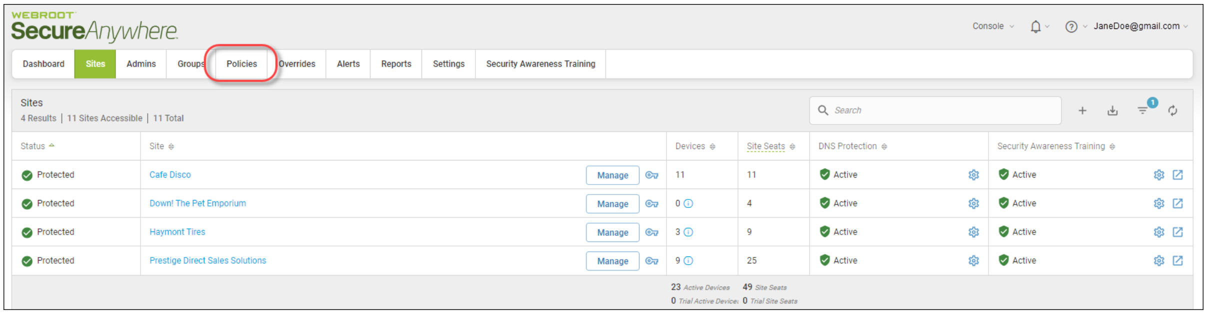
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

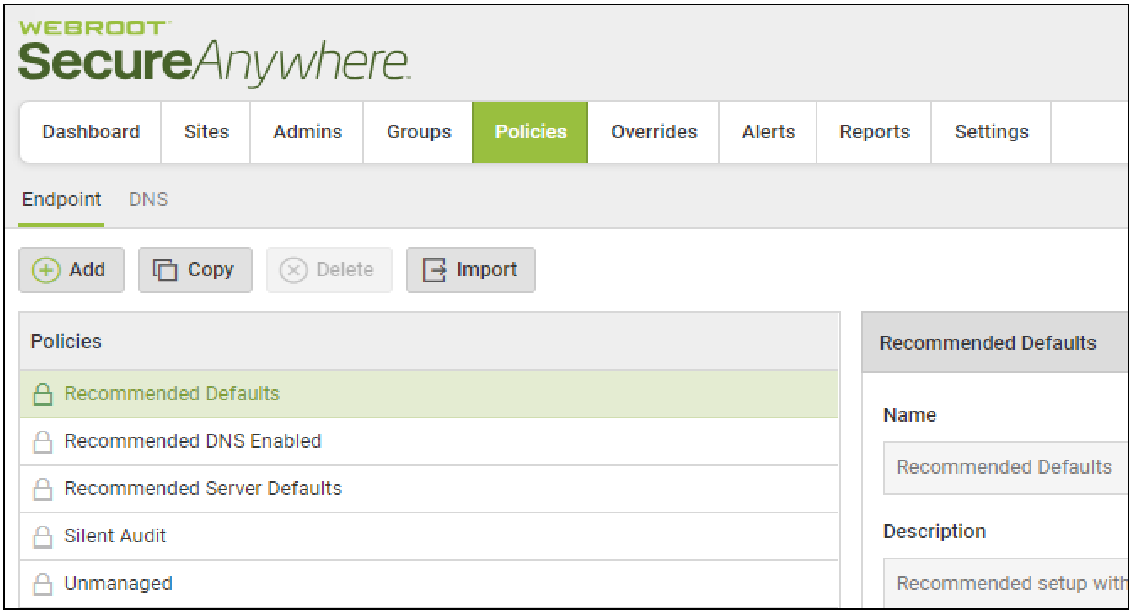
2. Click the **Policies** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

The Policies tab displays.



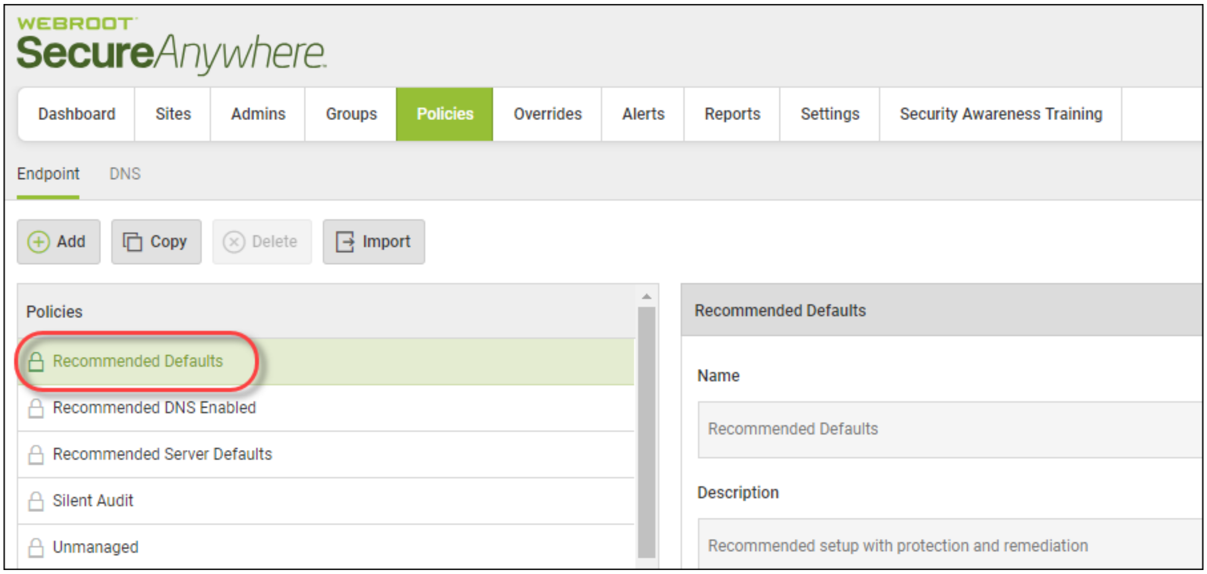
Name

Recommended Defaults

Description

Recommended setup with

3. In the Policies column, select a policy that you want to rename.



Name

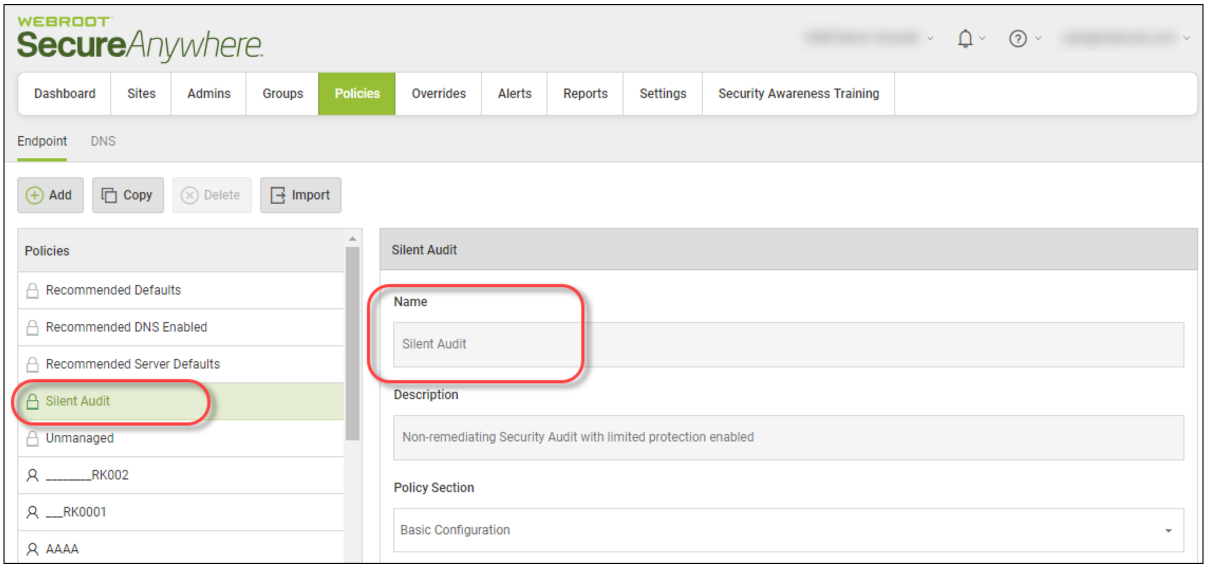
Recommended Defaults

Description

Recommended setup with protection and remediation

**Note:** For default Webroot Policies, you cannot edit the information in the Name or Description fields.

4. In the Name field, enter the new name.



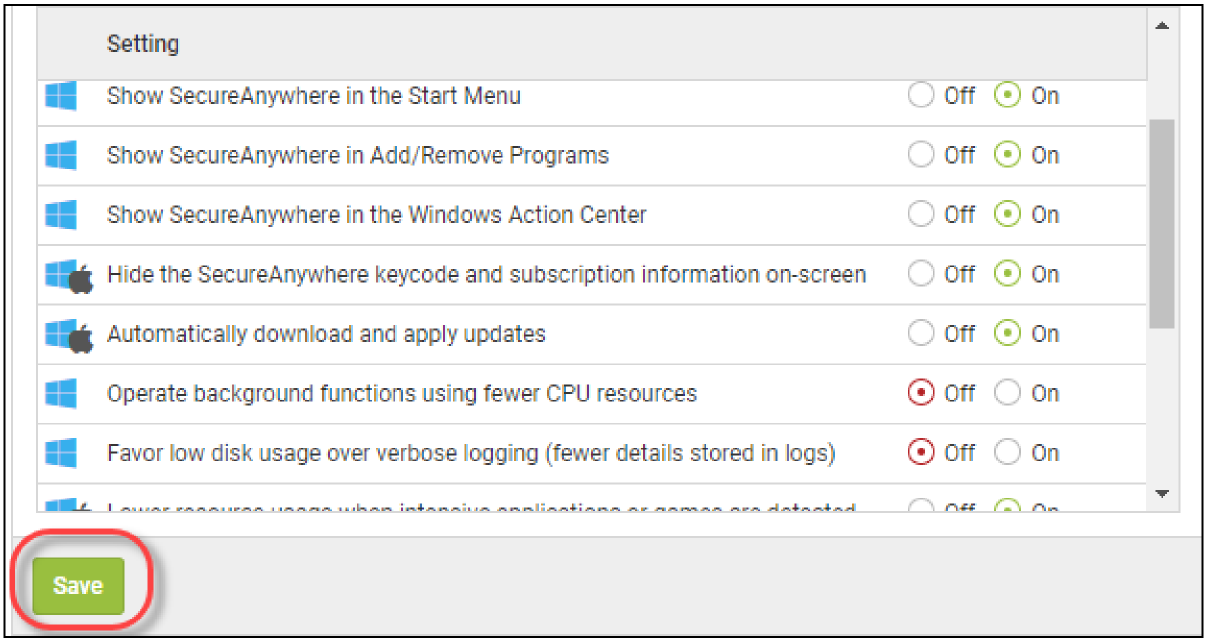
Silent Audit

Name: Silent Audit

Description: Non-remediating Security Audit with limited protection enabled

Policy Section: Basic Configuration

5. When you're done, click the **Save** button.



| Setting | | |
|---|---|---|
| Show SecureAnywhere in the Start Menu | ○ Off | ● On |
| Show SecureAnywhere in Add/Remove Programs | ○ Off | ● On |
| Show SecureAnywhere in the Windows Action Center | ○ Off | ● On |
| Hide the SecureAnywhere keycode and subscription information on-screen | ○ Off | ● On |
| Automatically download and apply updates | ○ Off | ● On |
| Operate background functions using fewer CPU resources | ● Off | ○ On |
| Favor low disk usage over verbose logging (fewer details stored in logs) | ● Off | ○ On |
| Lower resource usage when intensive applications or games are detected | ○ Off | ● On |

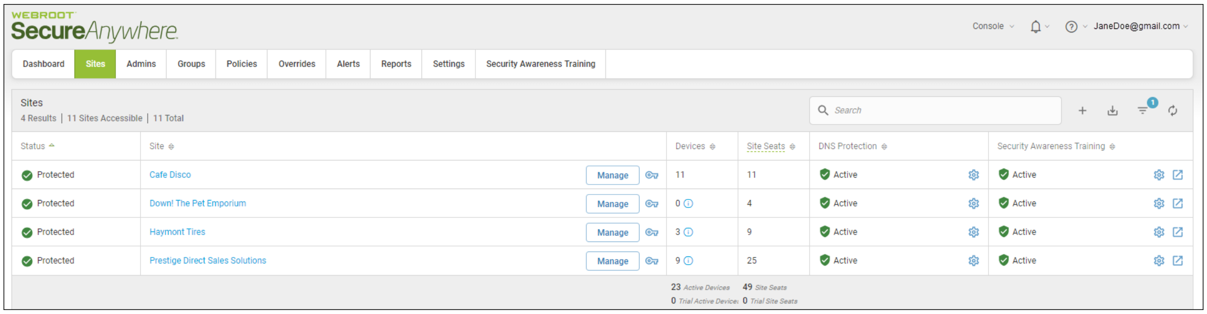
# Copying Policies

Follow this procedure to copy a policy. This is useful if you want to create a new policy that is similar to an existing one.

**To rename a policy:**

1. Log in to the management console.

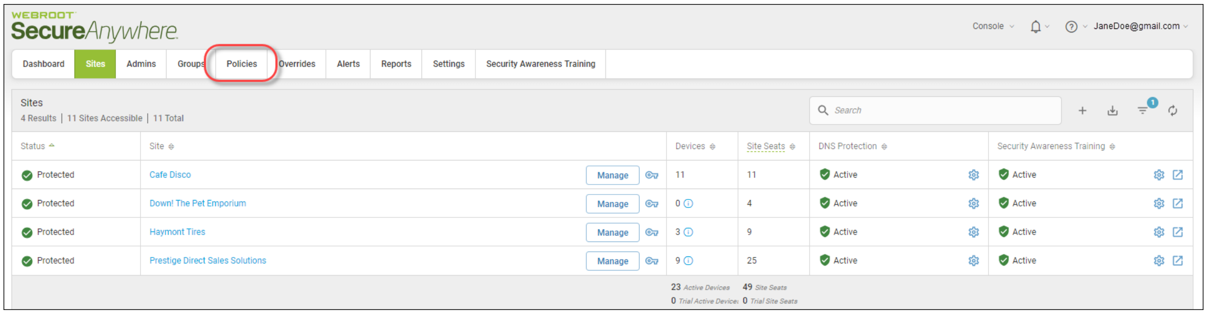
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

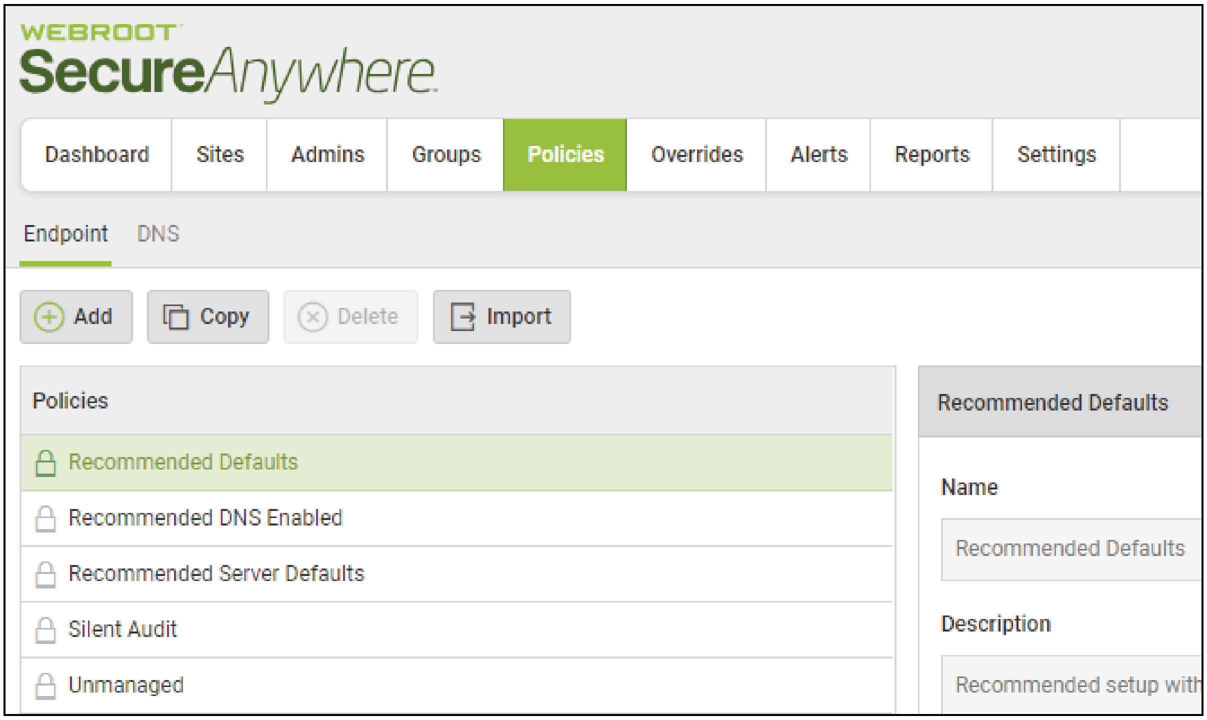
2. Click the **Policies** tab.



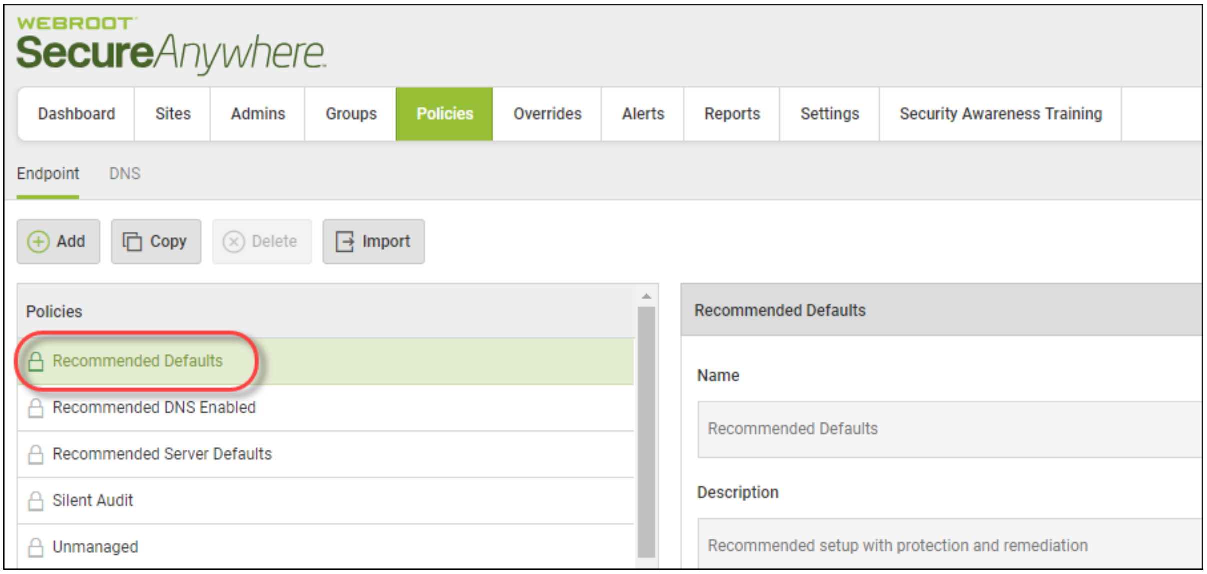
Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

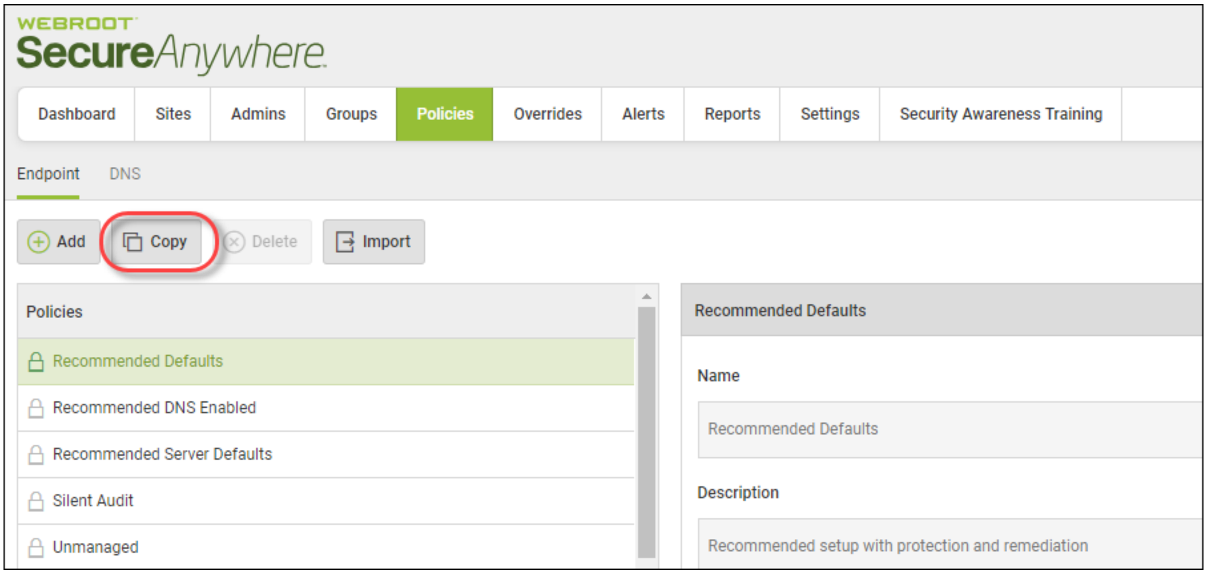
   The Policies tab displays.



3. In the Policies column, select a policy that you want to copy.



4. Click the **Copy** button.



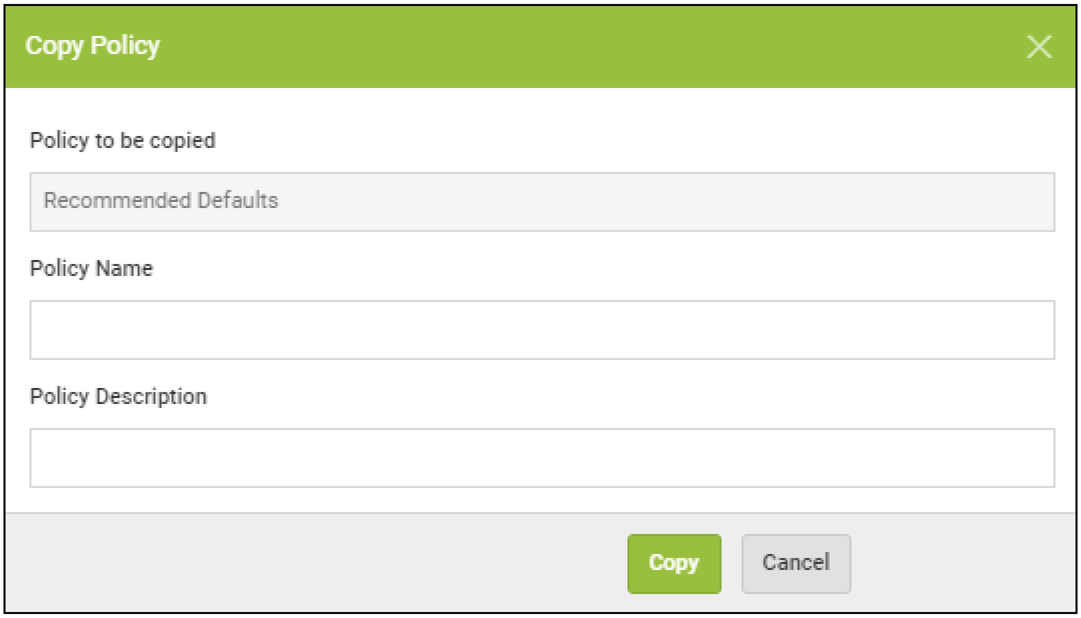
Policies
- Recommended Defaults
- Recommended DNS Enabled
- Recommended Server Defaults
- Silent Audit
- Unmanaged

Recommended Defaults

Name: Recommended Defaults

Description: Recommended setup with protection and remediation

The Copy Policy window displays.



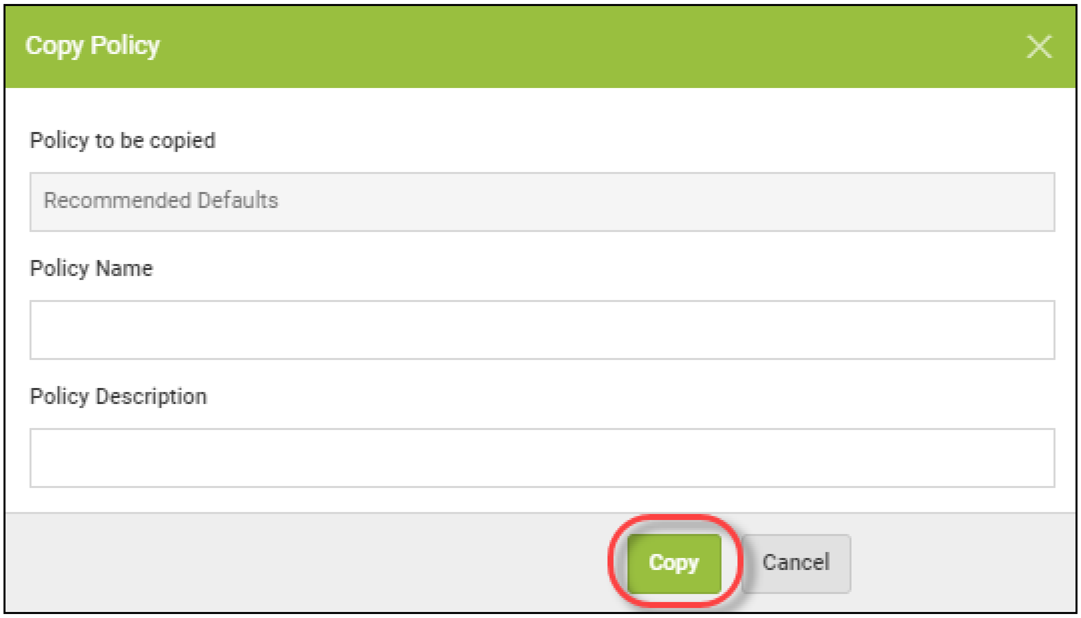
Policy to be copied: Recommended Defaults

Policy Name

Policy Description

5. In the Policy Name field, enter the new name for the policy.
6. In the Policy Description field, enter a new policy description.

7. When you're done, click the **Copy** button.



Copy Policy

Policy to be copied

Recommended Defaults

Policy Name

Policy Description

# Importing Policies Manually

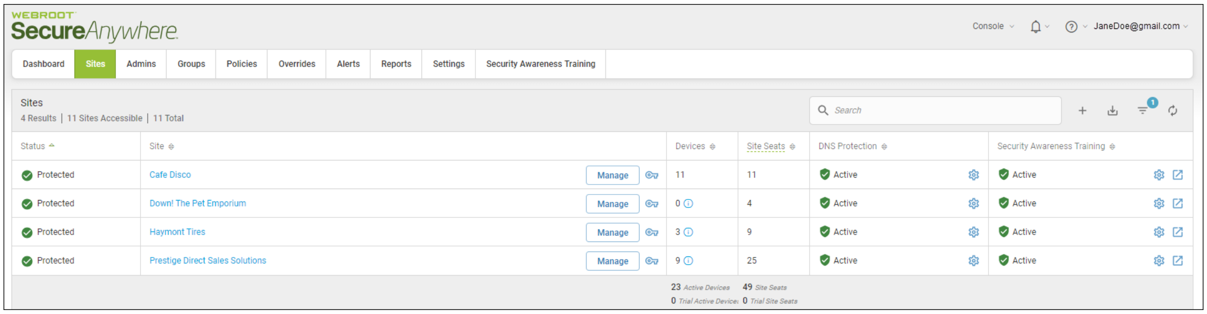
Use this procedure when an administrator wants to import a policy from a site they do not have access to, then only manual import is available.

This procedure useful for administrators' who may have multiple accounts under different email addresses, or who may simply wish to email their transfer code to a friend for them to import into their own site.

### To import a policy manually:

1. Log in to the management console.

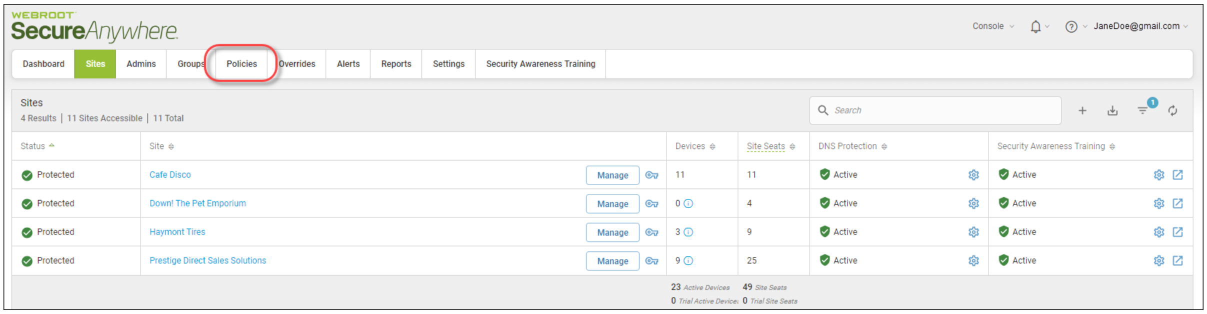
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

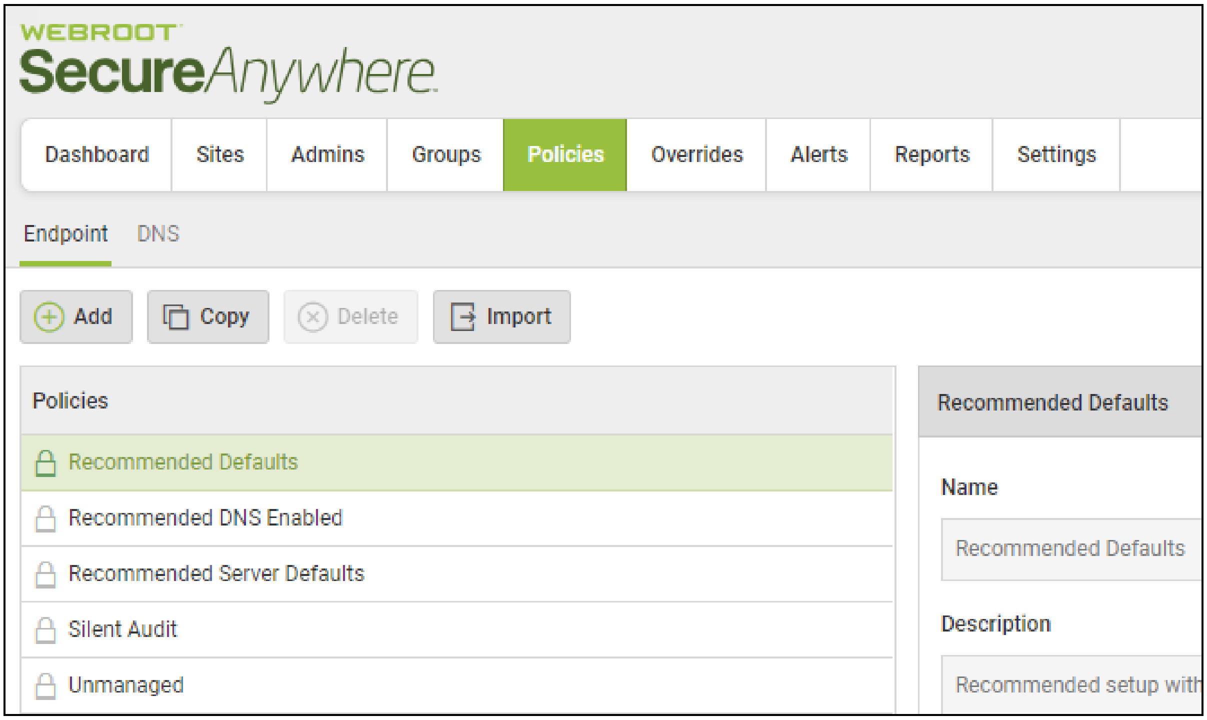
2. Click the **Policies** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Policies tab displays.



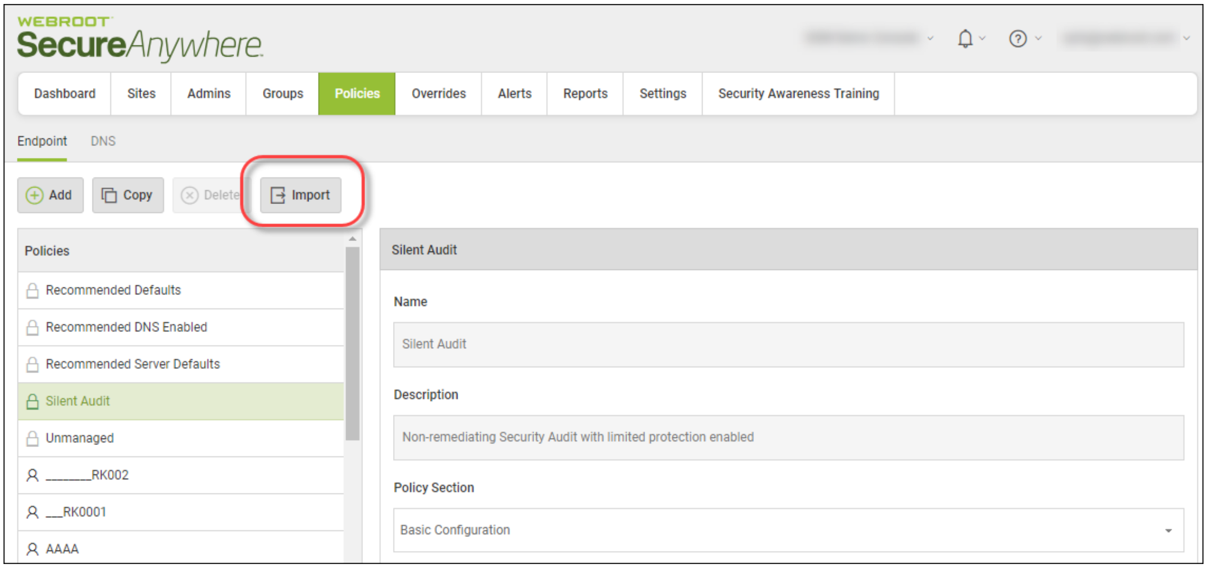
Name

Recommended Defaults

Description

Recommended setup with

3. Click the **Import** button.



Name

Silent Audit

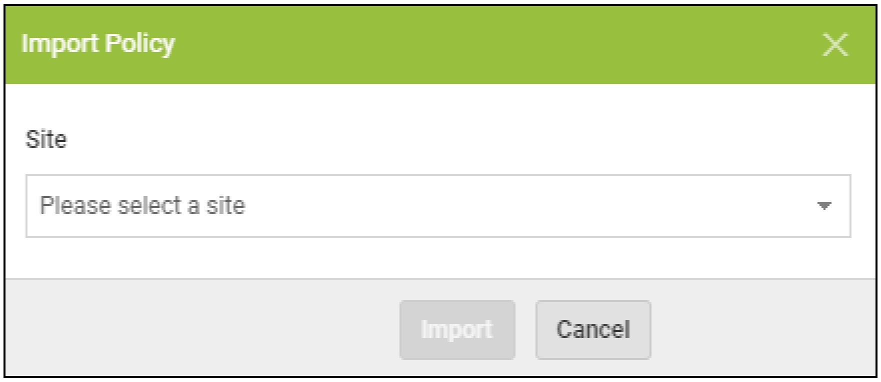
Description

Non-remediating Security Audit with limited protection enabled

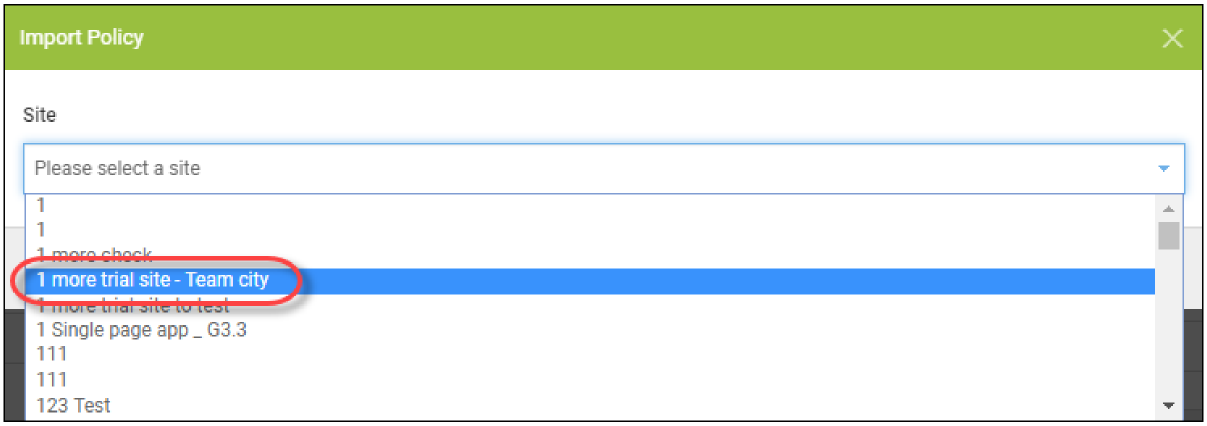
Policy Section

Basic Configuration

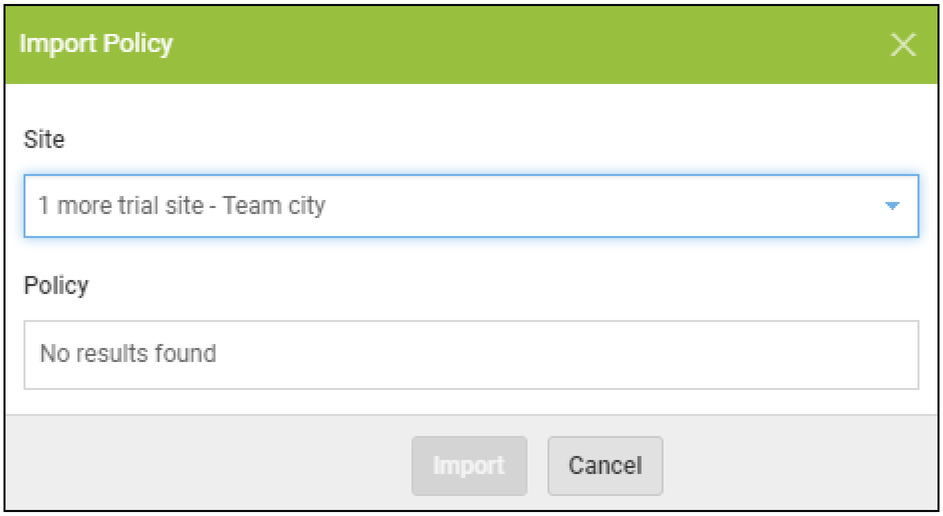
The system displays the Import Policy window.



4. In the Site drop-down menu, select the site you want to import the policy from.



The Policy field becomes active.



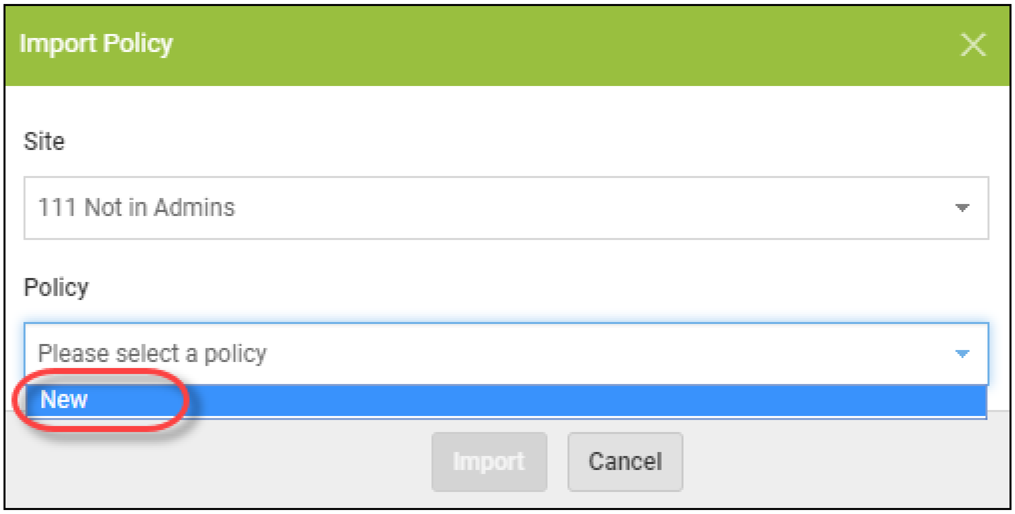
Site

1 more trial site - Team city

Policy

No results found

5. From the Policy drop-down menu, select the policy you want to import.



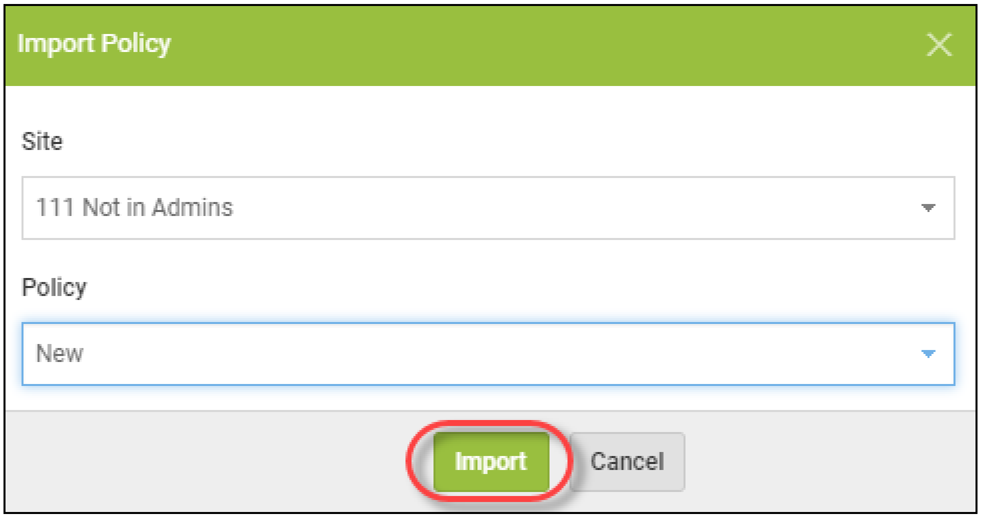
Site

111 Not in Admins

Policy

Please select a policy

6. When you're done, click the **Import** button.



Import Policy

Site: 111 Not in Admins

Policy: New

The system transfers the policy into your management console as a Global Policy.

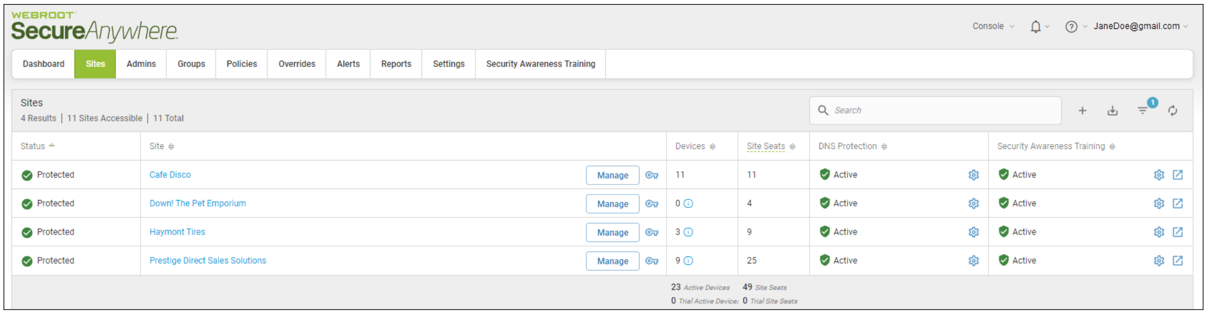
# Deleting Policies

You can delete all policies except for the original default policies. When you delete a policy, the system removes it from the list of active policies.

**To delete a policy:**

1. Log in to the management console.

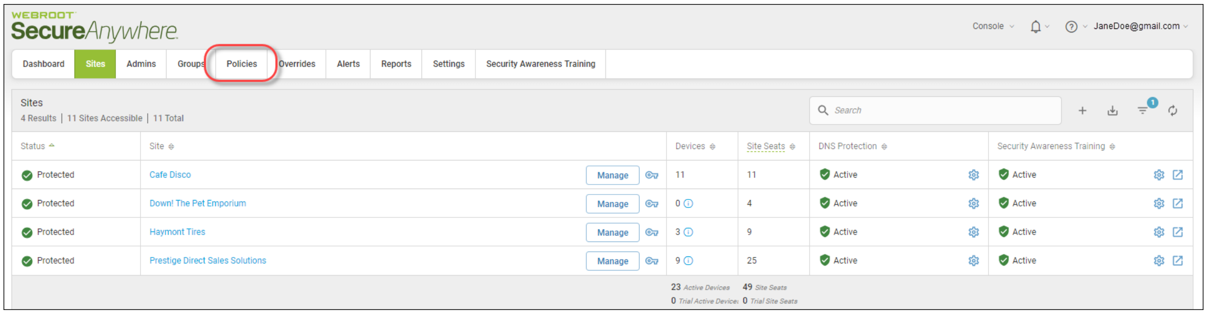
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

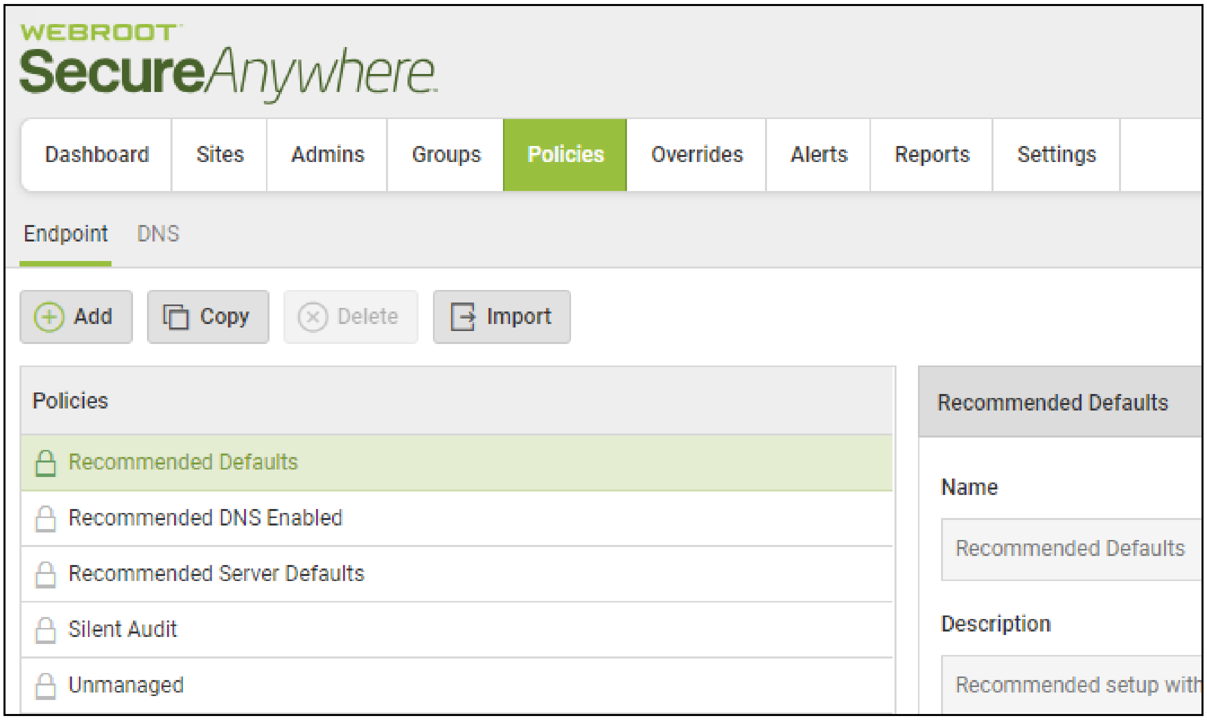
2. Click the **Policies** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Policies tab displays.



Policies

- Recommended Defaults
- Recommended DNS Enabled
- Recommended Server Defaults
- Silent Audit
- Unmanaged

Recommended Defaults

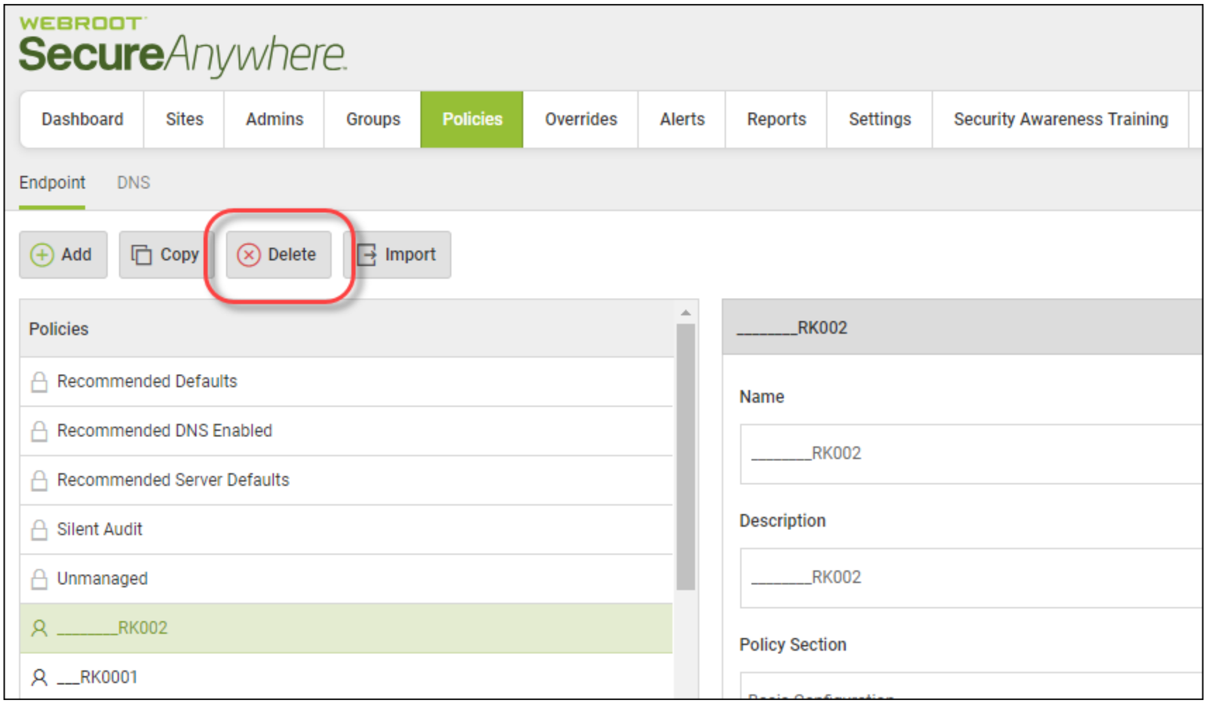
Name

Recommended Defaults

Description

Recommended setup with

3. In the Policies column, select the policy you want to delete and click the **Delete** button



Policies

- Recommended Defaults
- Recommended DNS Enabled
- Recommended Server Defaults
- Silent Audit
- Unmanaged
- ______RK002
- __RK0001

______RK002

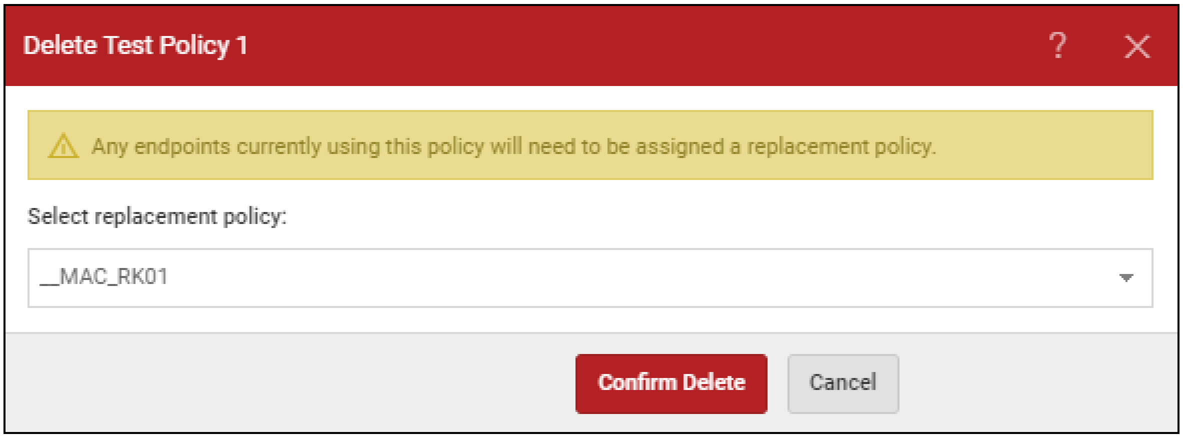
Name: ______RK002

Description: ______RK002

Policy Section

> **Note:** You cannot delete the default policies, so when you click on them, the Delete button does not become active.

The Delete Standard Policy window displays.



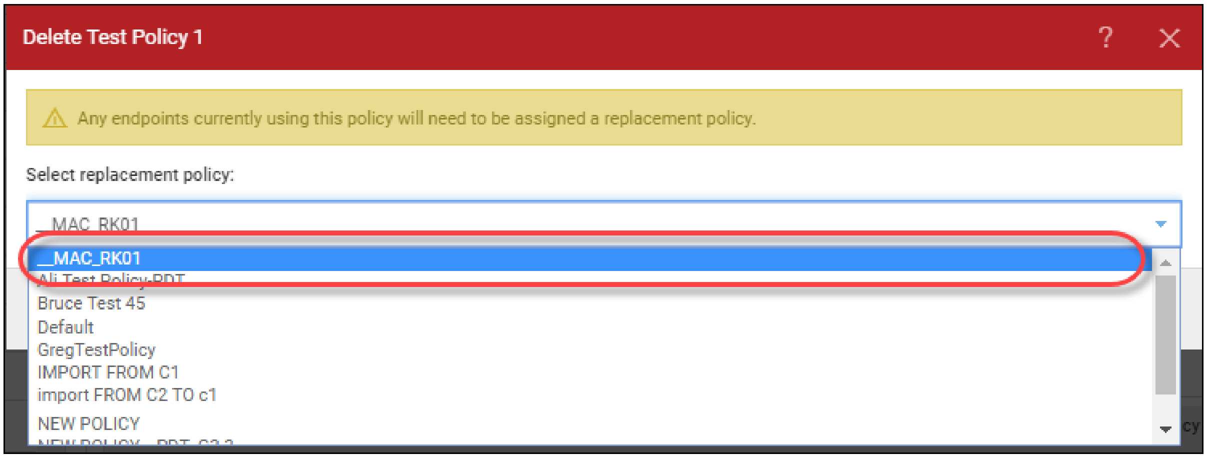
Delete Test Policy 1

Any endpoints currently using this policy will need to be assigned a replacement policy.

Select replacement policy: __MAC_RK01

**Note:** Any endpoints currently using this policy need to be assigned a replacement policy.

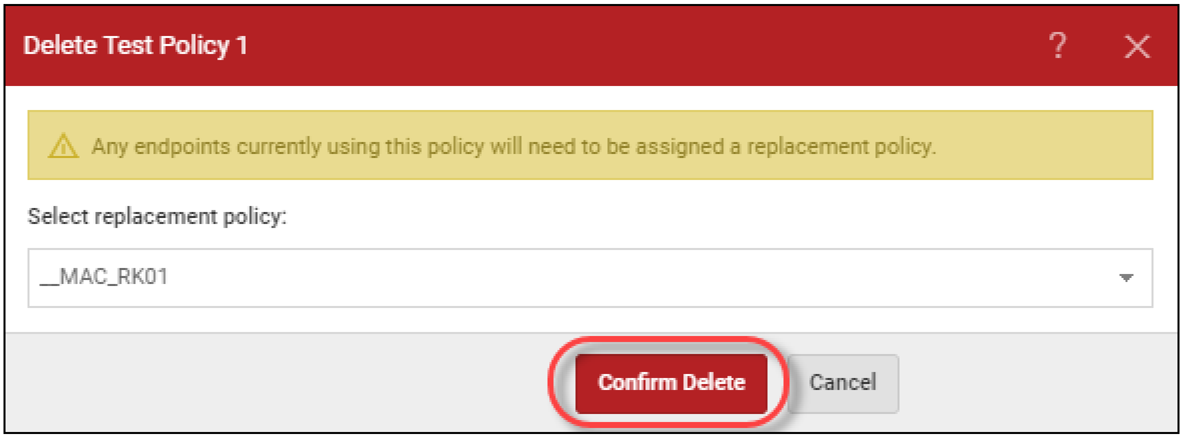
4. As needed, from the Select replacement policy drop-down menu, select a new policy.



Any endpoints currently using this policy will need to be assigned a replacement policy.

Select replacement policy: __MAC_RK01

5. Click the **Confirm Delete** button, and be sure to assign any necessary replacement policies.



Any endpoints currently using this policy will need to be assigned a replacement policy.

Select replacement policy: __MAC_RK01

The system deletes the policy.

# Chapter 8: Working With Overrides

To work with overrides, see the following topics:

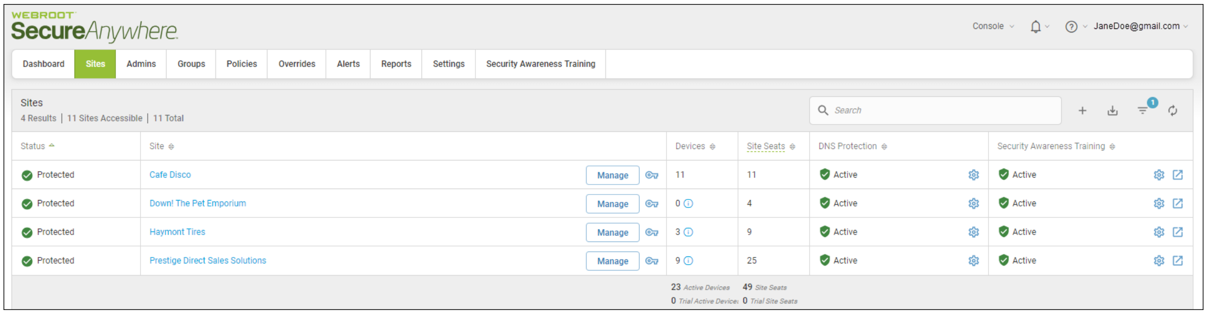
# Creating Web Overrides

Follow this procedure to create a web override that will override the default classifications of the default Web Threat Shield Protection functionality.

### To create a web override:

1. Log in to the management console.

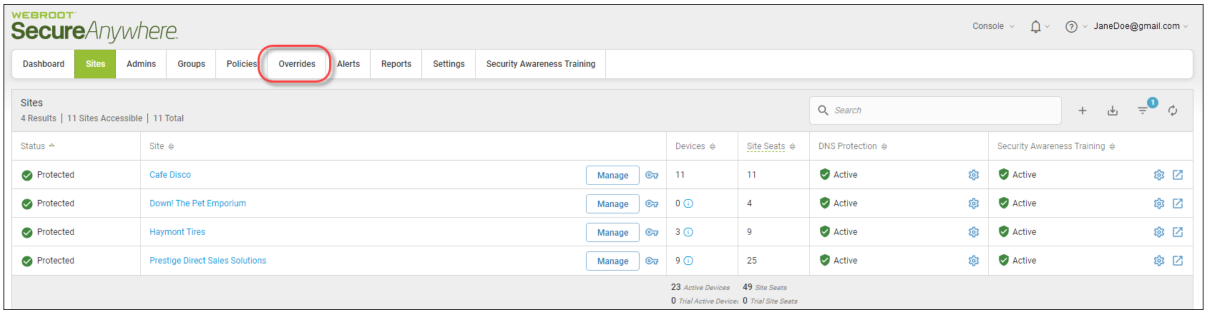
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

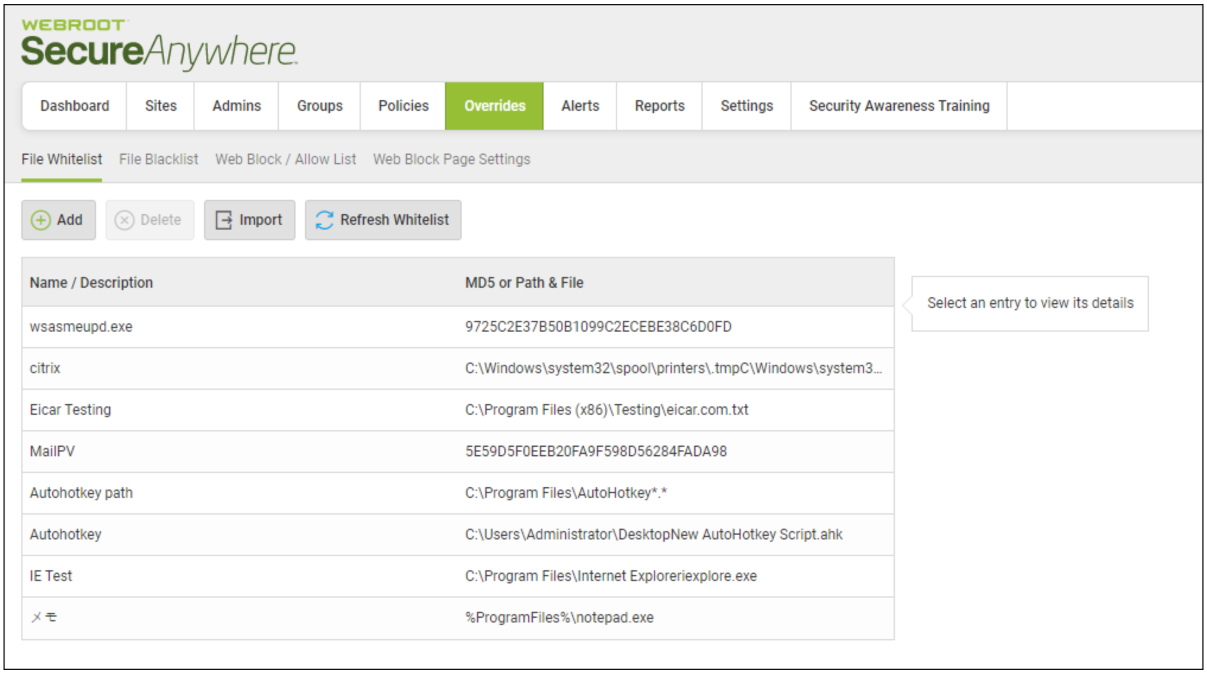
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

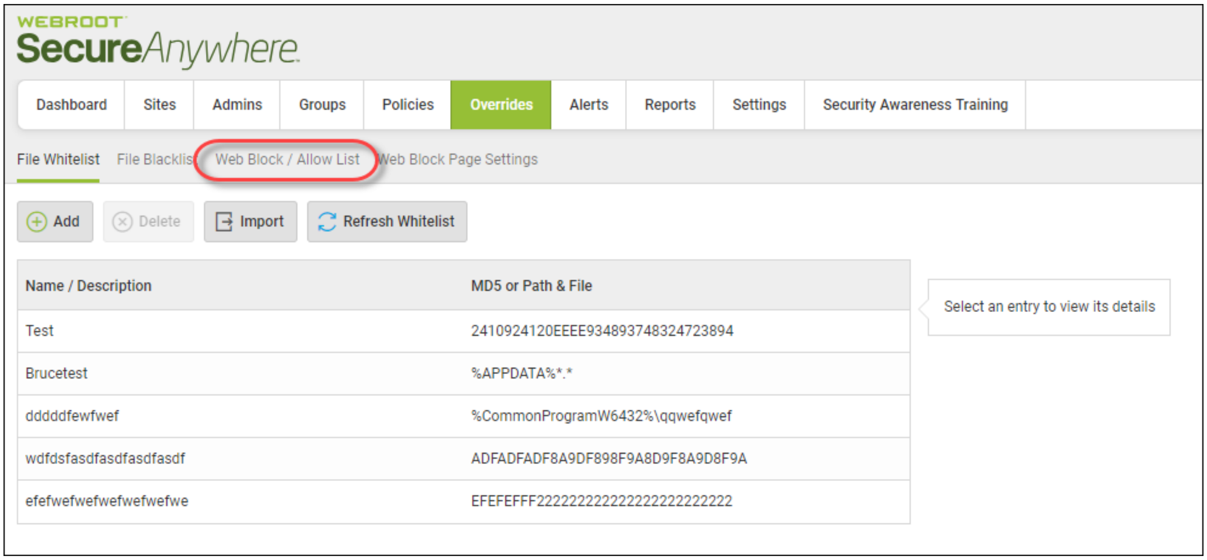
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

The Overrides tab displays, with the File Whitelist tab active.



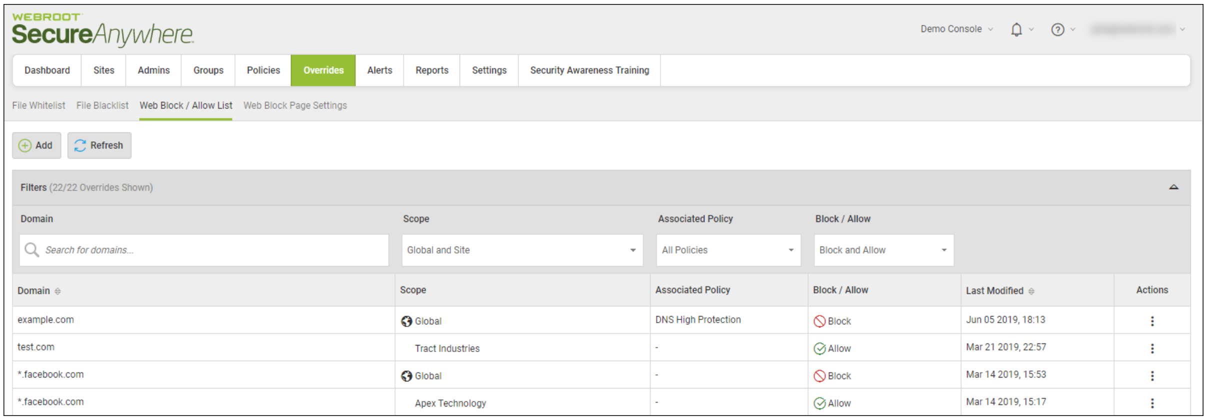
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. Click the **Web Block / Allow List** tab.



| Name / Description | MD5 or Path & File |
|---|---|
| Test | 2410924120EEEE934893748324723894 |
| Brucetest | %APPDATA%*.* |
| dddddfewfwef | %CommonProgramW6432%\qqwefqwef |
| wdfdsfasdfasdfasdfasdf | ADFADFADF8A9DF898F9A8D9F8A9D8F9A |
| efefwefwefwefwefwe | EFEFEFFF222222222222222222222222 |

The Web Block / Allow List tab displays.

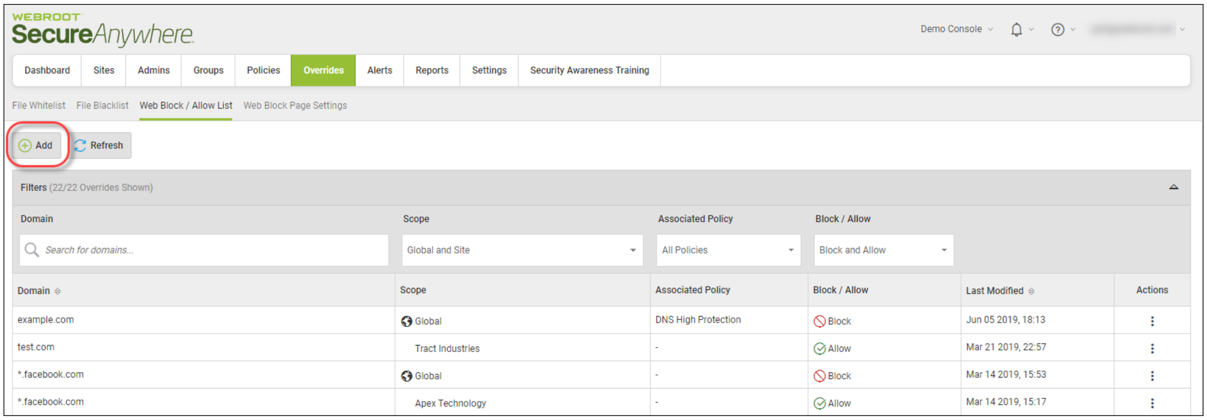


Filters (22/22 Overrides Shown)

| Domain | Scope | Associated Policy | Block / Allow |
|---|---|---|---|
| Search for domains... | Global and Site | All Policies | Block and Allow |

| Domain | Scope | Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|---|---|
| example.com | Global | DNS High Protection | Block | Jun 05 2019, 18:13 | ⋮ |
| test.com | Tract Industries | - | Allow | Mar 21 2019, 22:57 | ⋮ |
| *.facebook.com | Global | - | Block | Mar 14 2019, 15:53 | ⋮ |
| *.facebook.com | Apex Technology | - | Allow | Mar 14 2019, 15:17 | ⋮ |

4. Click the **Add** button.

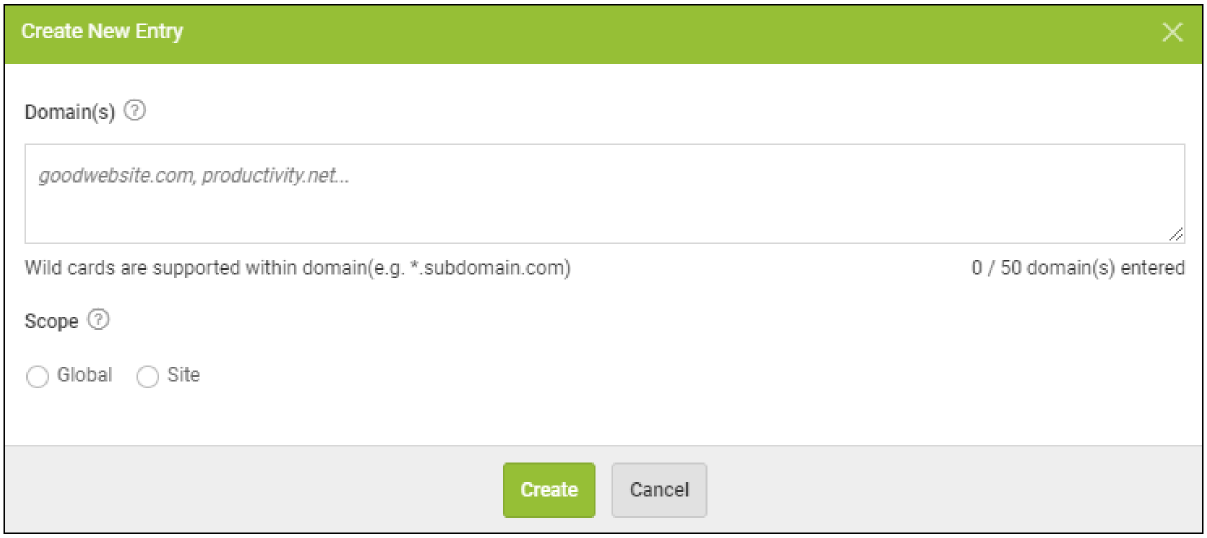


Filters (22/22 Overrides Shown)

| Domain | Scope | Associated Policy | Block / Allow |
|---|---|---|---|
| Search for domains... | Global and Site | All Policies | Block and Allow |

| Domain | Scope | Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|---|---|
| example.com | Global | DNS High Protection | Block | Jun 05 2019, 18:13 | ⋮ |
| test.com | Tract Industries | - | Allow | Mar 21 2019, 22:57 | ⋮ |
| *.facebook.com | Global | - | Block | Mar 14 2019, 15:53 | ⋮ |
| *.facebook.com | Apex Technology | - | Allow | Mar 14 2019, 15:17 | ⋮ |

The Create New Entry window displays.



Create New Entry

Domain(s) ⓘ

goodwebsite.com, productivity.net...

Wild cards are supported within domain(e.g. *.subdomain.com)

0 / 50 domain(s) entered

Scope ⓘ

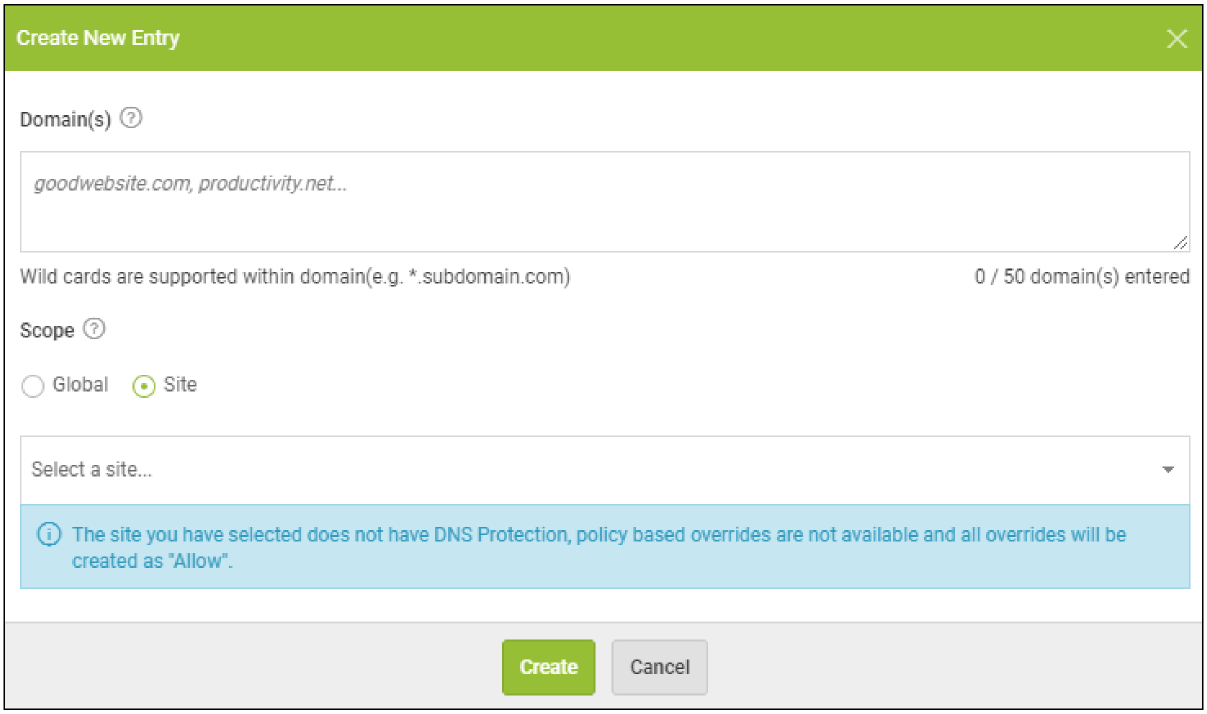
○ Global ○ Site

5. In the Domains field, enter the URL that you want to add as a web override.

> **Note:** When you are entering the URL, you do not have to enter any protocols such as *www*, *http*, or *https*. Also, wildcards are now supported in this field.

6. In the Scope area, select one of the following radio buttons to determine at which site you create the override:
   - **Global** — Makes this entry available for all sites that have the Include Global Overrides checkbox selected in their site settings. For more information, see *Editing Site Settings on page 136*.
   - **Site** — Applies the web override to the specific site that you have selected.

7. If you selected the Site radio button, select a site from the Site drop-down menu.



Create New Entry

Domain(s)

goodwebsite.com, productivity.net...

Wild cards are supported within domain(e.g. *.subdomain.com)

0 / 50 domain(s) entered

Scope

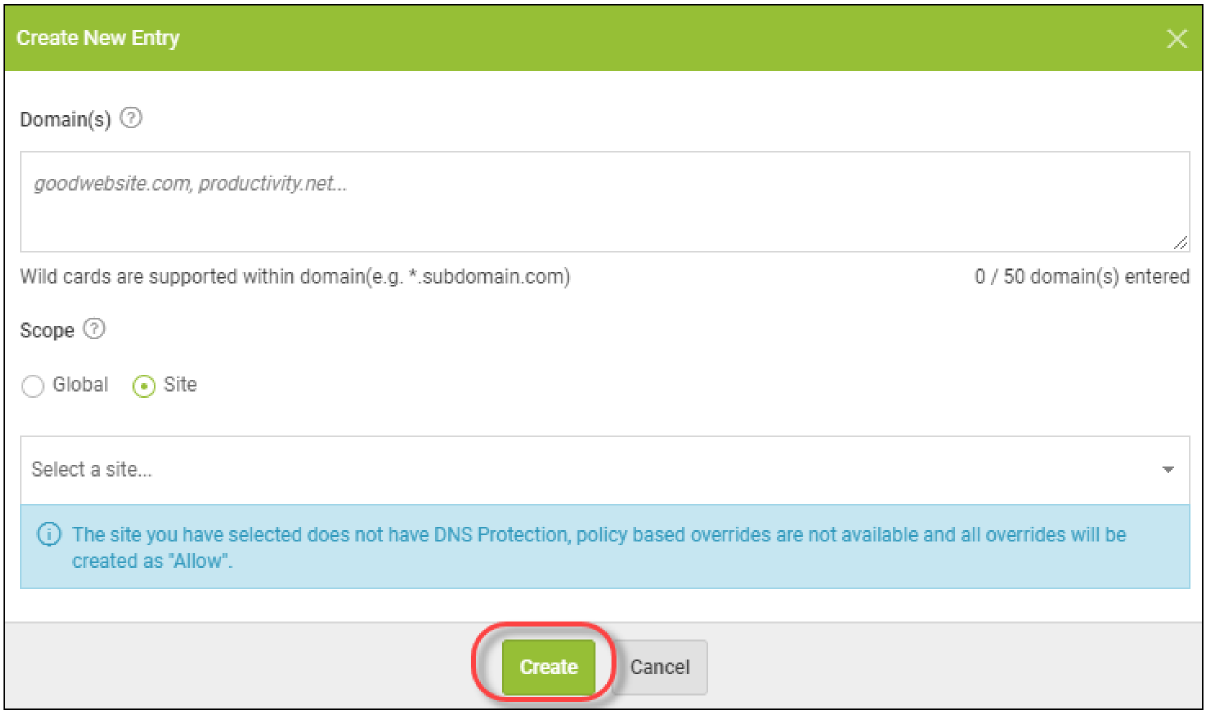
○ Global ● Site

Select a site...

The site you have selected does not have DNS Protection, policy based overrides are not available and all overrides will be created as "Allow".

**Note:** If your site has DNS Protection, see Creating DNS Protection Overrides in the in the Working With Block Pages and Overrides section in the DNS Protection Admin Guide.

8. When you're done, click the **Create** button.



The site you have selected does not have DNS Protection, policy based overrides are not available and all overrides will be created as "Allow".

# Creating Whitelist Overrides

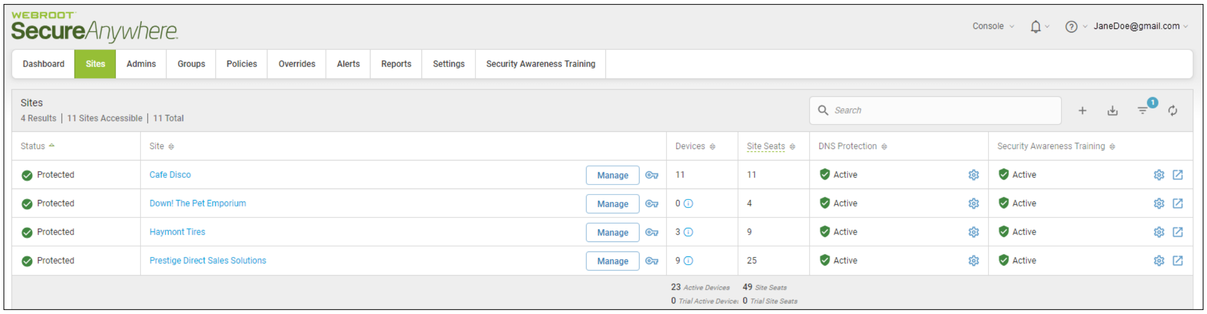
Under the overrides page at both management console and Site levels, you can now create whitelist overrides.

Global whitelist overrides can now be set on a file or folder level as well as the traditional MD5 level. This upgrade allows greater flexibility in the deployment of overrides and means that multiple related MD5 overrides no longer have to be whitelisted individually, instead the whole associated directory can simply be whitelisted.

**To create a whitelist override:**

1. Log in to the management console.

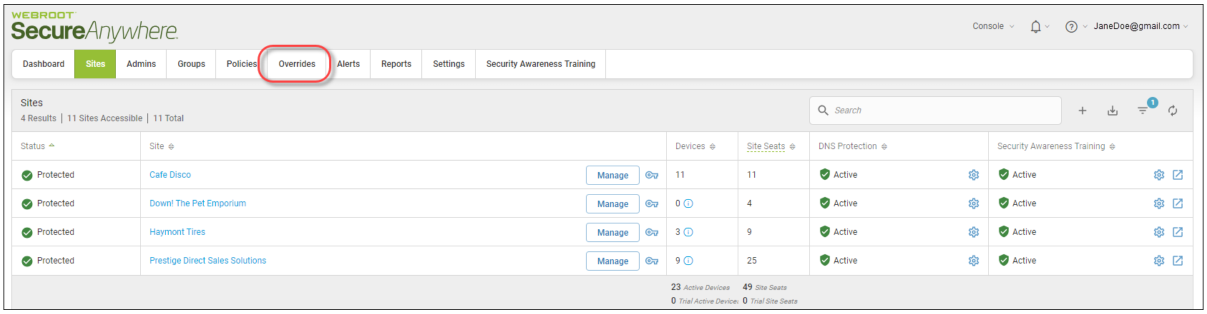
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

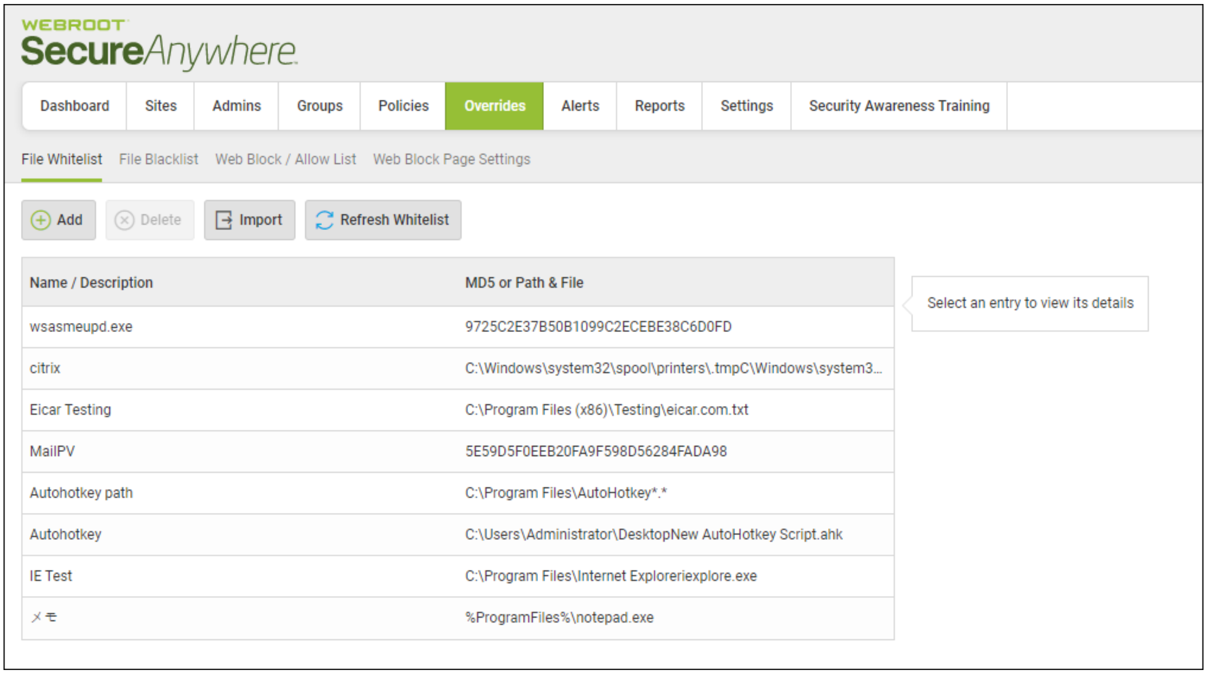
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

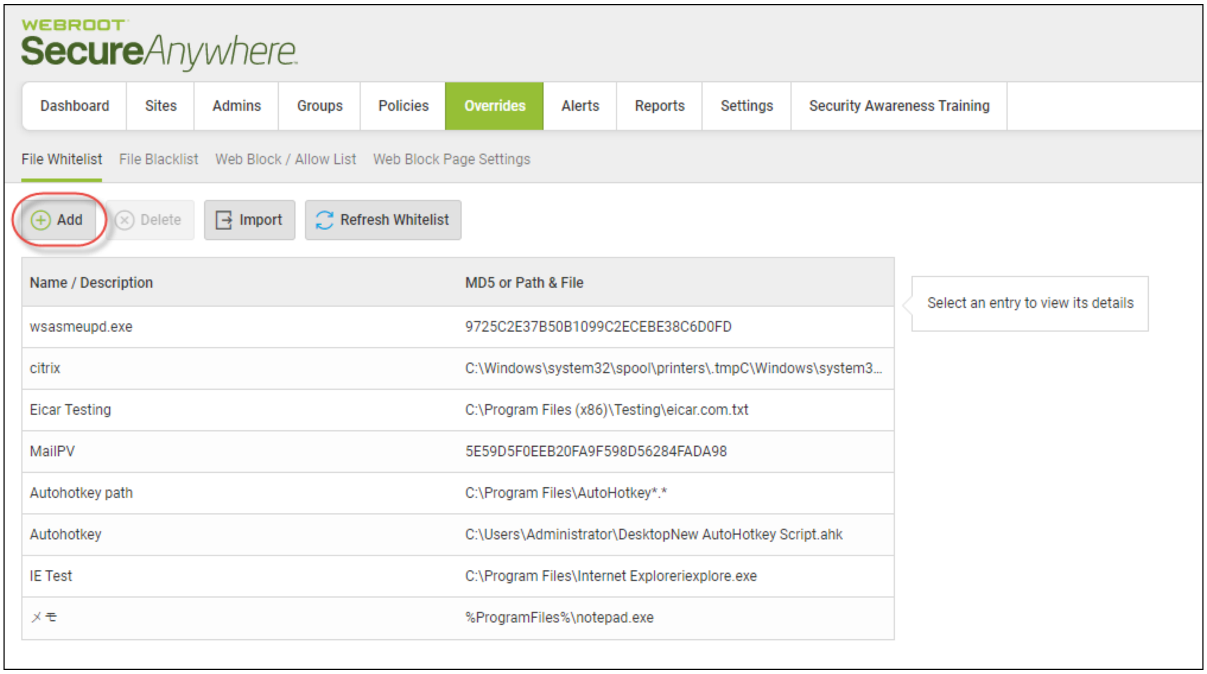
The Overrides tab displays, with the File Whitelist tab active.



| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

Select an entry to view its details

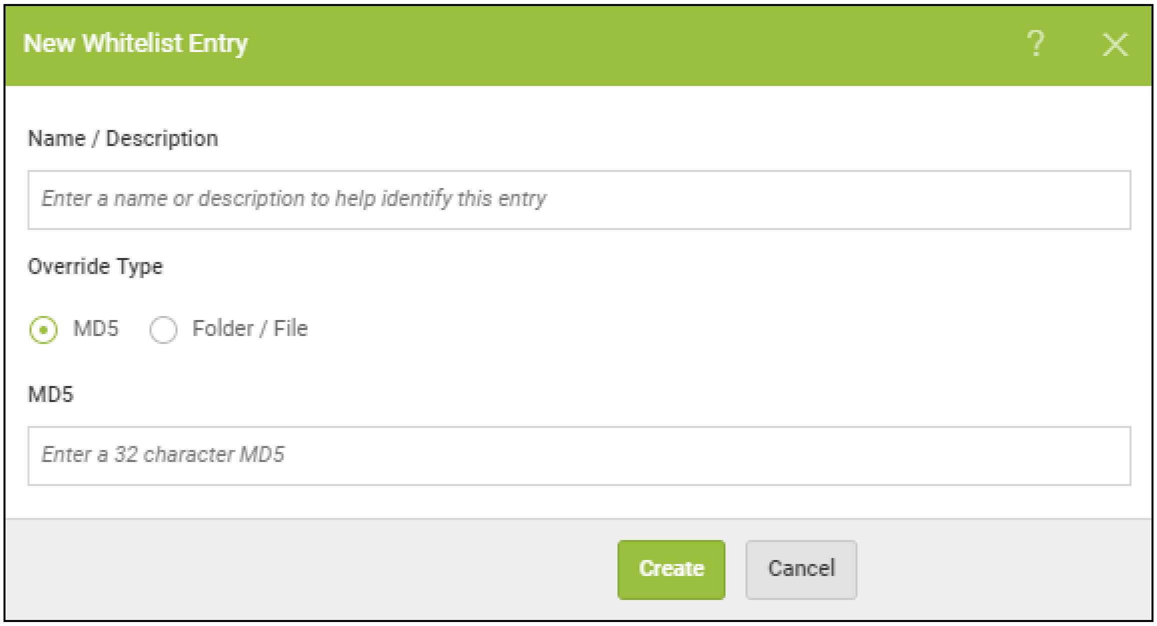
3. Click the **Add** button.



| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

Select an entry to view its details

4. The system displays the New Whitelist Entry window.



New Whitelist Entry

Name / Description

*Enter a name or description to help identify this entry*

Override Type

● MD5 ○ Folder / File

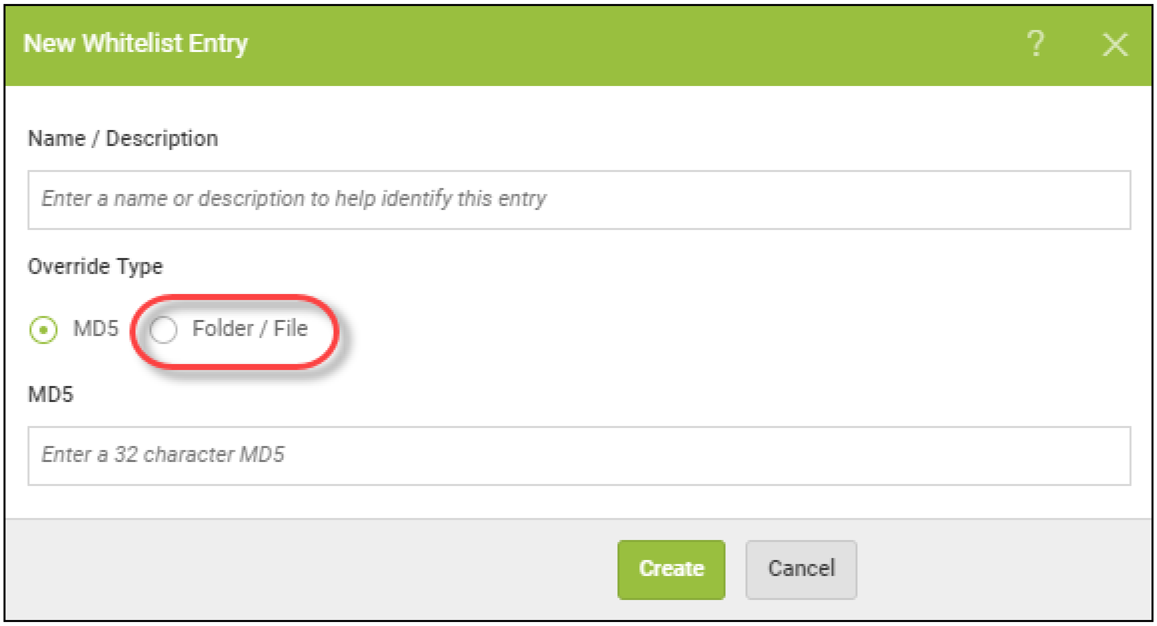
MD5

*Enter a 32 character MD5*

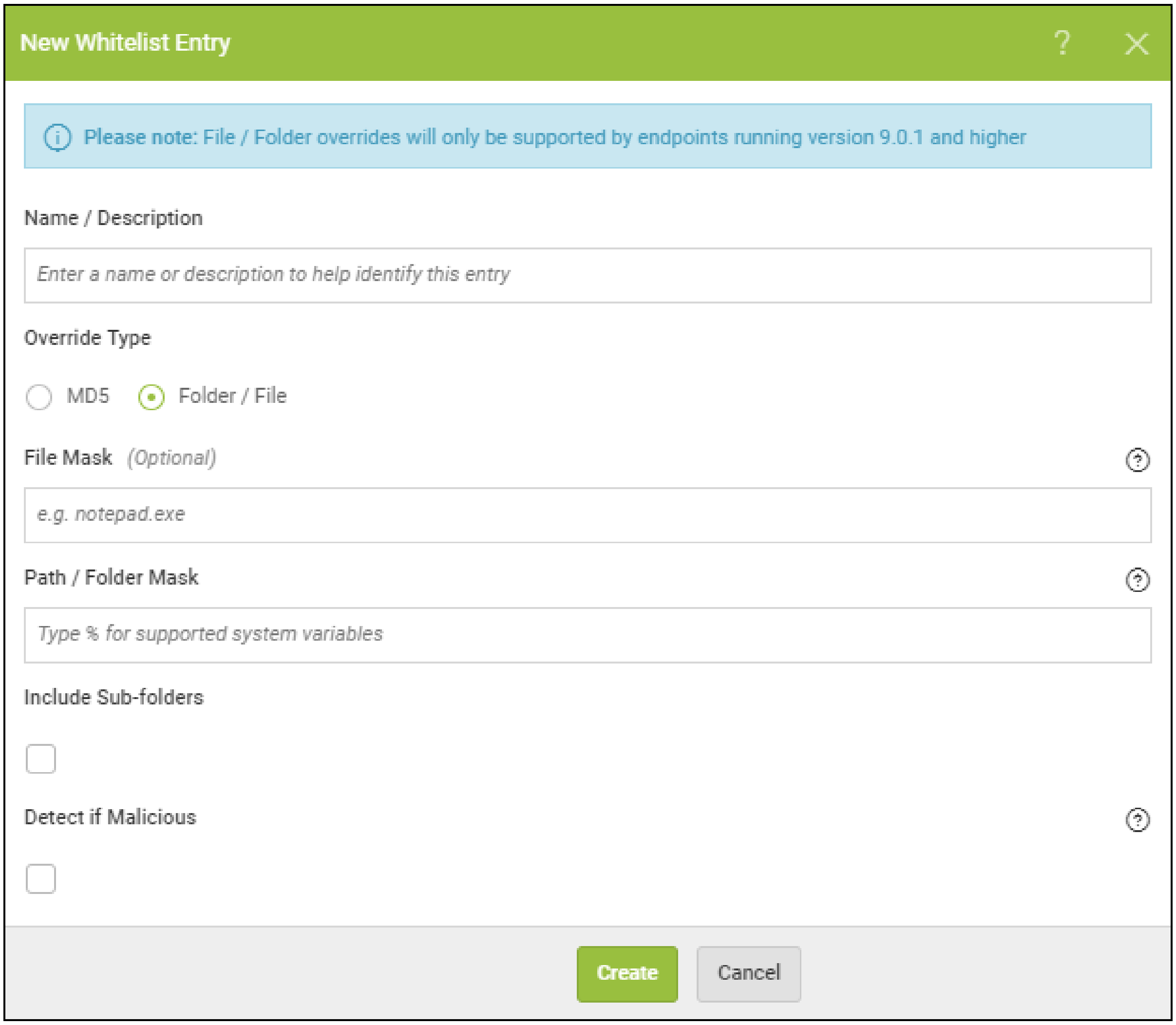
5. To create an MD5 override type, do the following:
   - In the Name/Description field, enter a name for the override
   - Select the **MD5** radio button.
   - In the MD5 field, enter the 32-character unique identifier for the file.
   - Click the **Create** button.
6. To create a Folder/File override, continue with this procedure.

> **Note:** To use File/Folder overrides please make sure endpoints are running version 9.0.1 or higher of Webroot SecureAnywhere Endpoint Protection. Earlier versions support MD5 overrides only.

7. In the New Whitelist Entry window, select the **Folder/File** radio button.



The system displays the New Whitelist Entry window with the relevant fields.

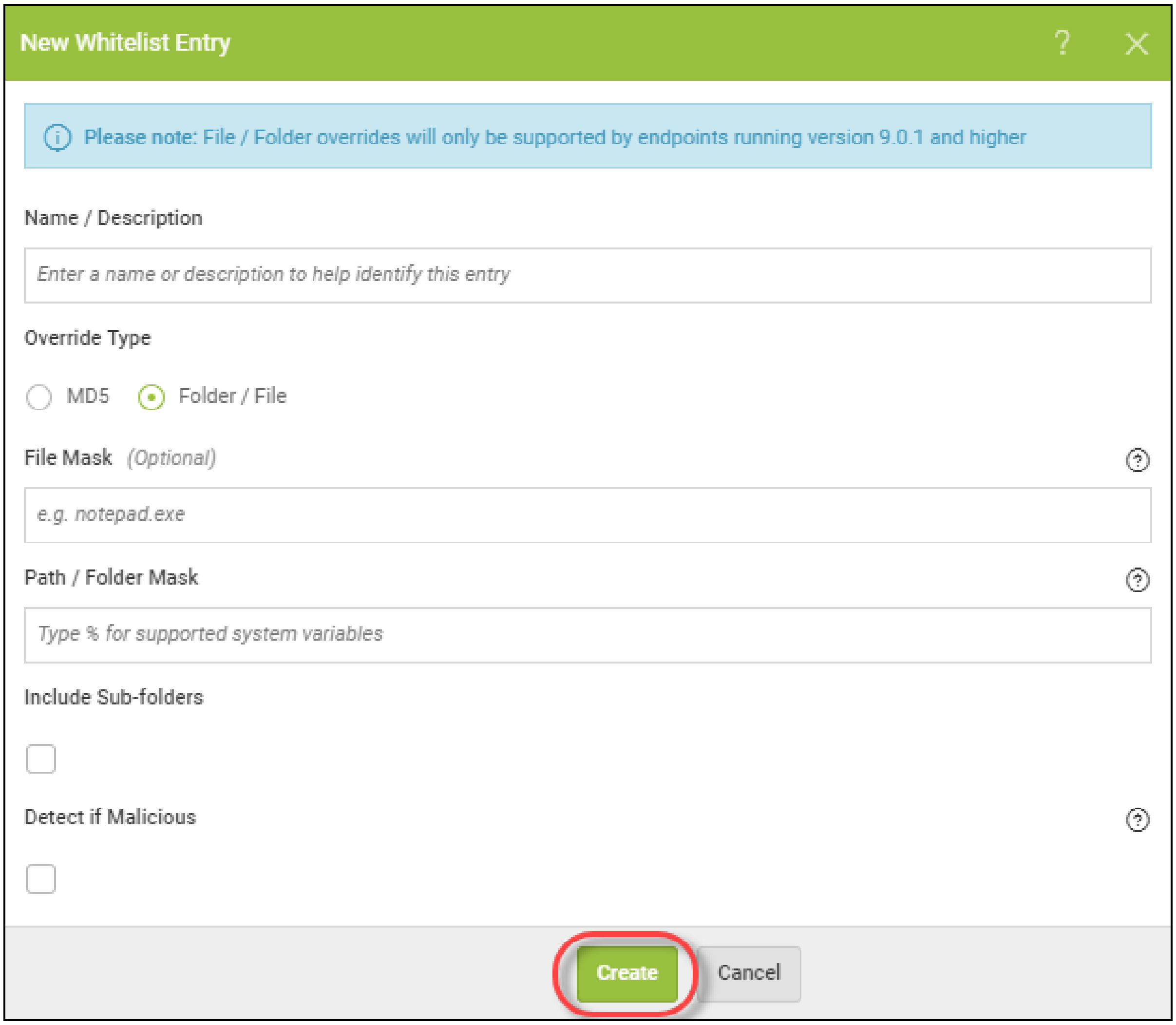

New Whitelist Entry
?
Please note: File / Folder overrides will only be supported by endpoints running version 9.0.1 and higher
Name / Description
Enter a name or description to help identify this entry
Override Type
○ MD5 ● Folder / File
File Mask (Optional)
e.g. notepad.exe
Path / Folder Mask
Type % for supported system variables
Include Sub-folders
□
Detect if Malicious
□
Create
Cancel

8. Populate the fields on the window using the information in the following table.

| FIELD | DESCRIPTION |
|---|---|
| **Name / Description** | Target a file or group of files by specifying a file mask with optional wildcards, for example, *.exe to target all executable files in the selected folder.<br>This will default to all files in the selected folder/path if not specified. |
| **Override Type** | You have already selected the Folder/File radio button. |
| **File Mask** | Target a file or group of files by specifying a file mask with optional wildcards, for example, *.exe to target all executable files in the selected folder. This will default to all files in the selected folder/path if not specified. |
| **Path / Folder Mask** | The folder to target with the override.<br>You can specify an absolute path, for example, 'x:\myfolder\' or a system variable with optional path, for example, '%SystemDrive%\myfolder'. Default supported environment variables are displayed when you type '%' however you may use any variable you have set up on the target machine with the exception of user variables, which are not supported.<br>You may not use '%temp%' for example as this refers to a specific users temp directory ('username/temp/'). Wildcards are not supported. |

| FIELD | DESCRIPTION |
|---|---|
| **Include Sub-folders** | Select this checkbox to apply the override to all sub-folders within this folder. |
| **Detect if Malicious** | If this setting is enabled Webroot will continue to protect the user against threats originating from the selected file/folder whitelist override but will disable monitoring and journaling.<br>This is primarily used to improve performance when monitoring and journaling is being applied to a large number of files with an unknown determination. Disabling this setting will provide a true whitelisting, allowing files to run without Webroot protection. |

9. When you're done, click the **Create** button.



New Whitelist Entry

Please note: File / Folder overrides will only be supported by endpoints running version 9.0.1 and higher

Name / Description

Enter a name or description to help identify this entry

Override Type

○ MD5 ● Folder / File

File Mask (Optional)

e.g. notepad.exe

Path / Folder Mask

Type % for supported system variables

Include Sub-folders

□

Detect if Malicious

□

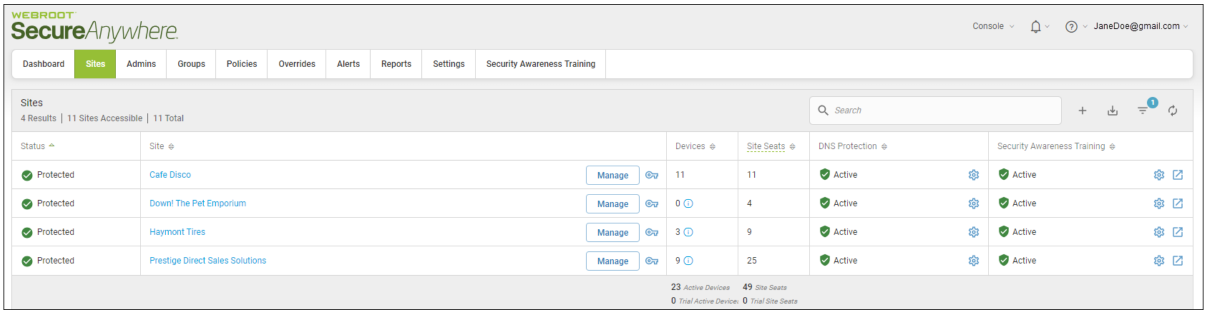
# Creating Blacklist Overrides

Under the overrides page at both management console and Site level, you can now create blacklist overrides.

**To create a blacklist override:**

1. Log in to the management console.

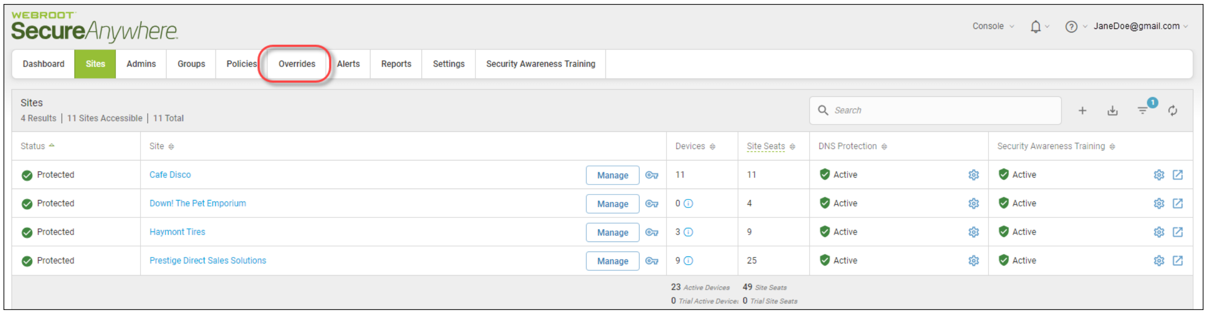
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

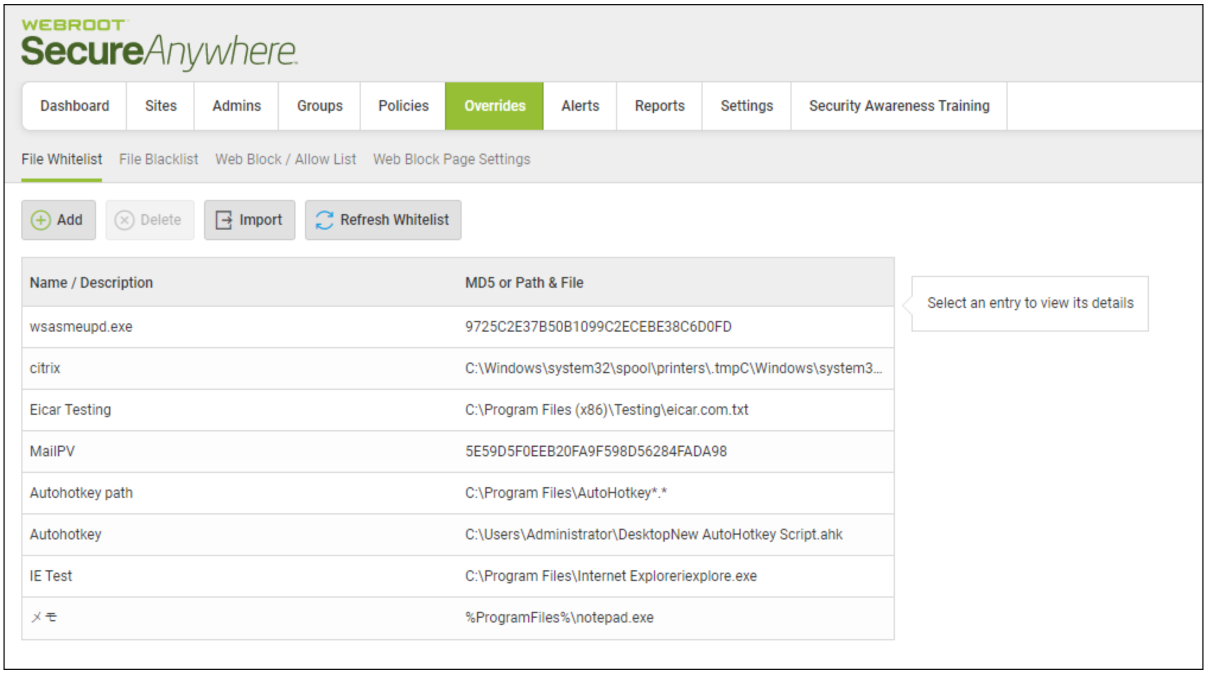
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

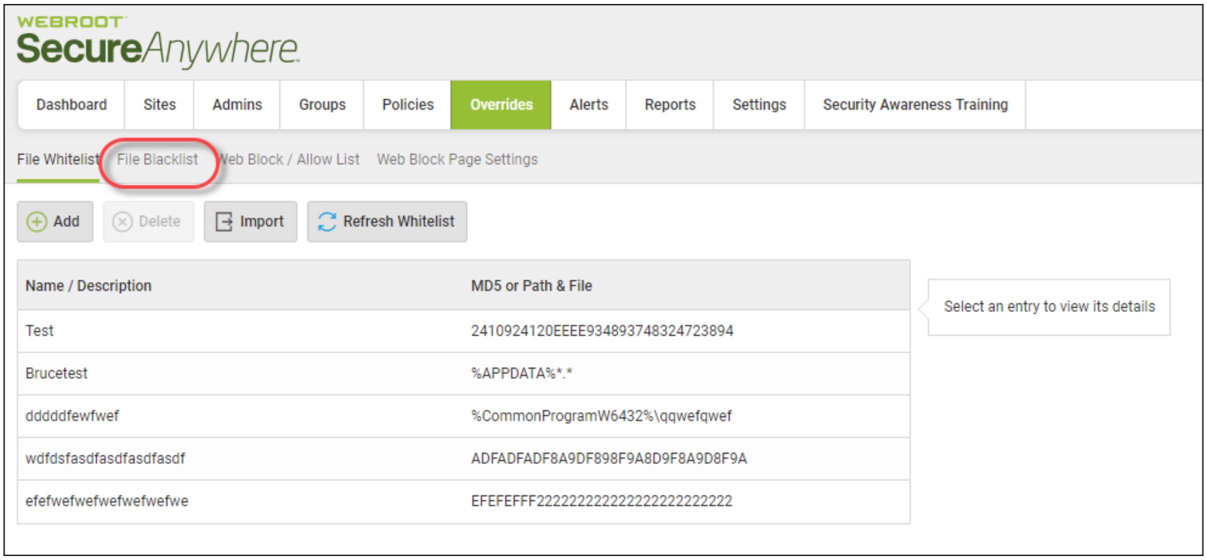
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

The Overrides tab displays, with the File Whitelist tab active.



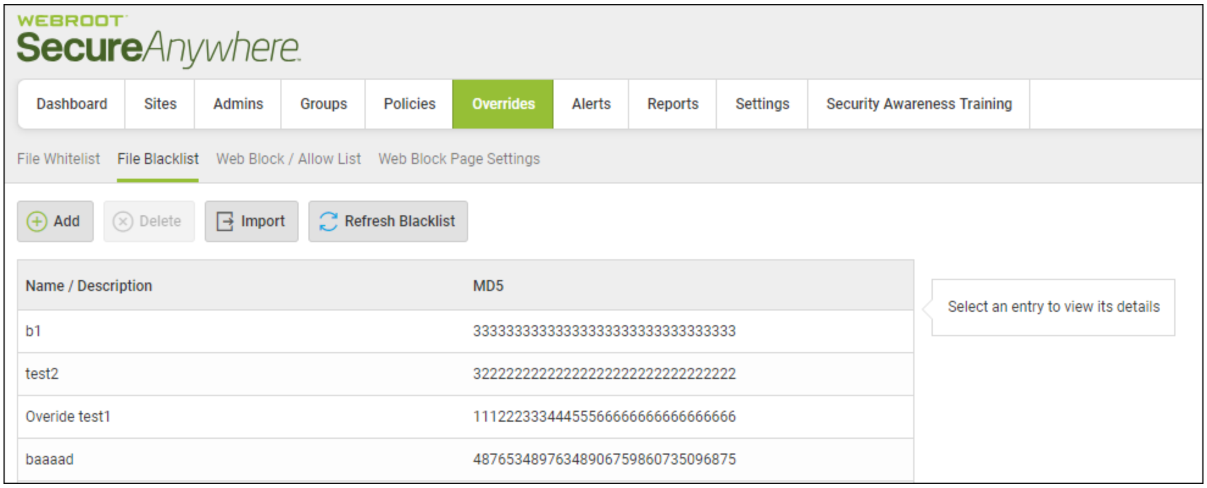
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. Click the **File Blacklist** tab.



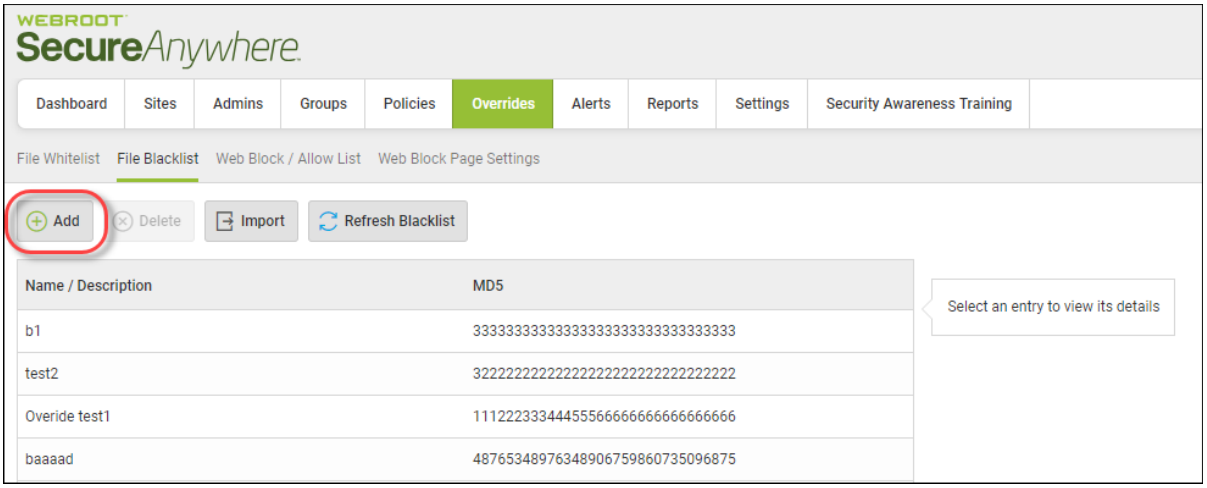
| Name / Description | MD5 or Path & File |
|---|---|
| Test | 2410924120EEEE934893748324723894 |
| Brucetest | %APPDATA%*.* |
| dddddfewfwef | %CommonProgramW6432%\qqwefqwef |
| wdfdsfasdfasdfasdfasdf | ADFADFADF8A9DF898F9A8D9F8A9D8F9A |
| efefwefwefwefwefwefwe | EFEFEFFF222222222222222222222222 |

The File Blacklist tab displays.



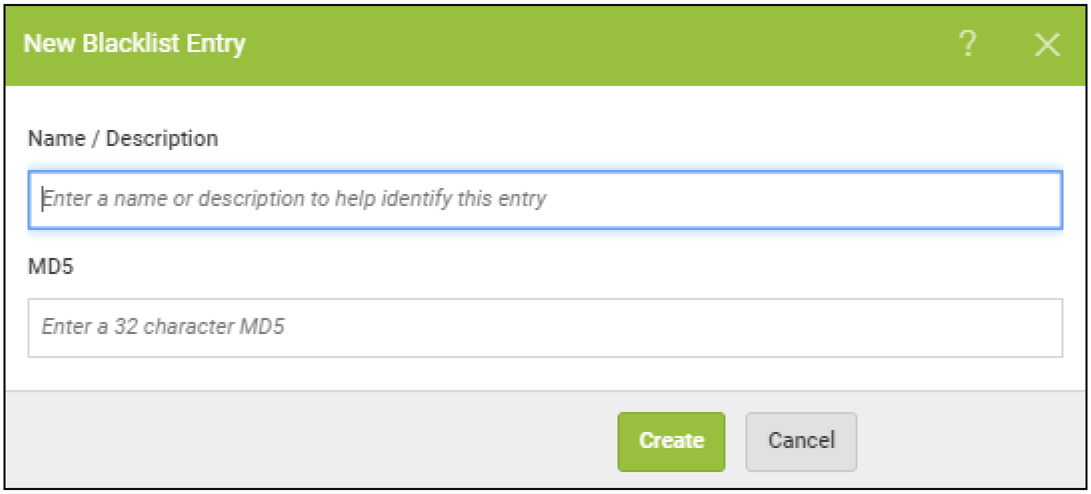
| Name / Description | MD5 |
|---|---|
| b1 | 33333333333333333333333333333333 |
| test2 | 32222222222222222222222222222222 |
| Overide test1 | 11122233344455566666666666666666 |
| baaaad | 48765348976348906759860735096875 |

4. Click the **Add** button.

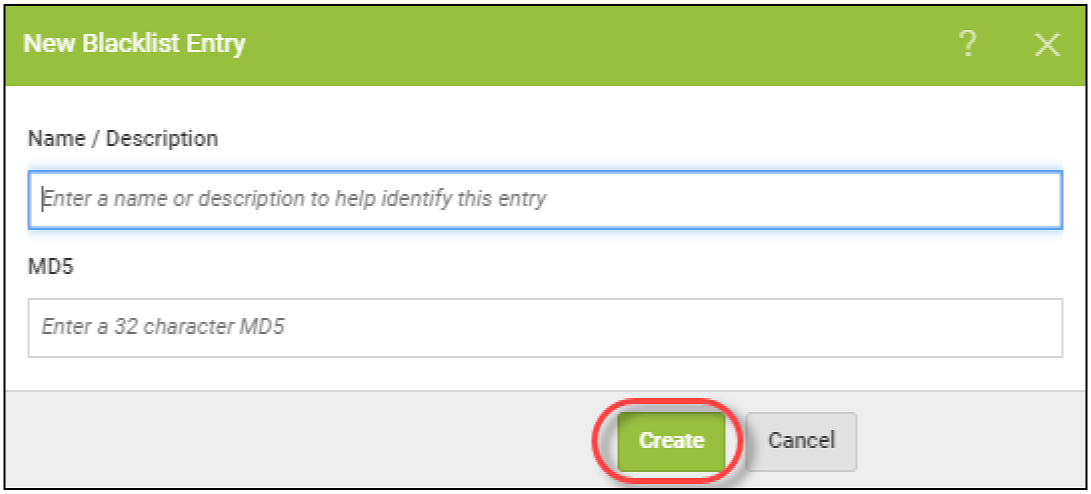


| Name / Description | MD5 |
|---|---|
| b1 | 33333333333333333333333333333333 |
| test2 | 32222222222222222222222222222222 |
| Overide test1 | 11122233344455566666666666666666 |
| baaaad | 48765348976348906759860735096875 |

The system displays the New Blacklist Entry window.



5. In the Name/Description field, enter a name for the override.
6. In the MD5 field, enter the 32-character unique identifier for the file.
7. When you're done, click the **Create** button.



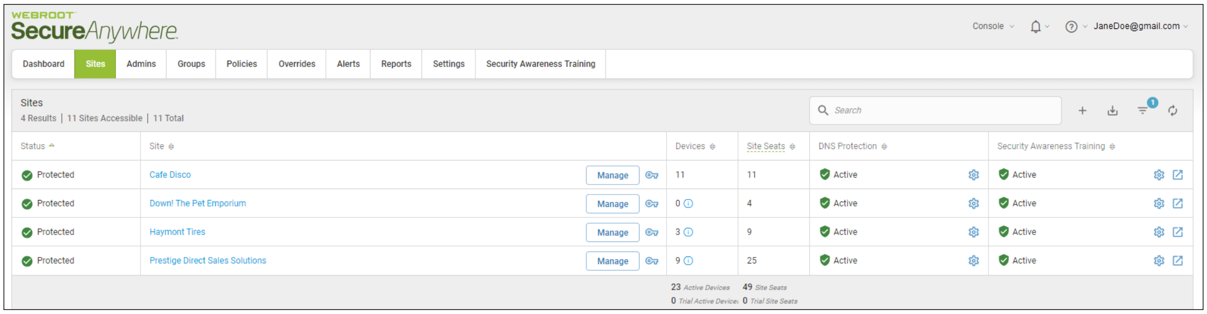
# Editing Web Overrides

Follow this procedure to edit web overrides.

**To edit a web override:**

1. Log in to the management console.

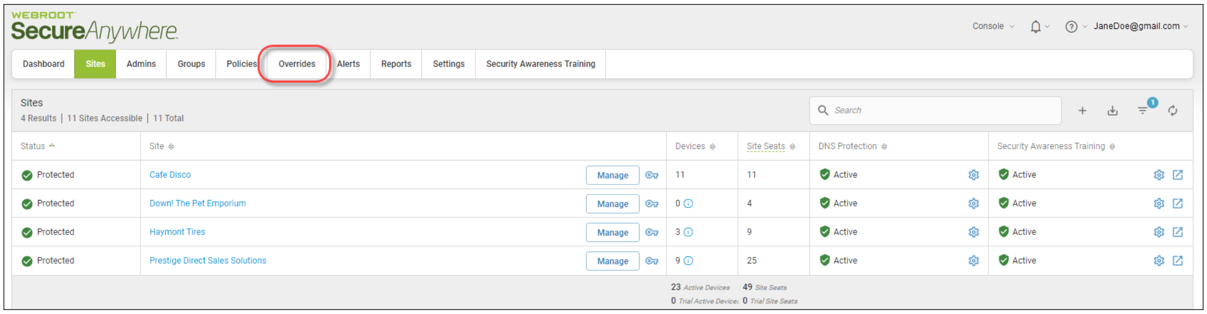
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

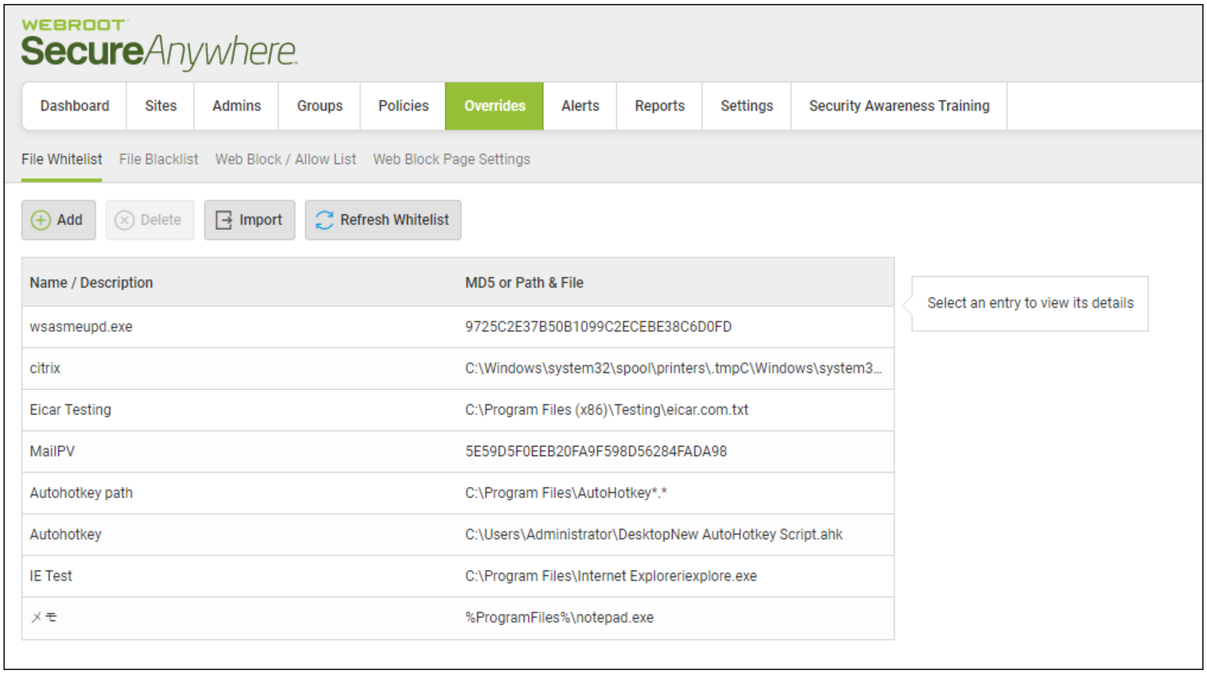
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

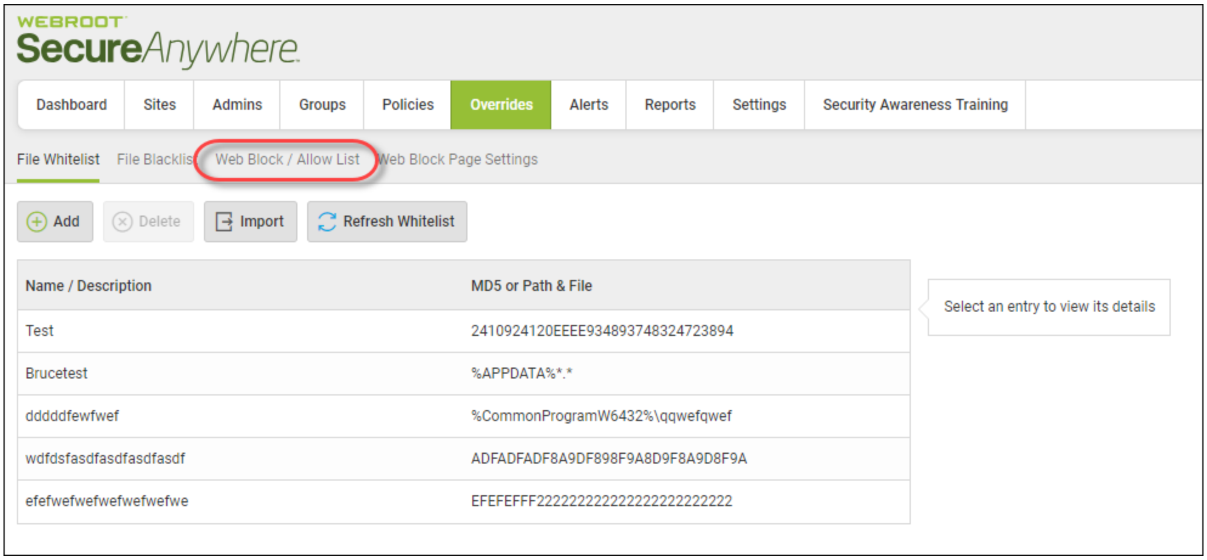
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

The Overrides tab displays, with the File Whitelist tab active.



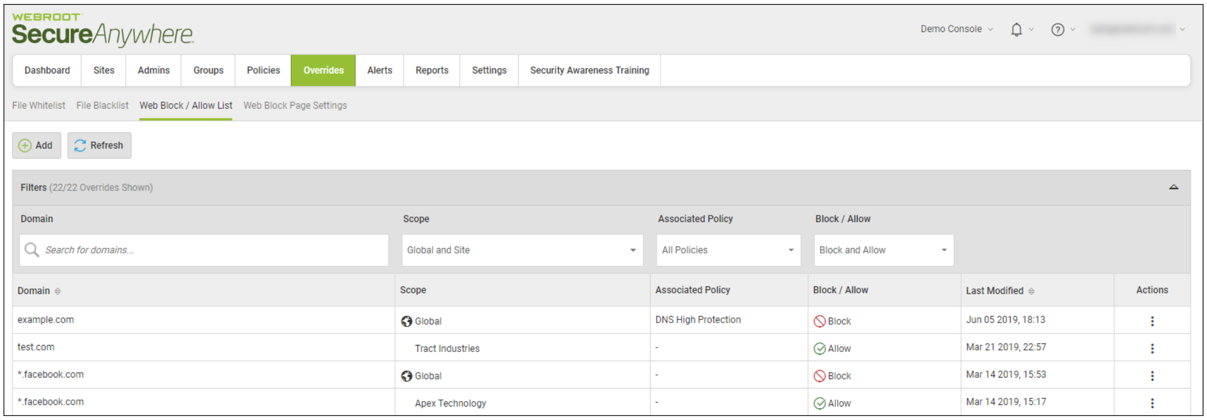
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. Click the **Web Block / Allow List** tab.



| Name / Description | MD5 or Path & File |
|---|---|
| Test | 2410924120EEEE934893748324723894 |
| Brucetest | %APPDATA%*.* |
| dddddfewfwef | %CommonProgramW6432%\qqwefqwef |
| wdfdsfasdfasdfasdfasdf | ADFADFADF8A9DF898F9A8D9F8A9D8F9A |
| efefwefwefwefwefwefwe | EFEFEFFF222222222222222222222222 |

The Web Block / Allow List tab displays.

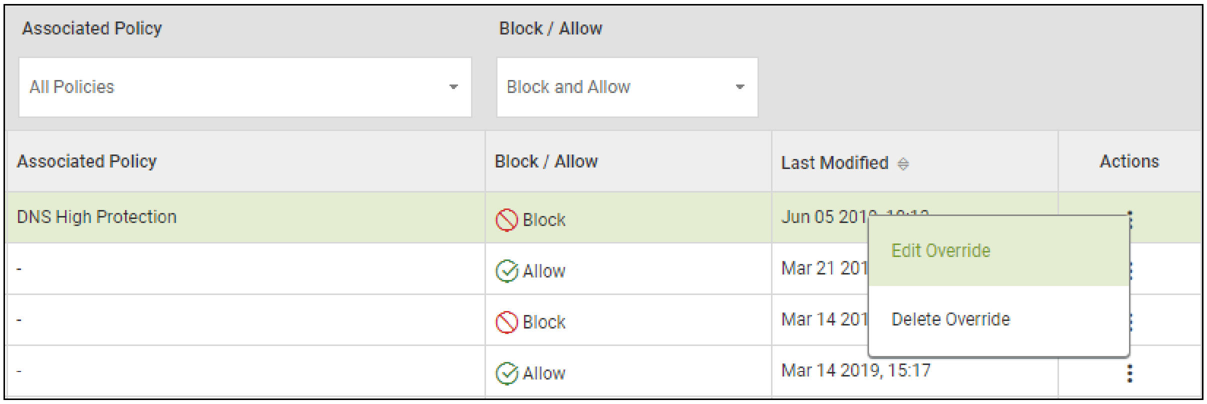


Filters (22/22 Overrides Shown)

Domain: Search for domains...
Scope: Global and Site
Associated Policy: All Policies
Block / Allow: Block and Allow

| Domain | Scope | Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|---|---|
| example.com | Global | DNS High Protection | Block | Jun 05 2019, 18:13 | ⋮ |
| test.com | Tract Industries | - | Allow | Mar 21 2019, 22:57 | ⋮ |
| *.facebook.com | Global | - | Block | Mar 14 2019, 15:53 | ⋮ |
| *.facebook.com | Apex Technology | - | Allow | Mar 14 2019, 15:17 | ⋮ |

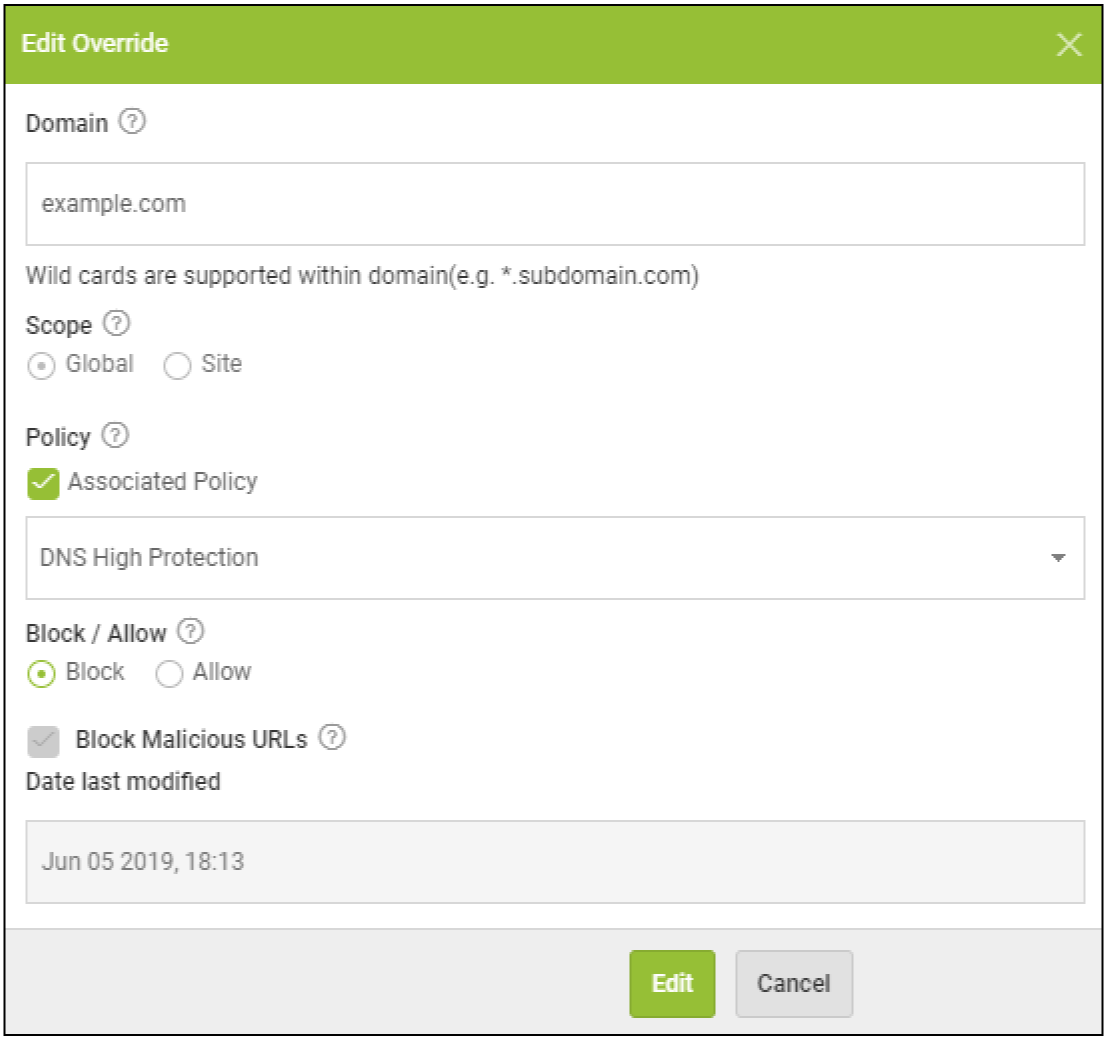
4. For the override you want to edit, in the Actions column, click the three ellipses, and select **Edit Override**.



Associated Policy: All Policies
Block / Allow: Block and Allow

| Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|
| DNS High Protection | Block | Jun 05 201 | ⋮ |
| - | Allow | Mar 21 201 | ⋮ |
| - | Block | Mar 14 201 | ⋮ |
| - | Allow | Mar 14 2019, 15:17 | ⋮ |

The Edit Override window displays.



Edit Override

Domain

example.com

Wild cards are supported within domain(e.g. *.subdomain.com)

Scope

● Global ○ Site

Policy

☑ Associated Policy

DNS High Protection

Block / Allow

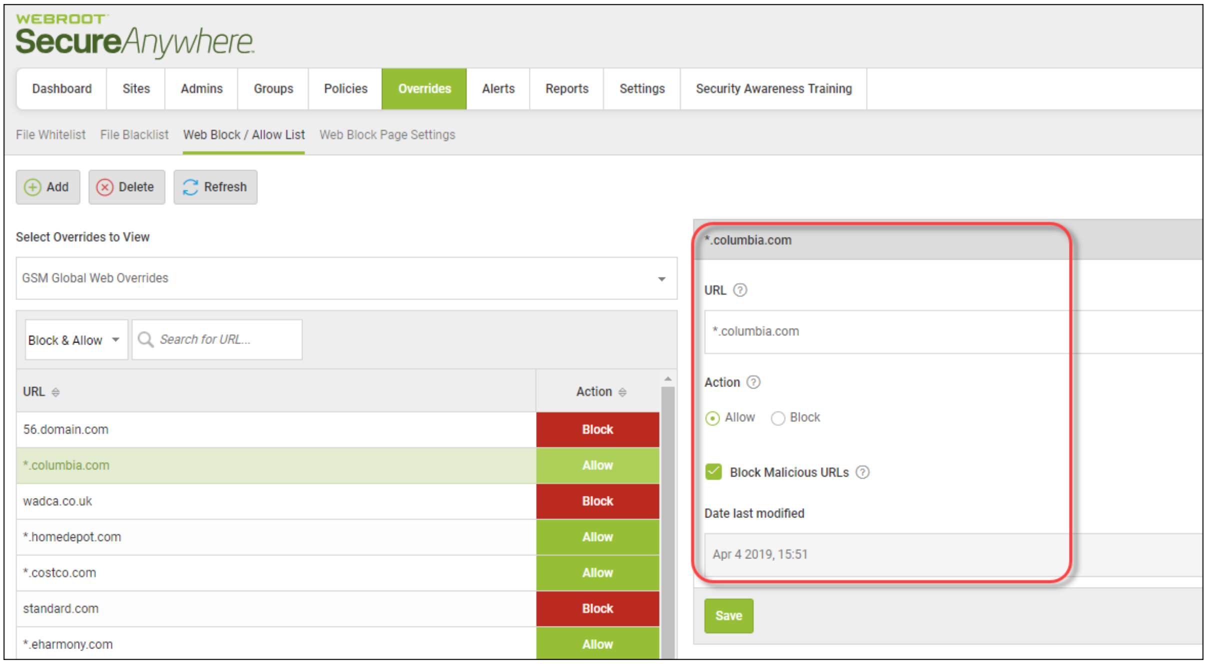
● Block ○ Allow

☑ Block Malicious URLs

Date last modified

Jun 05 2019, 18:13

5. Edit the fields, as needed.



Select Overrides to View

GSM Global Web Overrides

Block & Allow

| URL | Action |
|---|---|
| 56.domain.com | Block |
| *.columbia.com | Allow |
| wadca.co.uk | Block |
| *.homedepot.com | Allow |
| *.costco.com | Allow |
| standard.com | Block |
| *.eharmony.com | Allow |

*.columbia.com

URL

*.columbia.com

Action

● Allow ○ Block

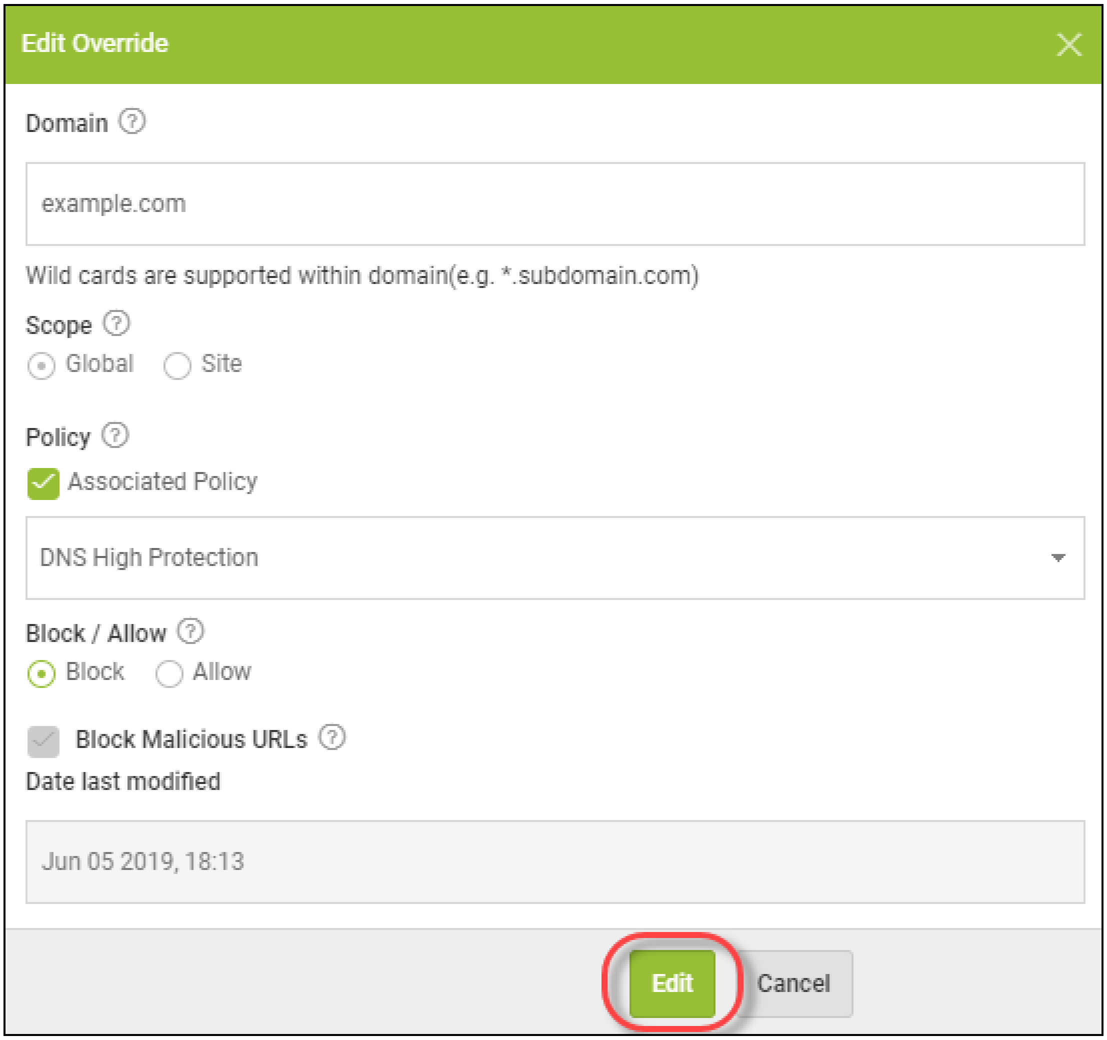
☑ Block Malicious URLs

Date last modified

Apr 4 2019, 15:51

**Note:** When you are entering the URL, you do not have to enter any protocols such as *www*, *http*, or *https*.

6. When you're done, click the **Edit** button.



Edit Override

Domain ⓘ

example.com

Wild cards are supported within domain(e.g. *.subdomain.com)

Scope ⓘ

● Global ○ Site

Policy ⓘ

☑ Associated Policy

DNS High Protection ▾

Block / Allow ⓘ

● Block ○ Allow

☑ Block Malicious URLs ⓘ

Date last modified

Jun 05 2019, 18:13

The system saves your updates.

# Importing Overrides

Under the overrides page at both management console and Site level, you can now import overrides from existing sites. This procedure is useful for administrators who wish to copy identical overrides from one site to another, instead of manually having to create the same override for each site.

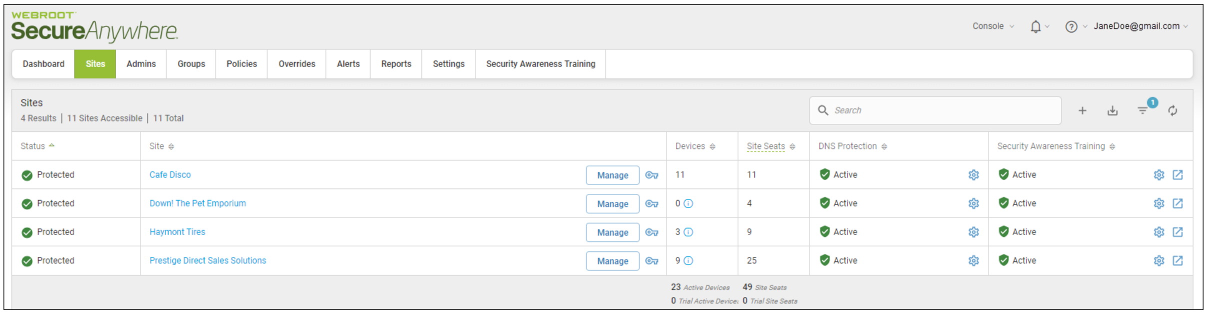
For Super Admins, this also means they can pull up overrides from a site, to then make global, and apply to all other sites which have the global overrides option selected.

Follow this procedure to import either whitelist or blacklist overrides.

### To import an override:

1. Log in to the management console.

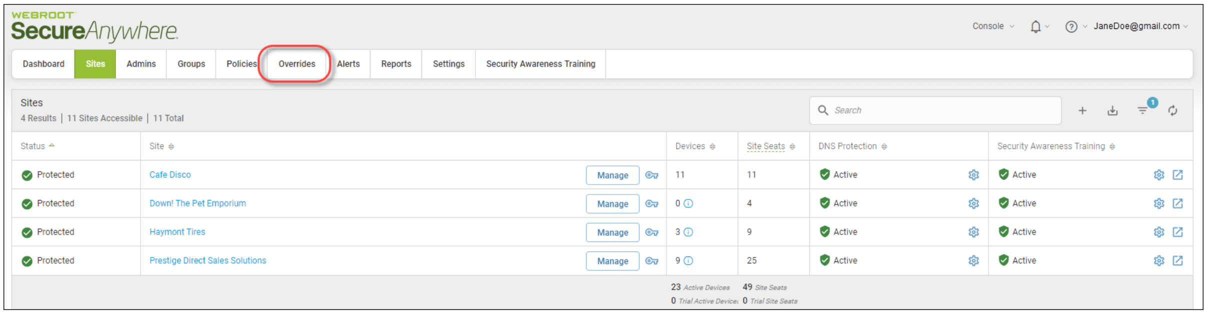
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

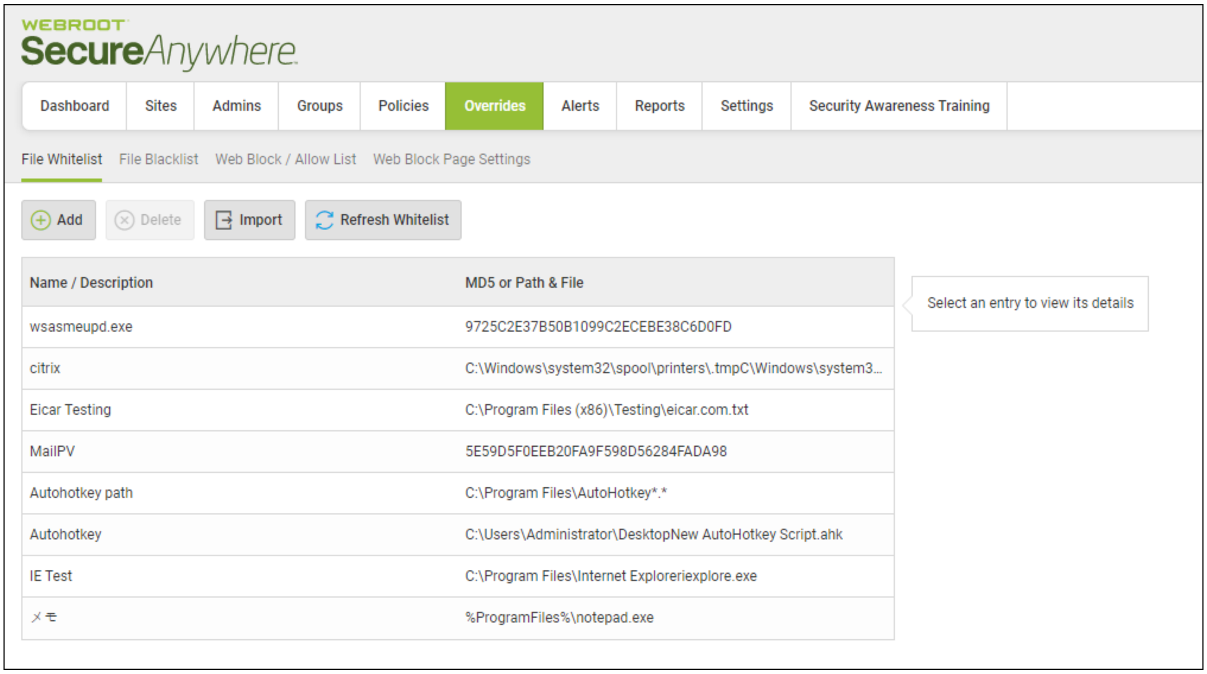
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

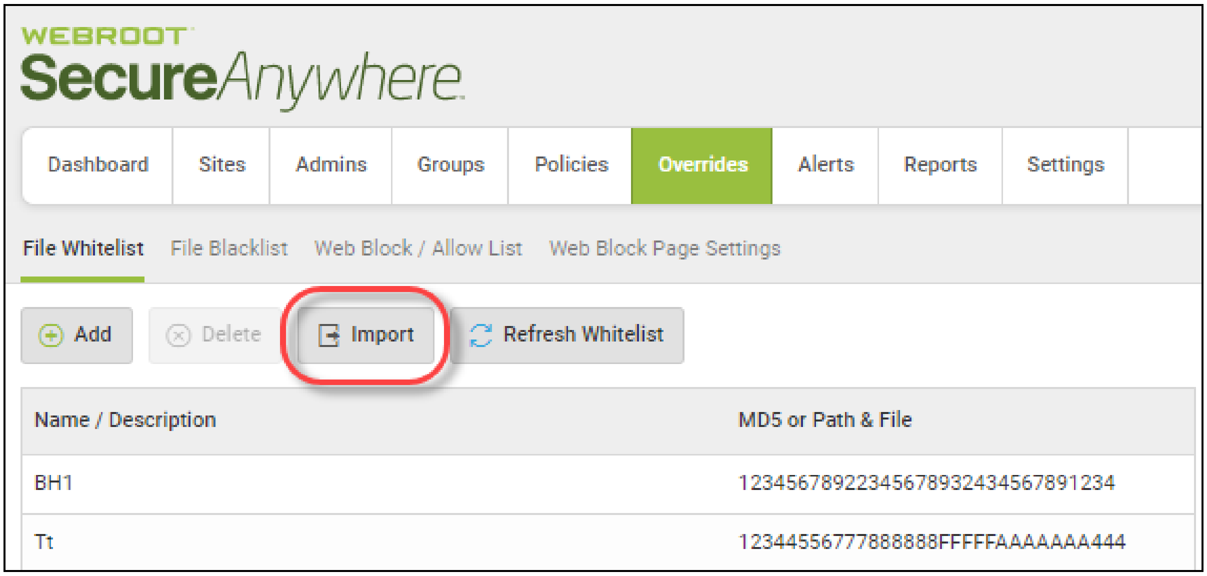
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Overrides tab displays, with the File Whitelist tab active.



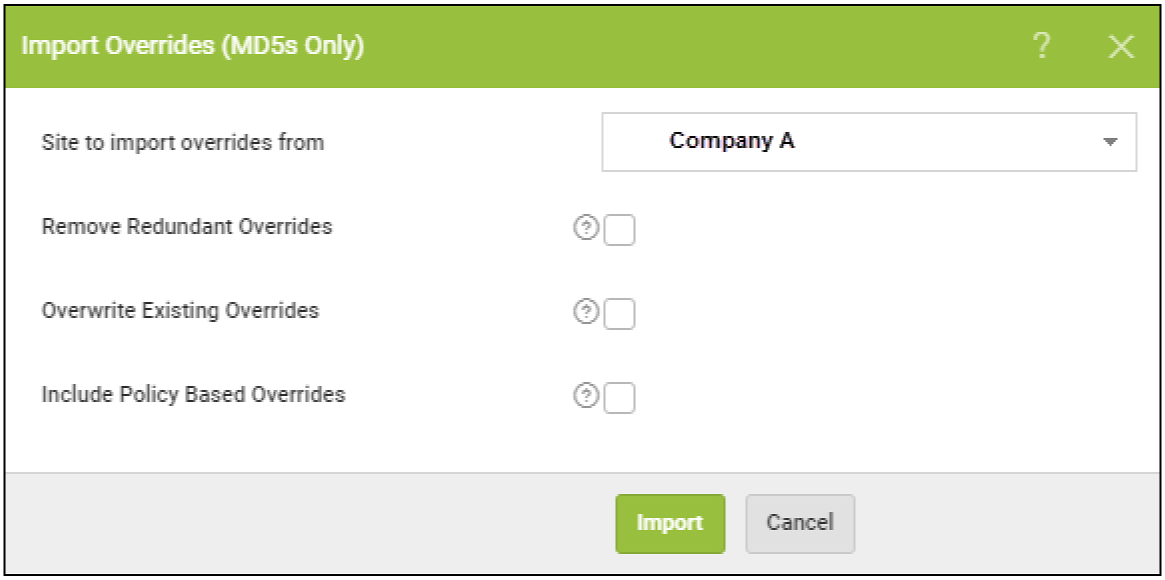
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. Click the **Import** button.



| Name / Description | MD5 or Path & File |
|---|---|
| BH1 | 12345678922345678932434567891234 |
| Tt | 12344556777888888FFFFFAAAAAAA444 |

The Import Overrides window displays.



Import Overrides (MD5s Only)

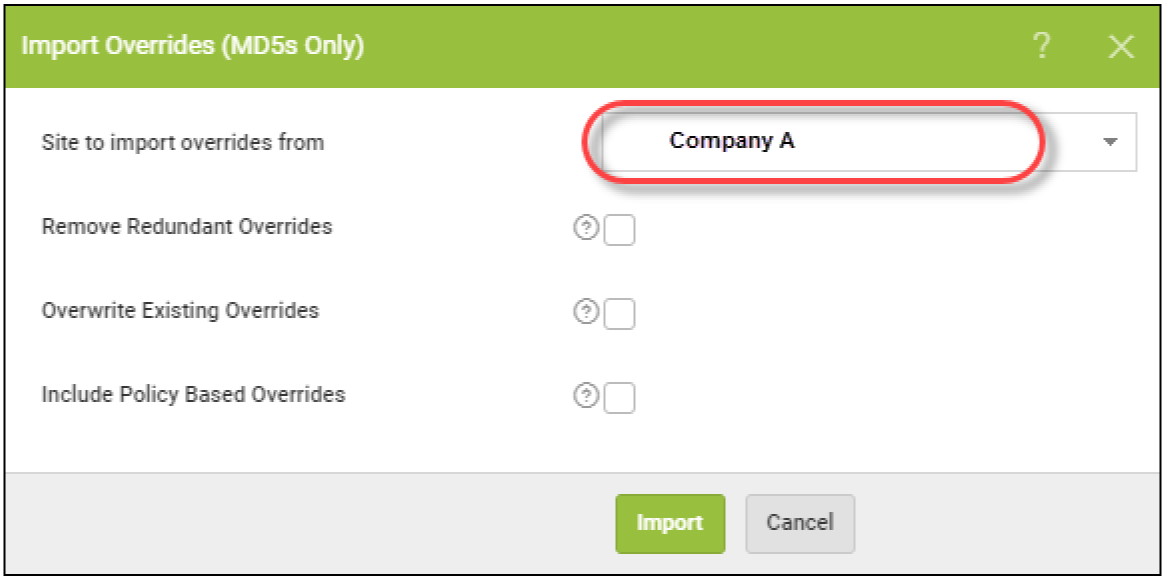
Site to import overrides from: Company A

Remove Redundant Overrides □

Overwrite Existing Overrides □

Include Policy Based Overrides □

4. From the Site to import overrides from drop-down menu, select the site from where you want to import overrides.



Import Overrides (MD5s Only)

Site to import overrides from: Company A

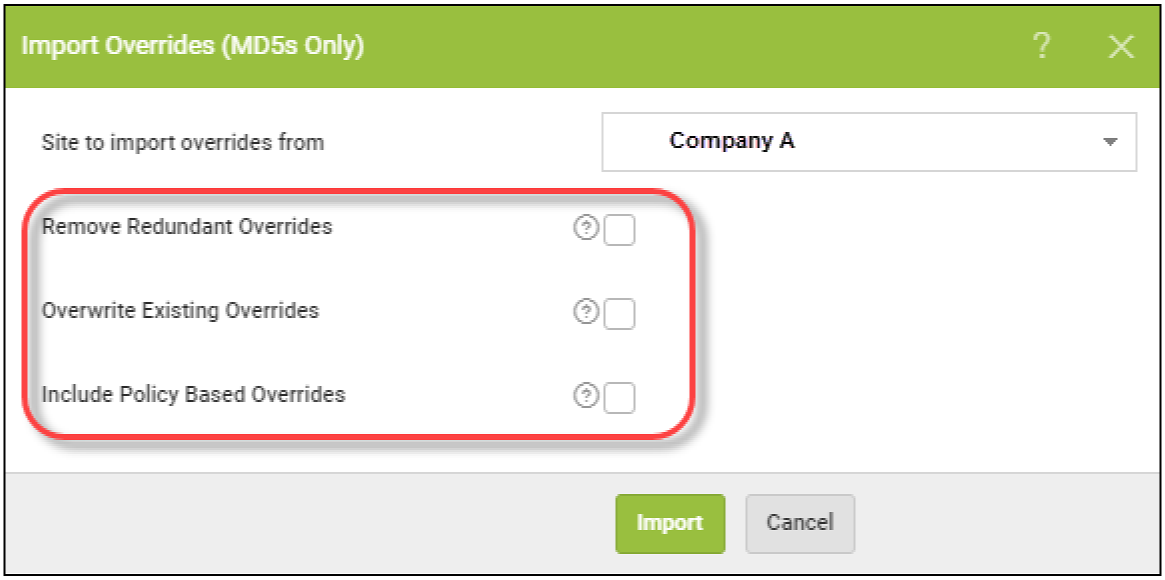
Remove Redundant Overrides □

Overwrite Existing Overrides □

Include Policy Based Overrides □

5. Based on your needs, select any of the following checkboxes:
   - **Remove Redundant Overrides** — Selecting this checkbox will not import overrides where the override matches the file determination, for example, a Whitelist entry for an MD5 which already has a determination of Good.

- **Overwrite Existing Overrides** — Selecting this checkbox determines whether any duplicate overrides within the imported list should override those already present.
- **Include Policy Based Overrides** — Allows the importation of overrides created in the Standard Console that were assigned only to a particular policy within the selected import site/console. Note that ability to assign overrides to a policy is a feature only available in the Standard Console.



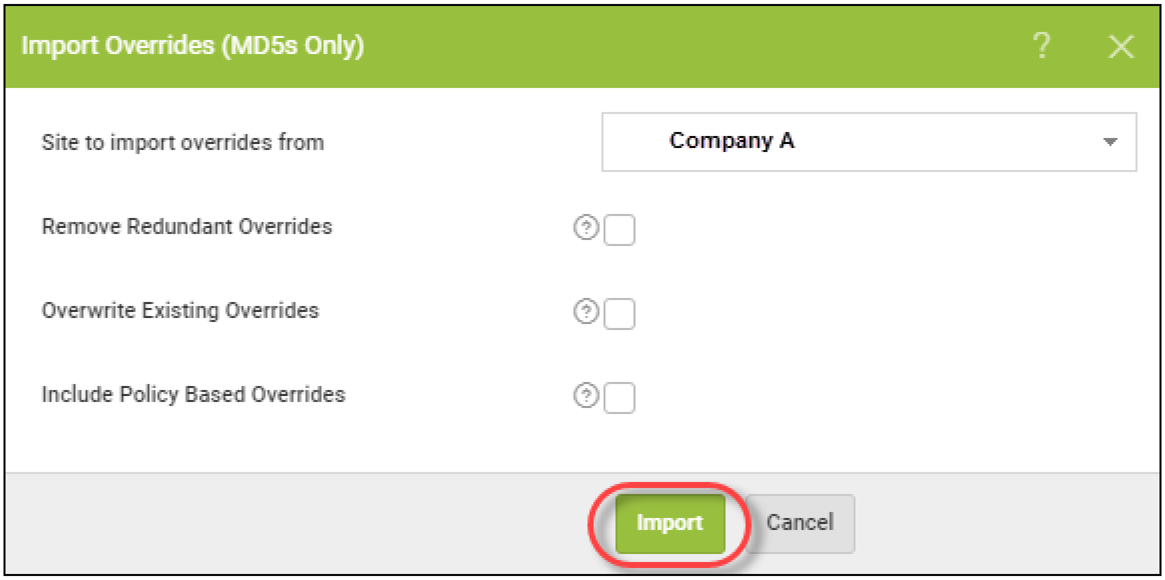
Site to import overrides from: Company A

Remove Redundant Overrides □

Overwrite Existing Overrides □

Include Policy Based Overrides □

6. When you’re done, click the **Import** button.



Site to import overrides from: Company A

Remove Redundant Overrides □

Overwrite Existing Overrides □

Include Policy Based Overrides □

The system imports all overrides from that site into your currently selected site.

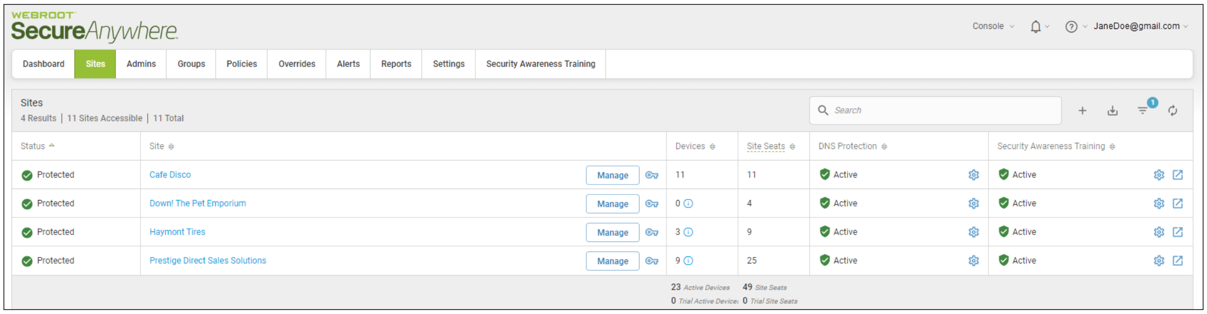
# Viewing Web Overrides

Follow this procedure to view additional information bout any of the web overrides that you've created.

**To view a web override:**

1. Log in to the management console.

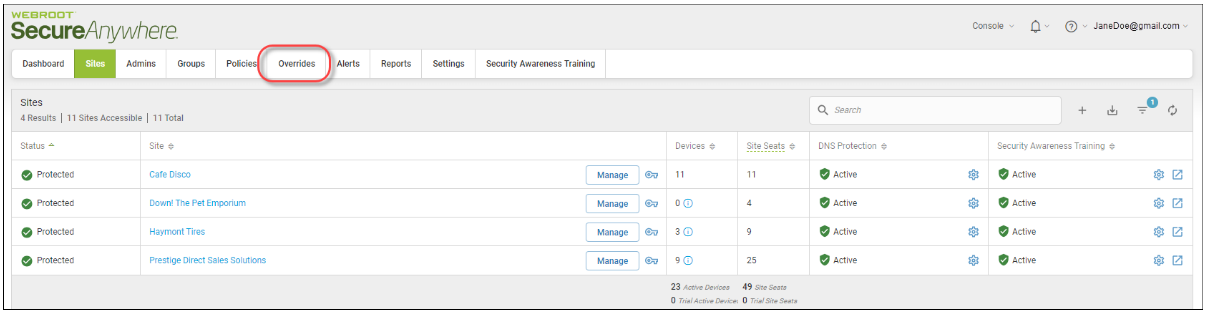
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| ✓ Protected | Cafe Disco | Manage | 11 | 11 | ✓ Active | ✓ Active |
| ✓ Protected | Down! The Pet Emporium | Manage | 0 ⓘ | 4 | ✓ Active | ✓ Active |
| ✓ Protected | Haymont Tires | Manage | 3 ⓘ | 9 | ✓ Active | ✓ Active |
| ✓ Protected | Prestige Direct Sales Solutions | Manage | 9 ⓘ | 25 | ✓ Active | ✓ Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

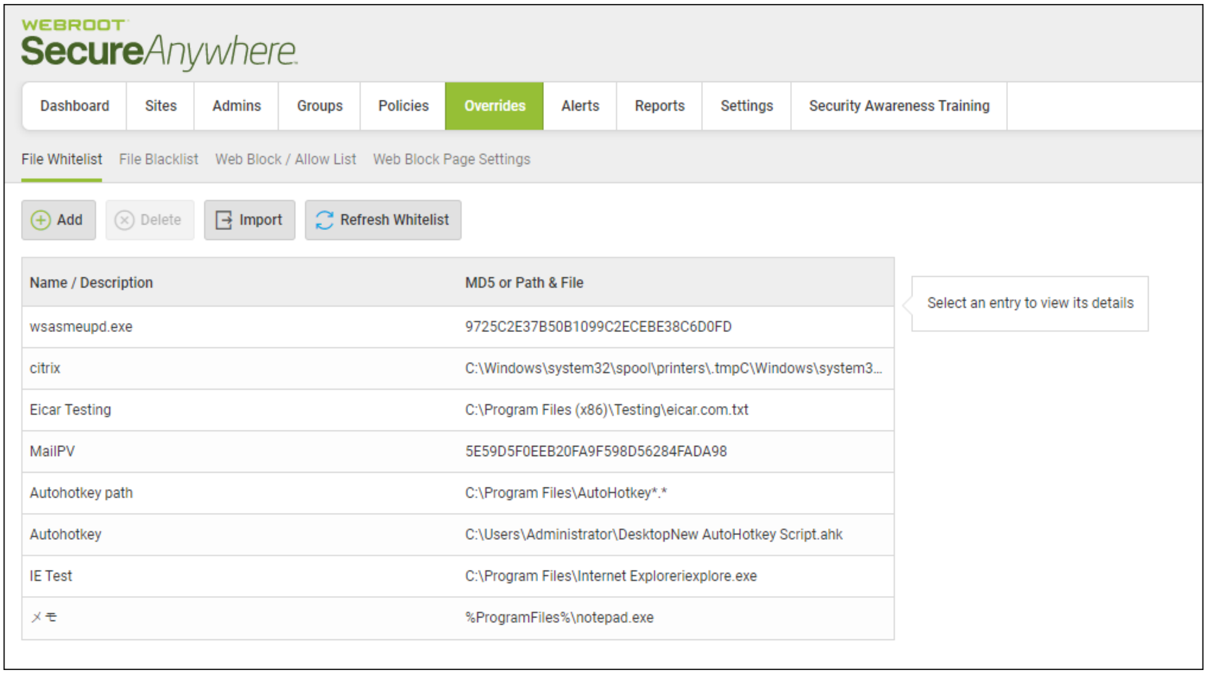
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

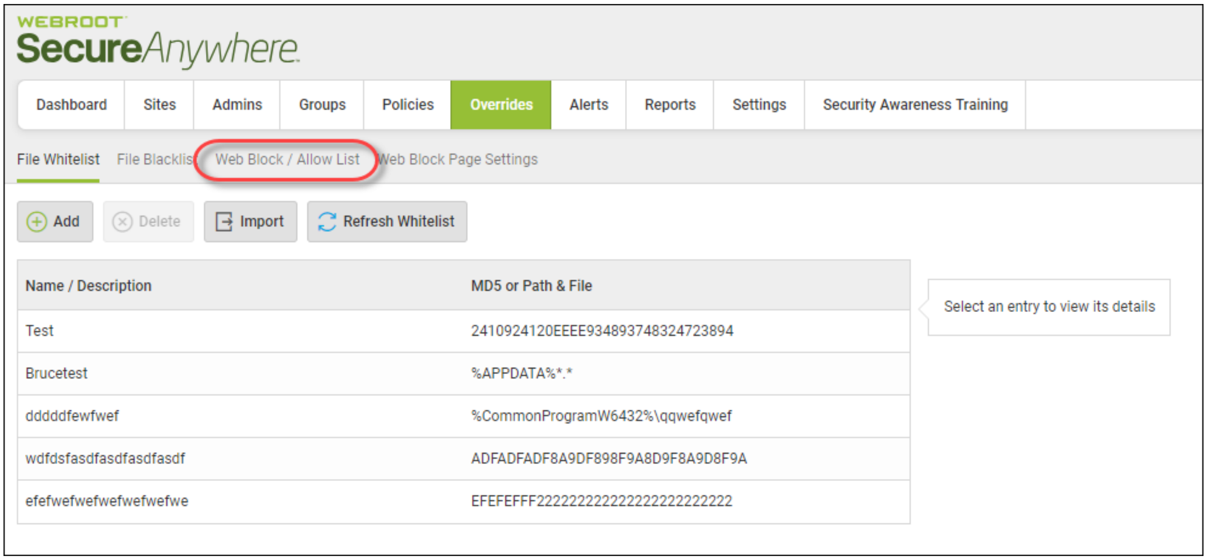
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| ✓ Protected | Cafe Disco | Manage | 11 | 11 | ✓ Active | ✓ Active |
| ✓ Protected | Down! The Pet Emporium | Manage | 0 ⓘ | 4 | ✓ Active | ✓ Active |
| ✓ Protected | Haymont Tires | Manage | 3 ⓘ | 9 | ✓ Active | ✓ Active |
| ✓ Protected | Prestige Direct Sales Solutions | Manage | 9 ⓘ | 25 | ✓ Active | ✓ Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Overrides tab displays, with the File Whitelist tab active.



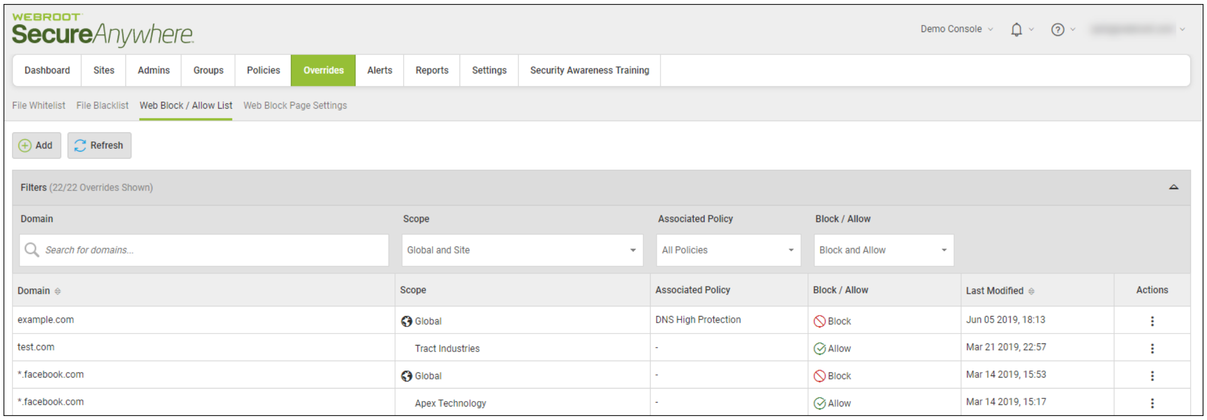
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3… |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. Click the **Web Block / Allow List** tab.



| Name / Description | MD5 or Path & File |
|---|---|
| Test | 2410924120EEEE934893748324723894 |
| Brucetest | %APPDATA%*.* |
| dddddfewfwef | %CommonProgramW6432%\qqwefqwef |
| wdfdsfasdfasdfasdfasdf | ADFADFADF8A9DF898F9A8D9F8A9D8F9A |
| efefwefwefwefwefwefwe | EFEFEFFF2222222222222222222222 |

The Web Block / Allow List tab displays.



Filters (22/22 Overrides Shown)

Domain: Search for domains...

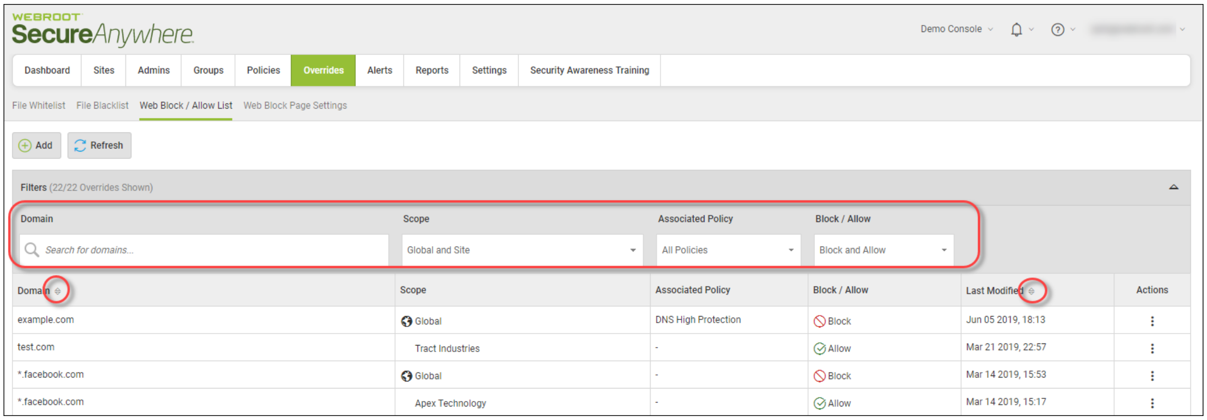
Scope: Global and Site

Associated Policy: All Policies

Block / Allow: Block and Allow

| Domain | Scope | Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|---|---|
| example.com | Global | DNS High Protection | Block | Jun 05 2019, 18:13 | ⋮ |
| test.com | Tract Industries | - | Allow | Mar 21 2019, 22:57 | ⋮ |
| *.facebook.com | Global | - | Block | Mar 14 2019, 15:53 | ⋮ |
| *.facebook.com | Apex Technology | - | Allow | Mar 14 2019, 15:17 | ⋮ |

4. Do any of the following to locate a specific override or to sort on overrides based on scope, associated policy, or block/allow status:
   - In the Domain field, enter the name of a domain you want to find.
   - From the Scope drop-down menu, select a policy based on its scope. For example, if you want to filter on only Global polices, select *Global*.
   - From the Associated Policy drop-down menu, select a domain based on the policy it's associated with.
   - From the Block/Allow drop-down menu, you can filter on any of the following:
     - Block and Allow
     - Block
     - Allow
   - Additionally, you can filter the following columns by clicking the Up or Down arrow at the top of the column:
     - **Domain** — Filters alphabetically.
     - **Last Modified** — Filters by date.



Filters (22/22 Overrides Shown)

| Domain | Scope | Associated Policy | Block / Allow |
|---|---|---|---|
| Search for domains... | Global and Site | All Policies | Block and Allow |

| Domain | Scope | Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|---|---|
| example.com | Global | DNS High Protection | Block | Jun 05 2019, 18:13 | ⋮ |
| test.com | Tract Industries | - | Allow | Mar 21 2019, 22:57 | ⋮ |
| *.facebook.com | Global | - | Block | Mar 14 2019, 15:53 | ⋮ |
| *.facebook.com | Apex Technology | - | Allow | Mar 14 2019, 15:17 | ⋮ |

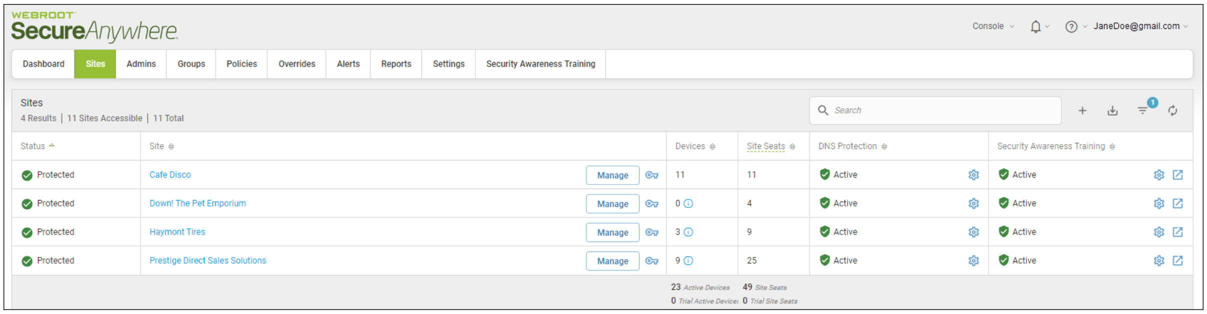
# Deleting Overrides

Follow this procedure to delete either whitelist or blacklist overrides.

### To delete an override:

1. Log in to the management console.

   The management console displays, with the Sites tab active.



WEBROOT SecureAnywhere

Console | JaneDoe@gmail.com

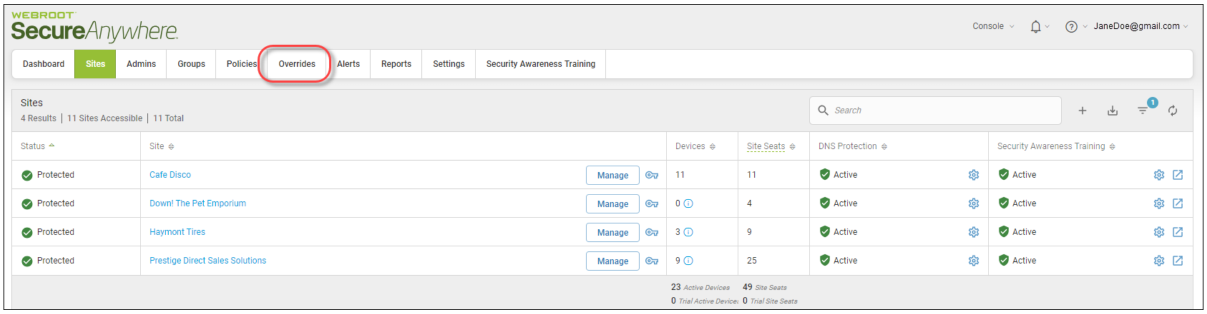
Dashboard | Sites | Admins | Groups | Policies | Overrides | Alerts | Reports | Settings | Security Awareness Training

Sites
4 Results | 11 Sites Accessible | 11 Total

Search

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

2. Click the **Overrides** tab.



WEBROOT SecureAnywhere

Console | JaneDoe@gmail.com

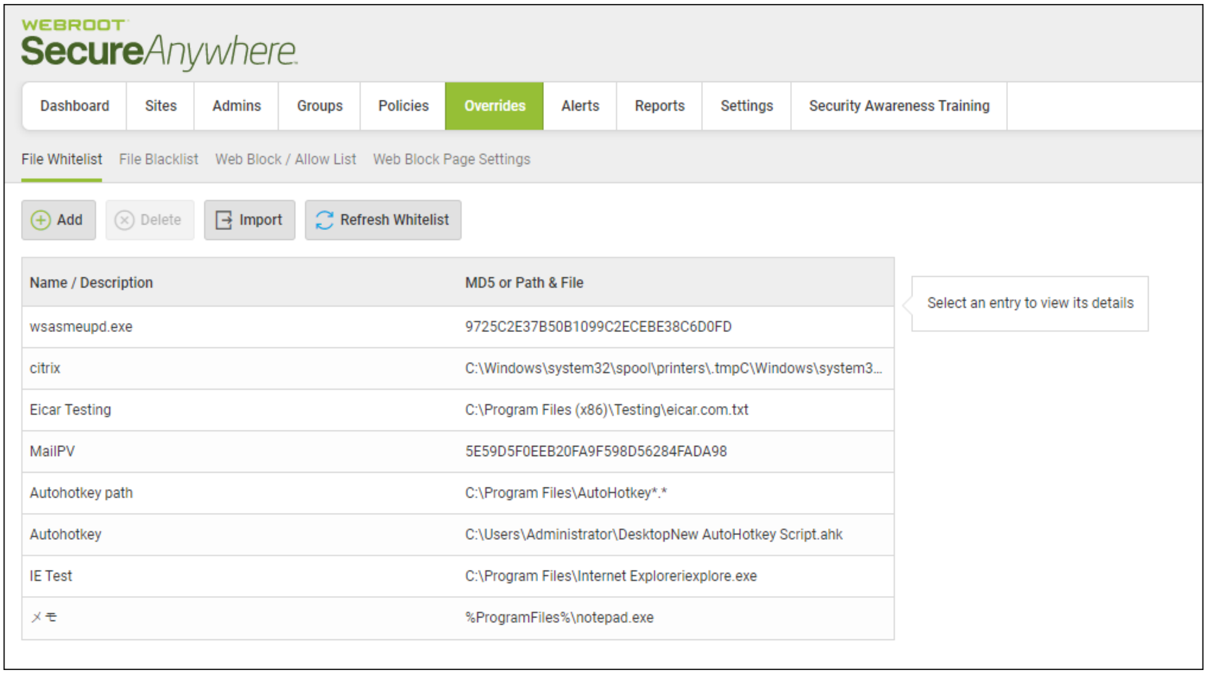
Dashboard | Sites | Admins | Groups | Policies | Overrides | Alerts | Reports | Settings | Security Awareness Training

Sites
4 Results | 11 Sites Accessible | 11 Total

Search

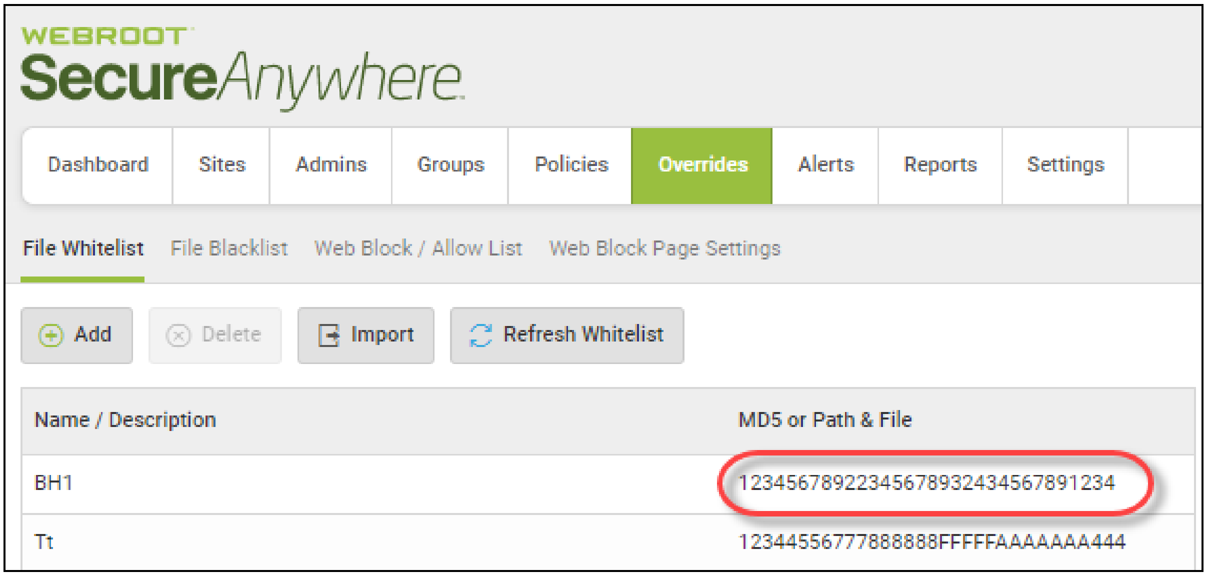
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The Overrides tab displays, with the File Whitelist tab active.



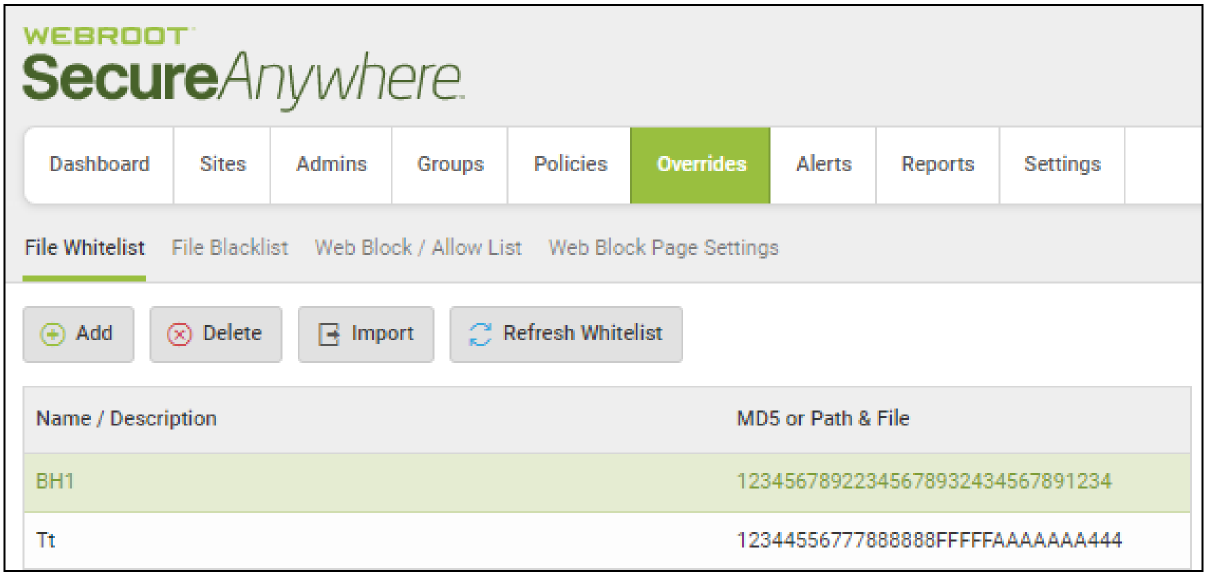
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. On either the Whitelist or the Blacklist tab, highlight the override that you want to delete.



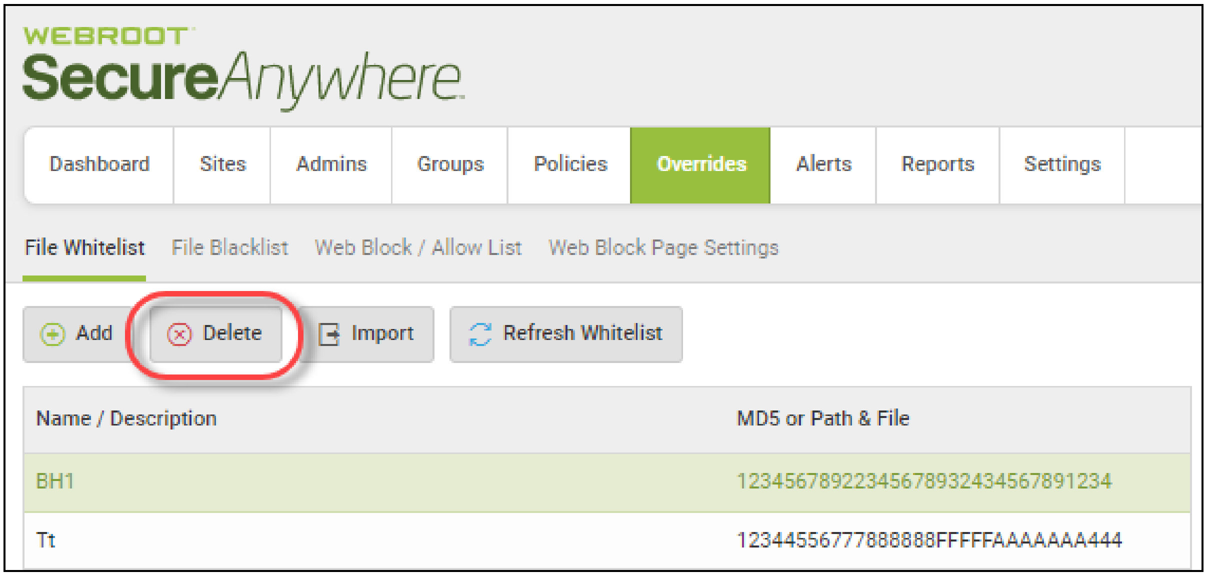
| Name / Description | MD5 or Path & File |
|---|---|
| BH1 | 12345678922345678932434567891234 |
| Tt | 12344556777888888FFFFFAAAAAAAA444 |

The override you selected is highlighted, and the Delete button becomes active.



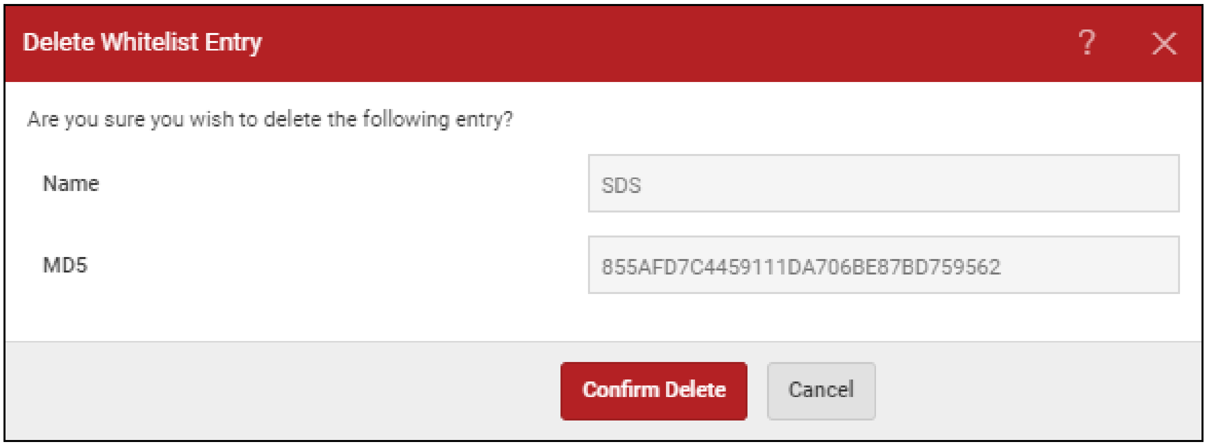
| Name / Description | MD5 or Path & File |
|---|---|
| BH1 | 12345678922345678932434567891234 |
| Tt | 12344556777888888FFFFFAAAAAAAA444 |

4. Click the **Delete** button.



| Name / Description | MD5 or Path & File |
|---|---|
| BH1 | 12345678922345678932434567891234 |
| Tt | 12344556777888888FFFFFAAAAAAAA444 |

The system displays the Delete Whitelist/Blacklist Entry confirmation window.

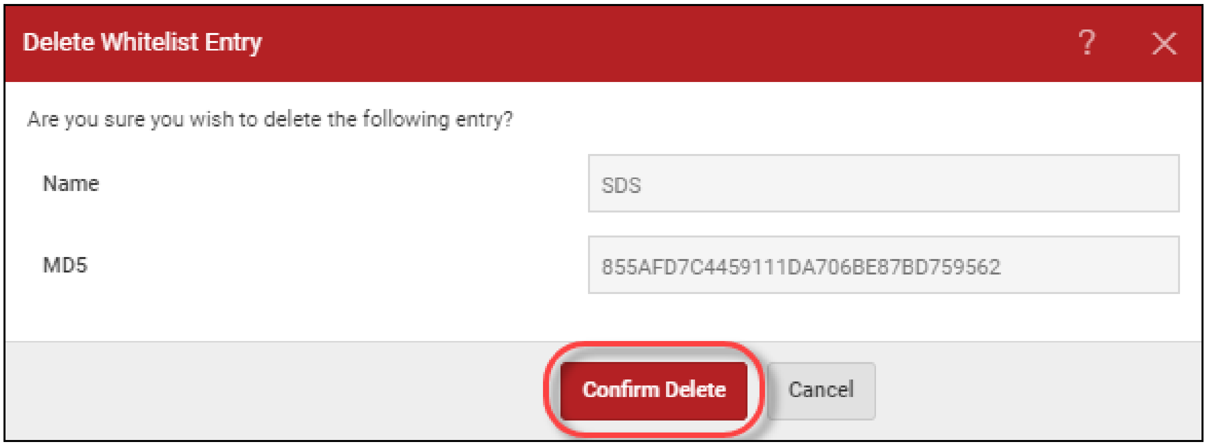


Are you sure you wish to delete the following entry?

Name: SDS

MD5: 855AFD7C4459111DA706BE87BD759562

5. Click the **Confirm Delete** button.



Are you sure you wish to delete the following entry?

Name: SDS

MD5: 855AFD7C4459111DA706BE87BD759562

The system deletes the override.

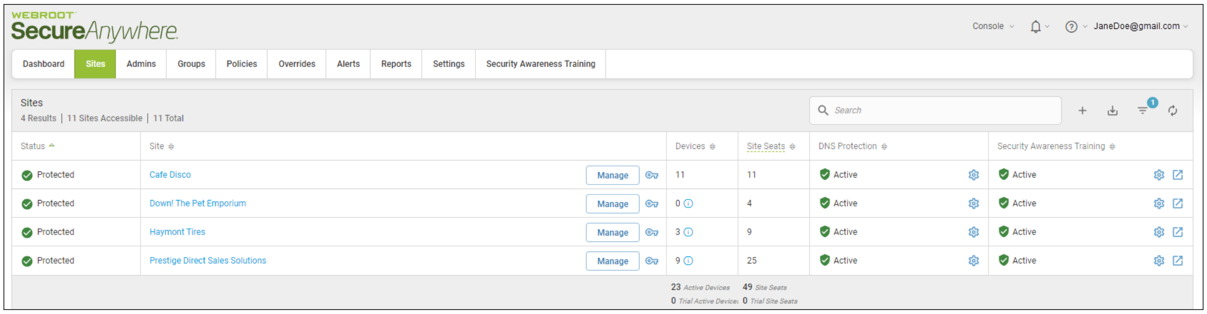
# Deleting Web Overrides

Follow this procedure to delete web overrides that you no longer need.

### To delete a web override:

1. Log in to the management console.

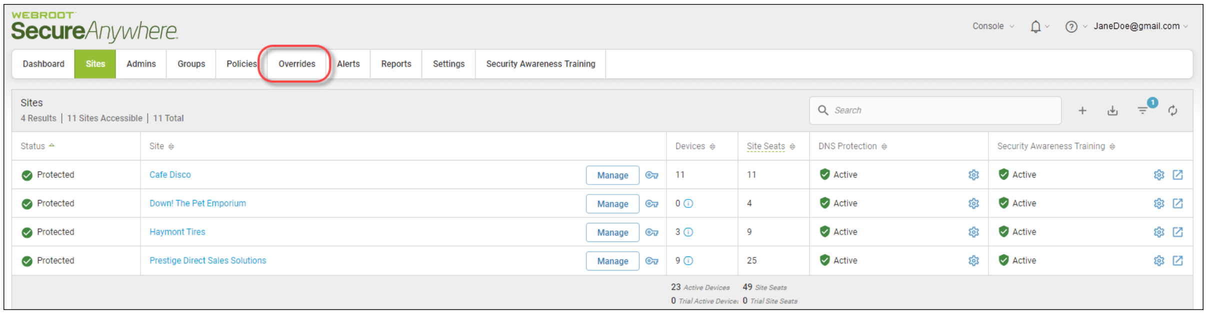
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

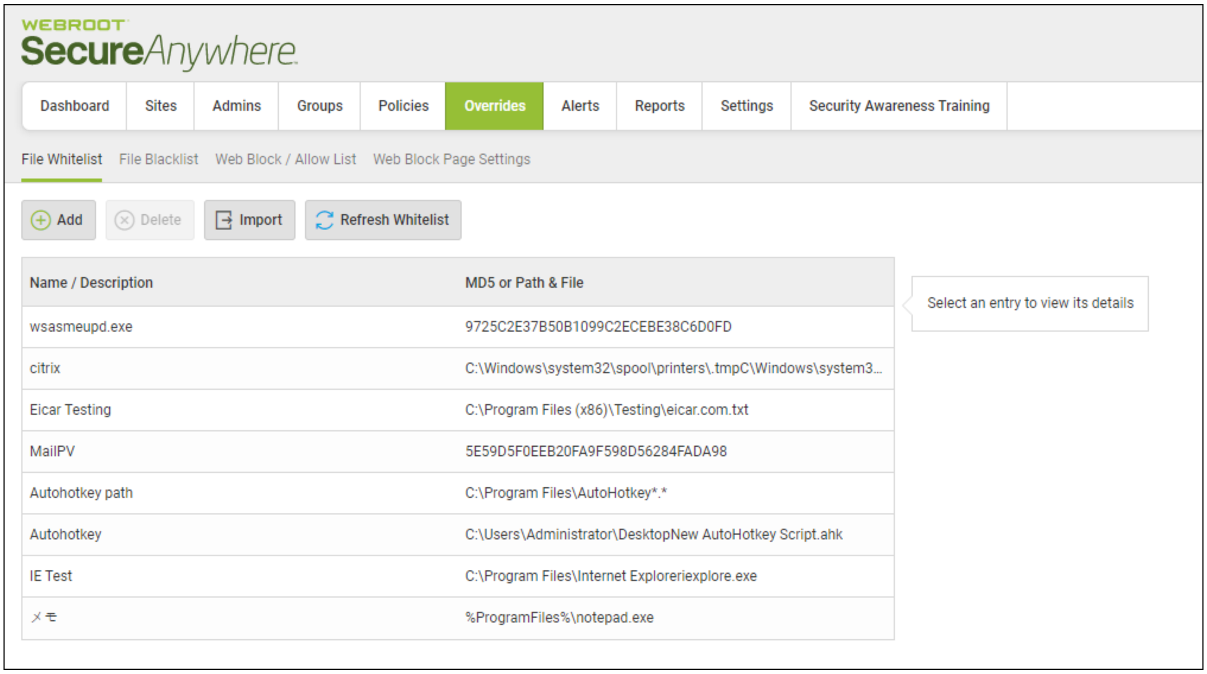
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

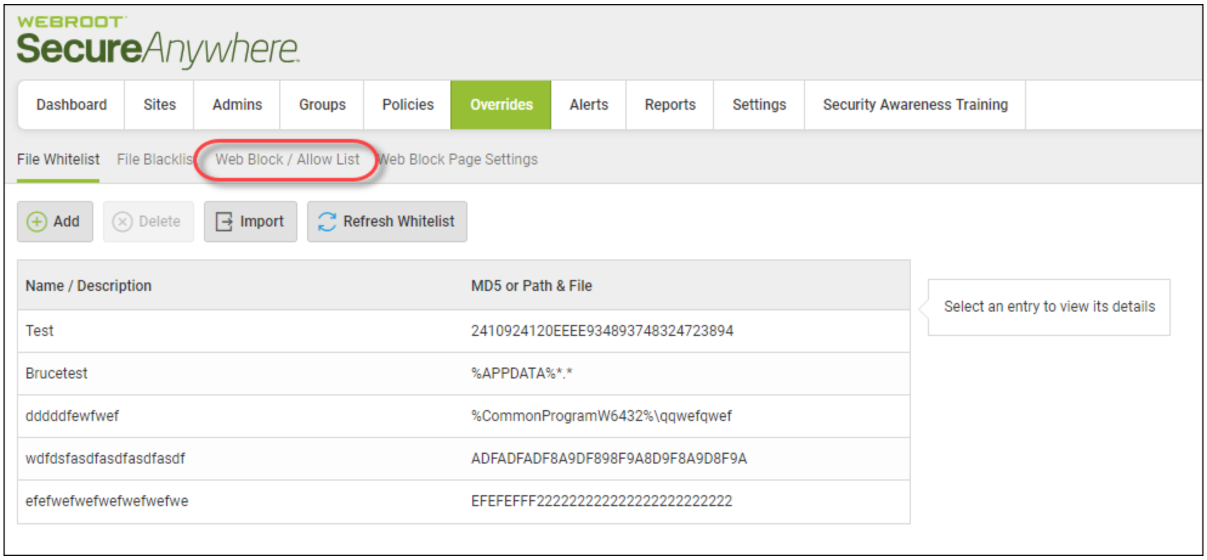
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Overrides tab displays, with the File Whitelist tab active.



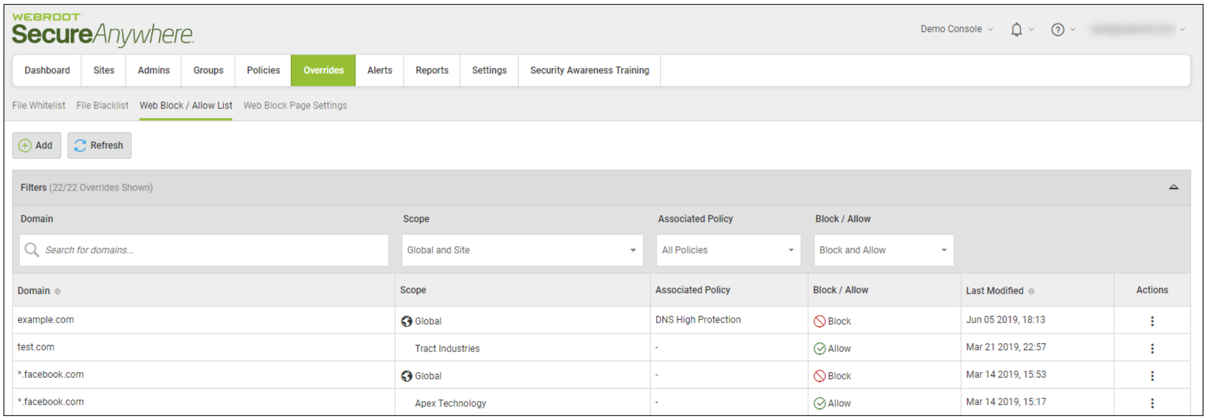
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. Click the **Web Block / Allow List** tab.



| Name / Description | MD5 or Path & File |
|---|---|
| Test | 2410924120EEEE934893748324723894 |
| Brucetest | %APPDATA%*.* |
| dddddfewfwef | %CommonProgramW6432%\qqwefqwef |
| wdfdsfasdfasdfasdfasdf | ADFADFADF8A9DF898F9A8D9F8A9D8F9A |
| efefwefwefwefwefwefwe | EFEFEFFF222222222222222222222222 |

The Web Overrides tab displays with the Allow List tab active.

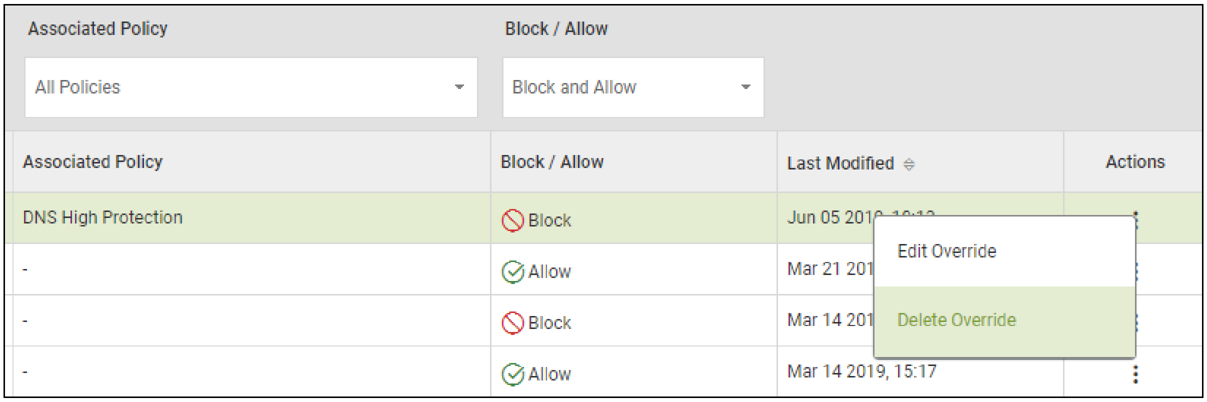


Filters (22/22 Overrides Shown)

| Domain | Scope | Associated Policy | Block / Allow |
|---|---|---|---|
| Search for domains... | Global and Site | All Policies | Block and Allow |

| Domain | Scope | Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|---|---|
| example.com | Global | DNS High Protection | Block | Jun 05 2019, 18:13 | ⋮ |
| test.com | Tract Industries | - | Allow | Mar 21 2019, 22:57 | ⋮ |
| *.facebook.com | Global | - | Block | Mar 14 2019, 15:53 | ⋮ |
| *.facebook.com | Apex Technology | - | Allow | Mar 14 2019, 15:17 | ⋮ |

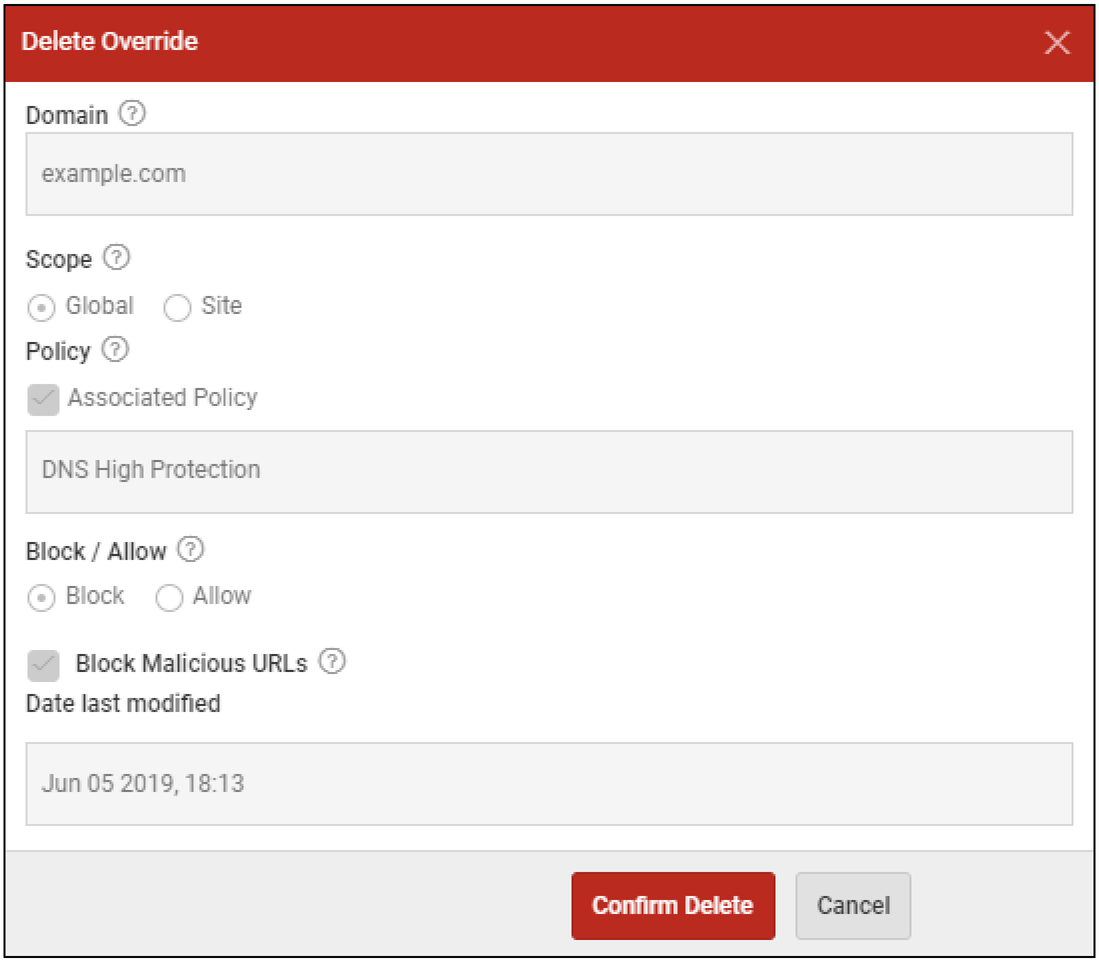
4. For the web override you want to delete, in the Actions column, click the three ellipses and select **Delete**.



| Associated Policy | Block / Allow |
|---|---|
| All Policies | Block and Allow |

| Associated Policy | Block / Allow | Last Modified | Actions |
|---|---|---|---|
| DNS High Protection | Block | Jun 05 201 | ⋮ |
| - | Allow | Mar 21 201 | ⋮ |
| - | Block | Mar 14 201 | ⋮ |
| - | Allow | Mar 14 2019, 15:17 | ⋮ |

The Delete window displays with the URL for the web override that you selected.



Delete Override

Domain

example.com

Scope

● Global ○ Site

Policy

☑ Associated Policy

DNS High Protection

Block / Allow

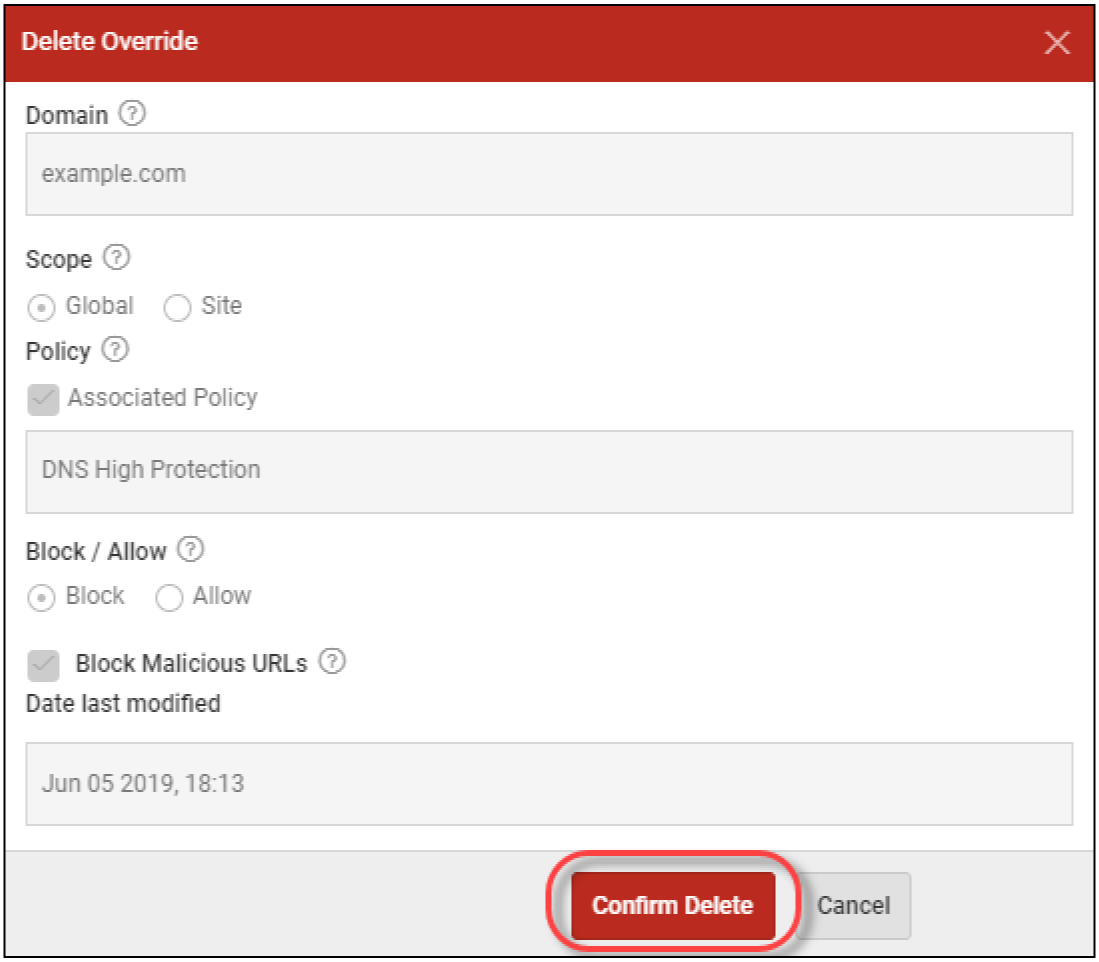
● Block ○ Allow

☑ Block Malicious URLs

Date last modified

Jun 05 2019, 18:13

5. Click the **Confirm Delete** button.



Delete Override

Domain

example.com

Scope

● Global ○ Site

Policy

☑ Associated Policy

DNS High Protection

Block / Allow

● Block ○ Allow

☑ Block Malicious URLs

Date last modified

Jun 05 2019, 18:13

The system deletes the web override.

# Customizing Block Pages

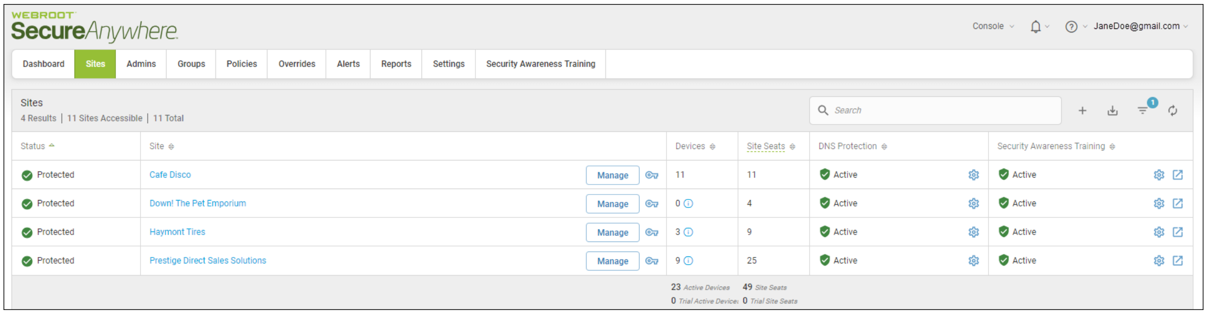
The Block Page can be customized for each management console, which allows admins to notify users with more information.

- Admins can include company-based logos.
- 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.

**To customize a block page:**

1. Log in to the [management console](management console).

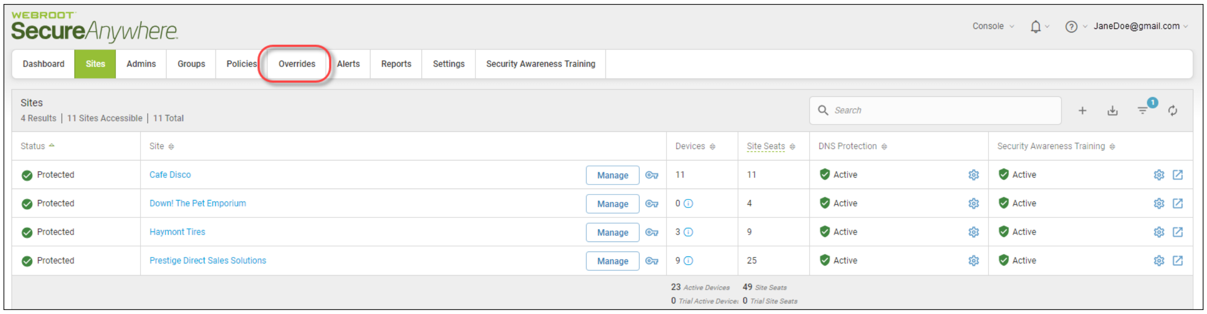
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

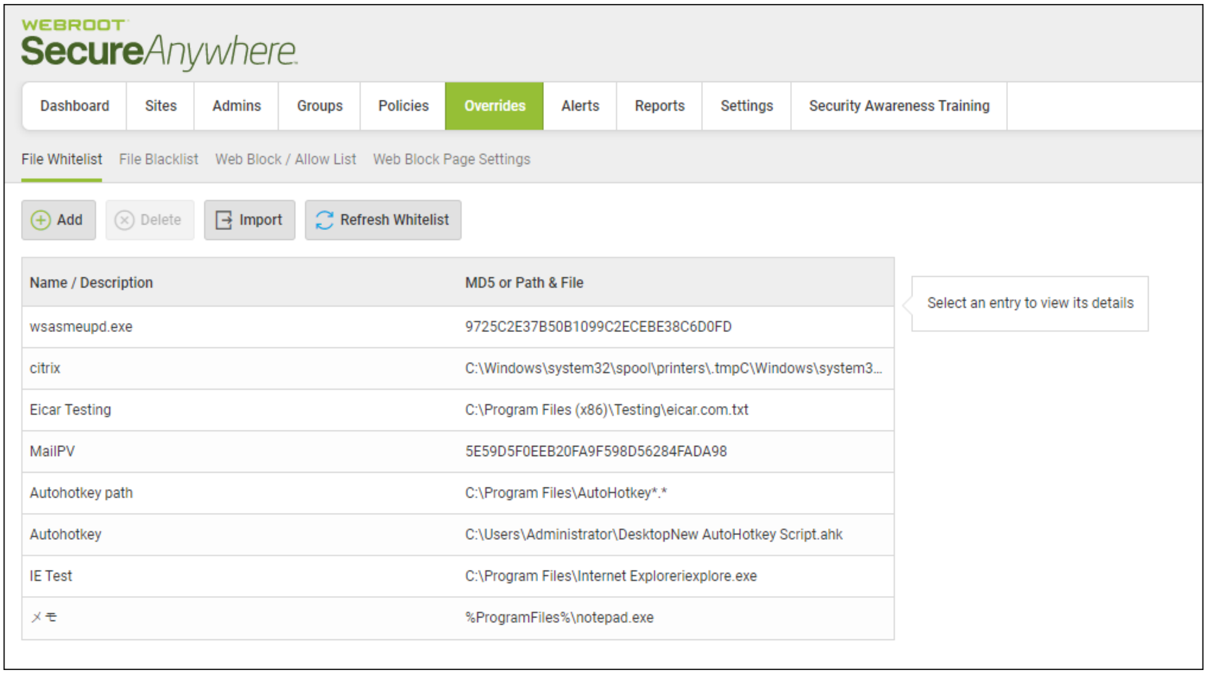
2. Click the **Overrides** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

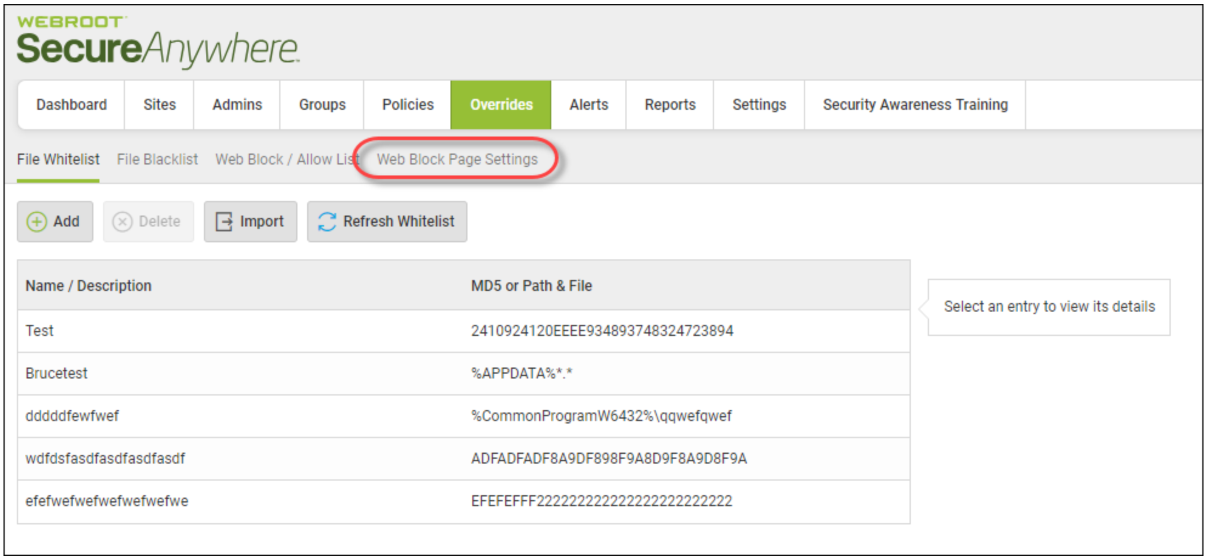
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

   The Overrides tab displays, with the File Whitelist tab active.



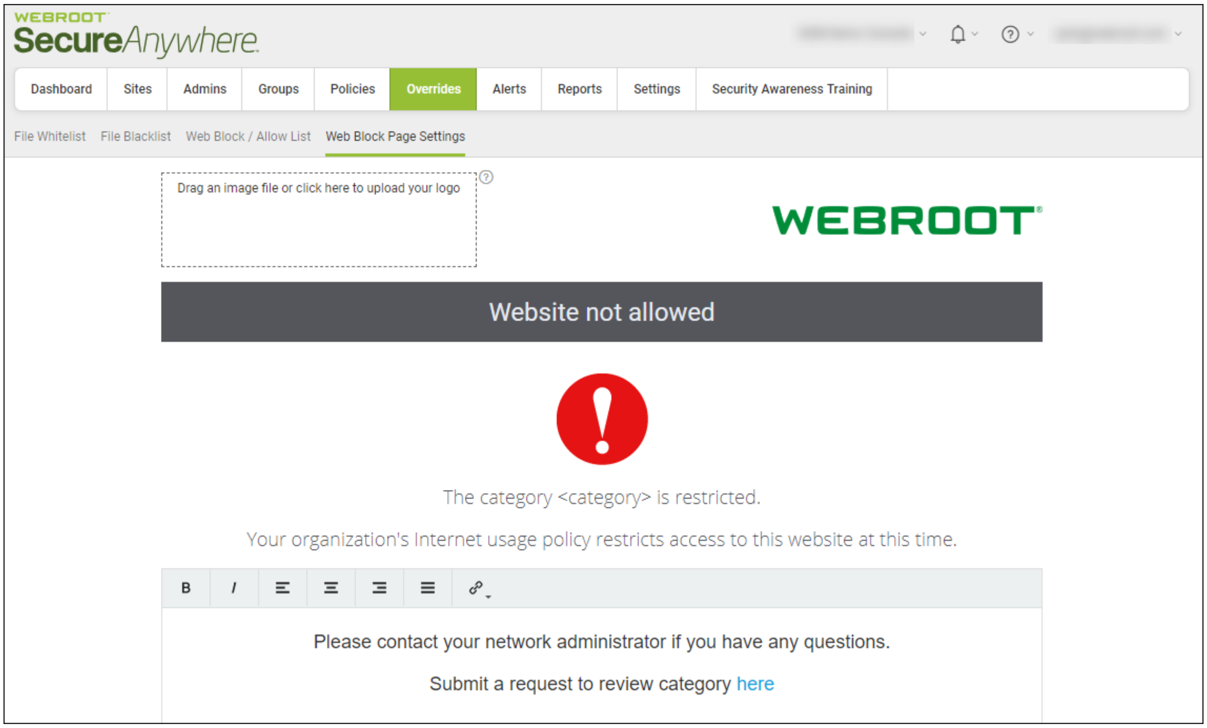
| Name / Description | MD5 or Path & File |
|---|---|
| wsasmeupd.exe | 9725C2E37B50B1099C2ECEBE38C6D0FD |
| citrix | C:\Windows\system32\spool\printers\.tmpC\Windows\system3... |
| Eicar Testing | C:\Program Files (x86)\Testing\eicar.com.txt |
| MailPV | 5E59D5F0EEB20FA9F598D56284FADA98 |
| Autohotkey path | C:\Program Files\AutoHotkey*.* |
| Autohotkey | C:\Users\Administrator\DesktopNew AutoHotkey Script.ahk |
| IE Test | C:\Program Files\Internet Exploreriexplore.exe |
| メモ | %ProgramFiles%\notepad.exe |

3. Click the **Web Block Page Settings** tab.



| Name / Description | MD5 or Path & File |
|---|---|
| Test | 2410924120EEEE934893748324723894 |
| Brucetest | %APPDATA%*.* |
| dddddfewfwef | %CommonProgramW6432%\qqwefqwef |
| wdfdsfasdfasdfasdfasdf | ADFADFADF8A9DF898F9A8D9F8A9D8F9A |
| efefwefwefwefwefwefwe | EFEFEFFF2222222222222222222222 |

The Web Block Page Settings tab displays.



Website not allowed

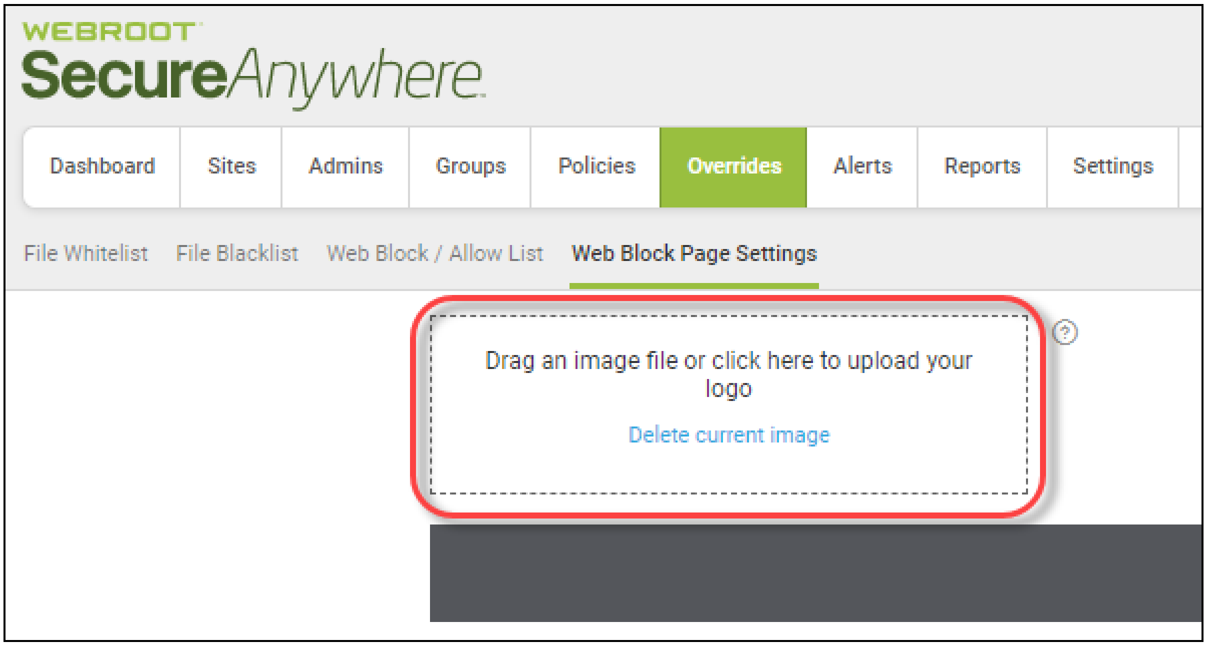
The category <category> is restricted.

Your organization's Internet usage policy restricts access to this website at this time.

Please contact your network administrator if you have any questions.

Submit a request to review category here

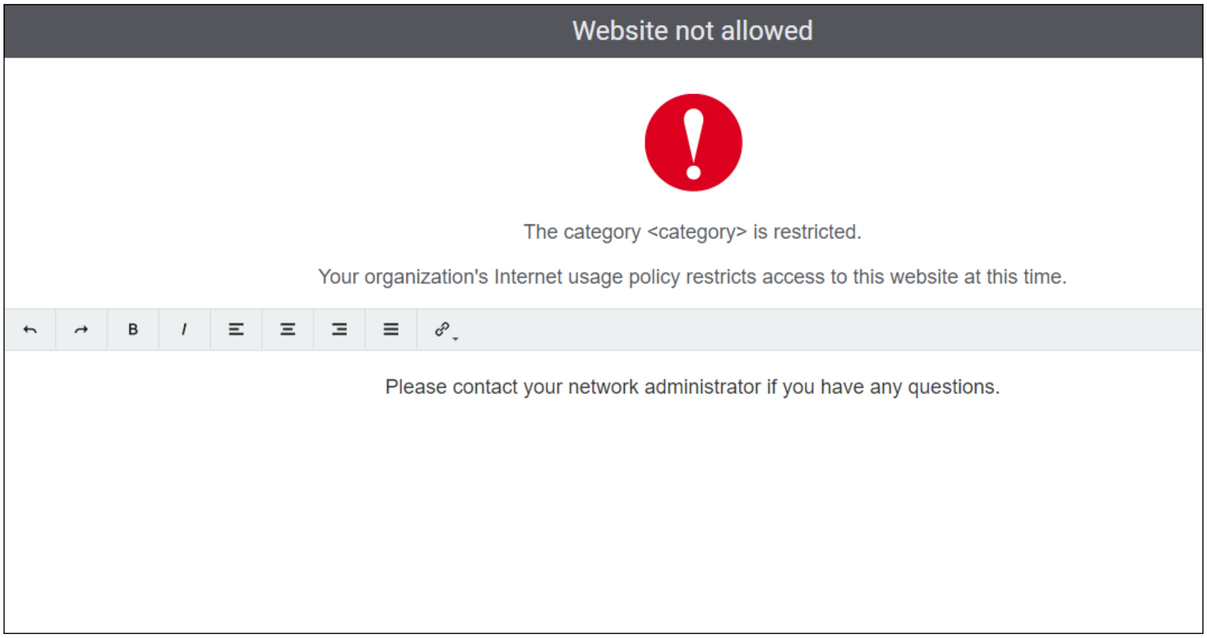
4. In the upper left corner, do either of the following:
   - Drag an image or click in the area to upload your logo.
   - Click the **Delete current image** to delete the space for a logo.



**Note:** Logos can be no bigger than 1 MB, and have a maximum height of 50 pixels, and a maximum width of 500 pixels.

5. In the free-form field, enter a message that displays for your users whenever the attempt to access a restricted website.
   - The blue box in the lower left of the screen displays the number of characters used.
   - The default message is *Please contact your network administrator if you have any questions*, which can be changed, as needed.

- Use the WYSIWYG editing menu to format the message, as needed.



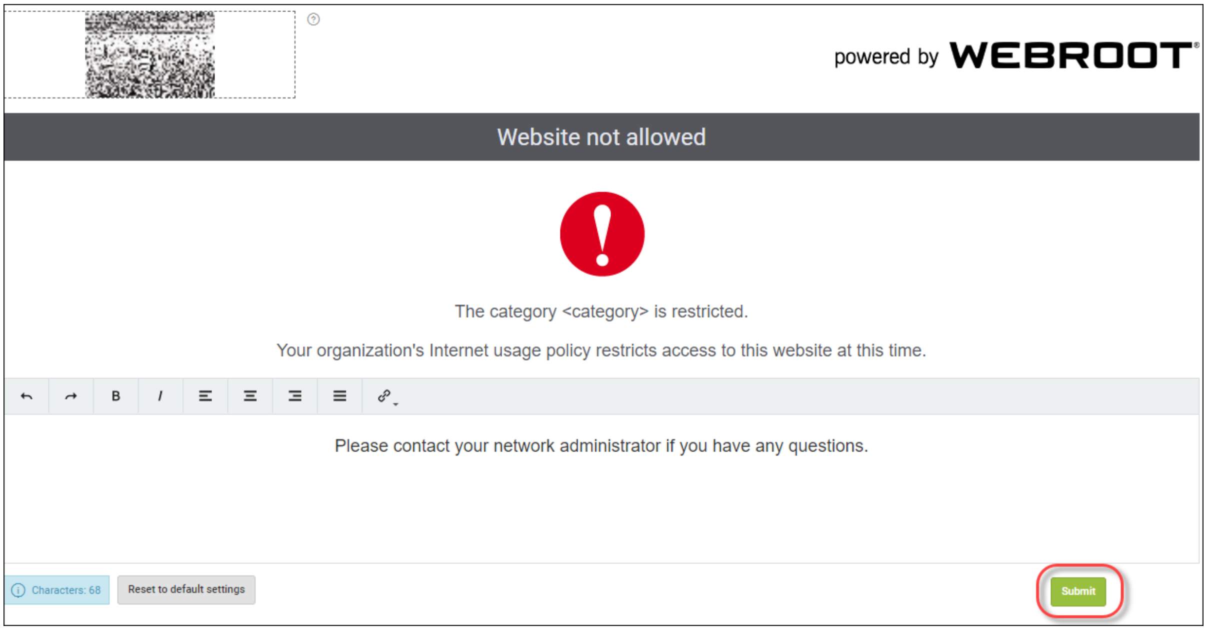
Website not allowed

The category <category> is restricted.

Your organization's Internet usage policy restricts access to this website at this time.

Please contact your network administrator if you have any questions.

6. When you're done, click the **Submit** button.



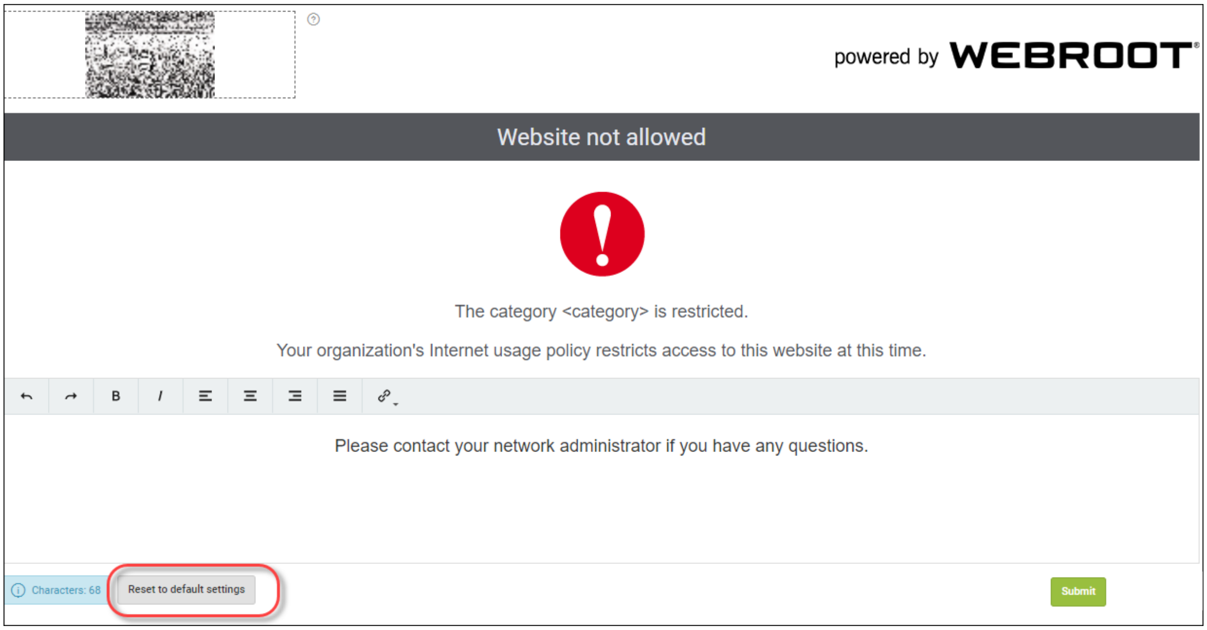
Website not allowed

The category <category> is restricted.

Your organization's Internet usage policy restricts access to this website at this time.

Please contact your network administrator if you have any questions.

7. As needed, click the **Reset to default settings** button.



Website not allowed

The category <category> is restricted.

Your organization's Internet usage policy restricts access to this website at this time.

Please contact your network administrator if you have any questions.

# Chapter 9: Working With Alerts

To work with alerts, see the following topics:

# Creating Alerts

You can now create alerts at the global level, which reduces the maintenance overhead as these can now all be handled from one shared location instead of having to manually manage individual site alerts.

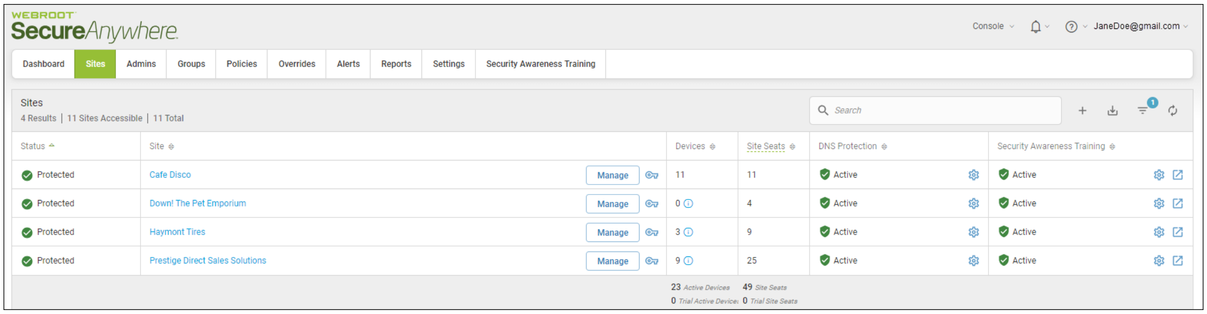
Alerts can now be set up and managed centrally by selecting which type of alert you want to send, either Infection Alert, Installation Alert, Infection Summary, or Installation Summary, along with the frequency at which these alerts should be sent. You can then apply alerts to any child endpoint protection site.

> **Note:** Global alerts created at the management console level are visible at the Site level in view-only mode

**To create an alert:**

1. Log in to the management console.

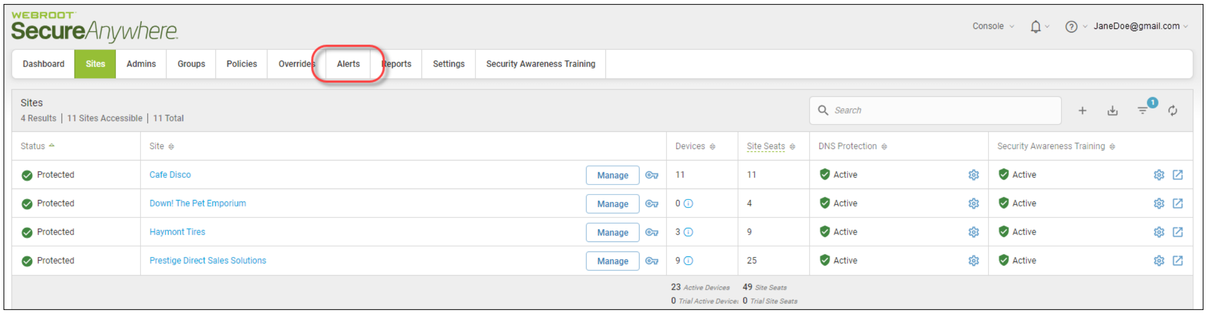
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

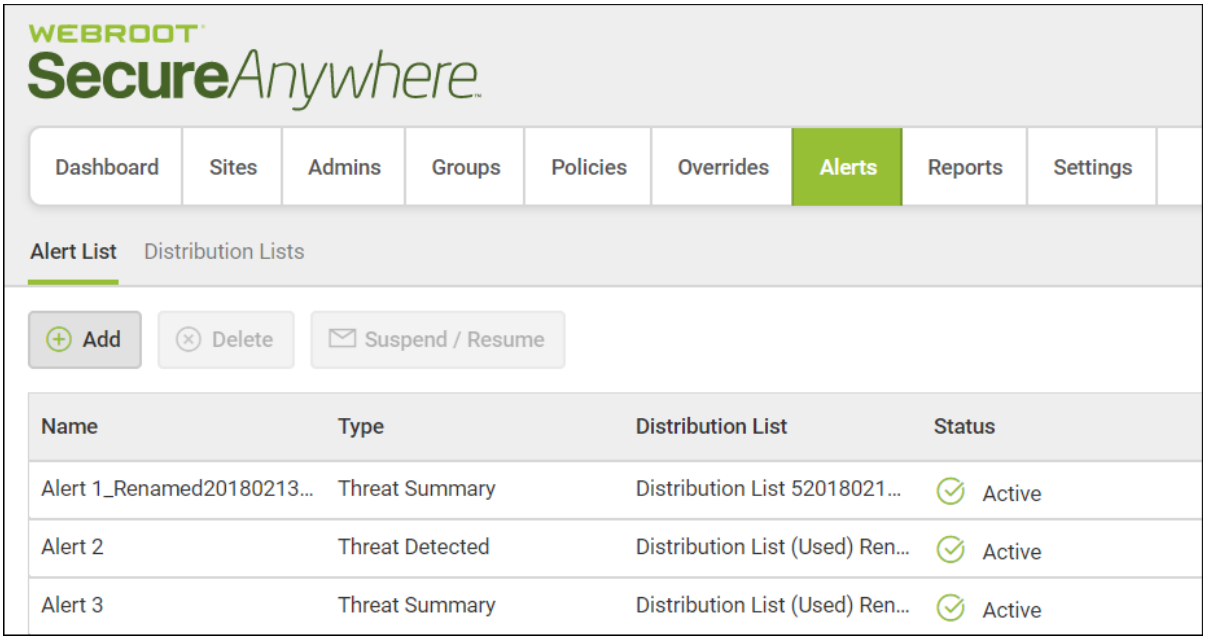
2. Click the **Alerts** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

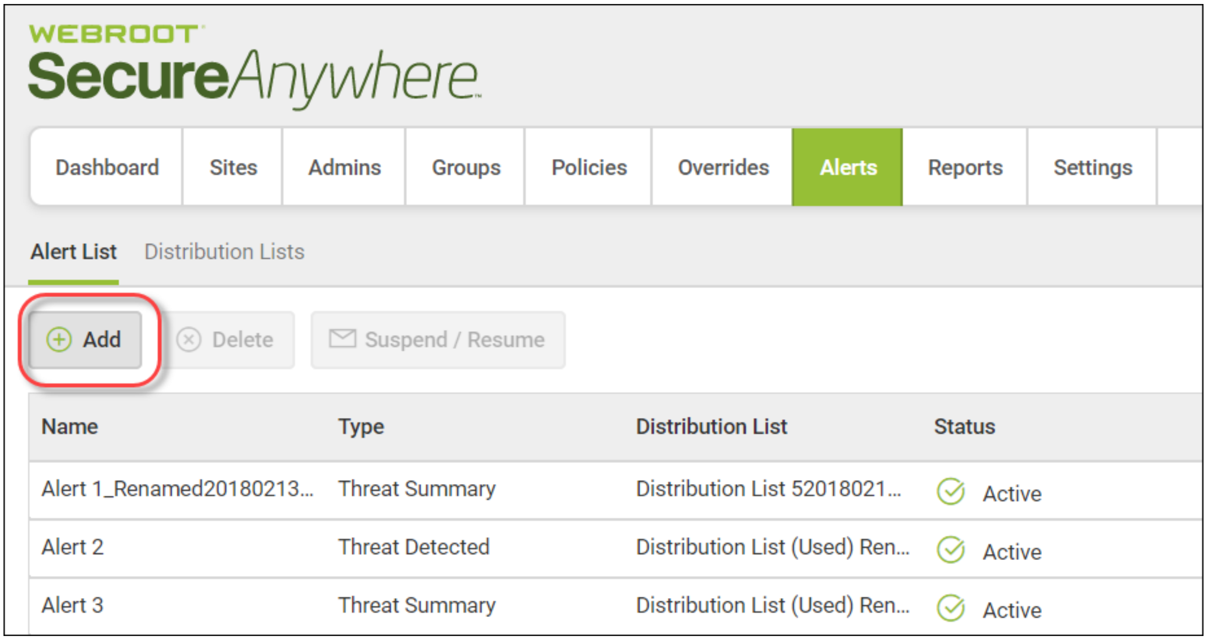
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

   The system displays the Alerts tab, with the Alert List tab active.



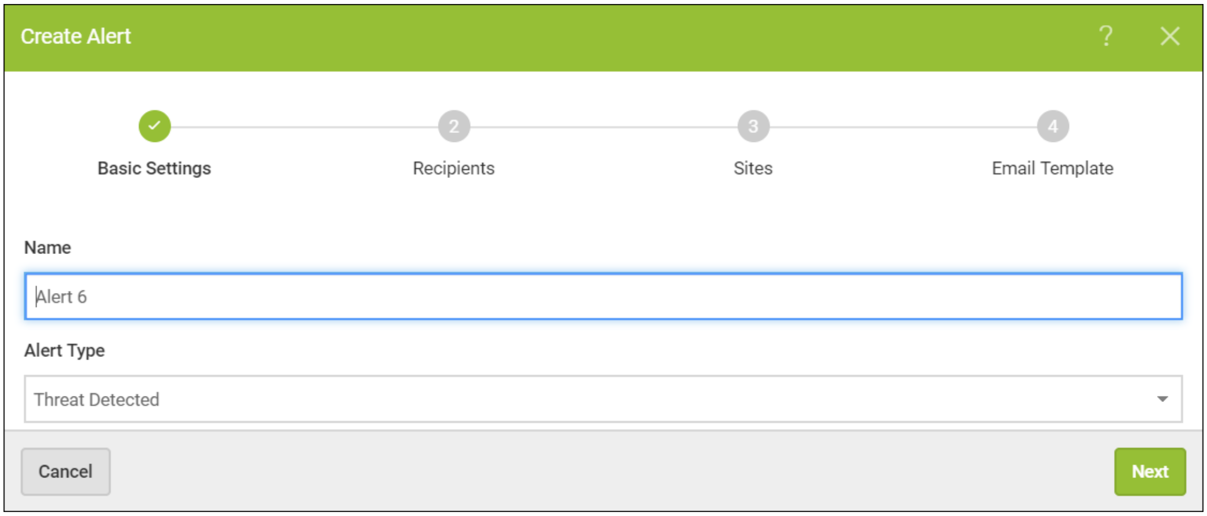
| Name | Type | Distribution List | Status |
|---|---|---|---|
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

3. Click the **Add** button.



| Name | Type | Distribution List | Status |
|---|---|---|---|
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

The system displays the Create Alert window.



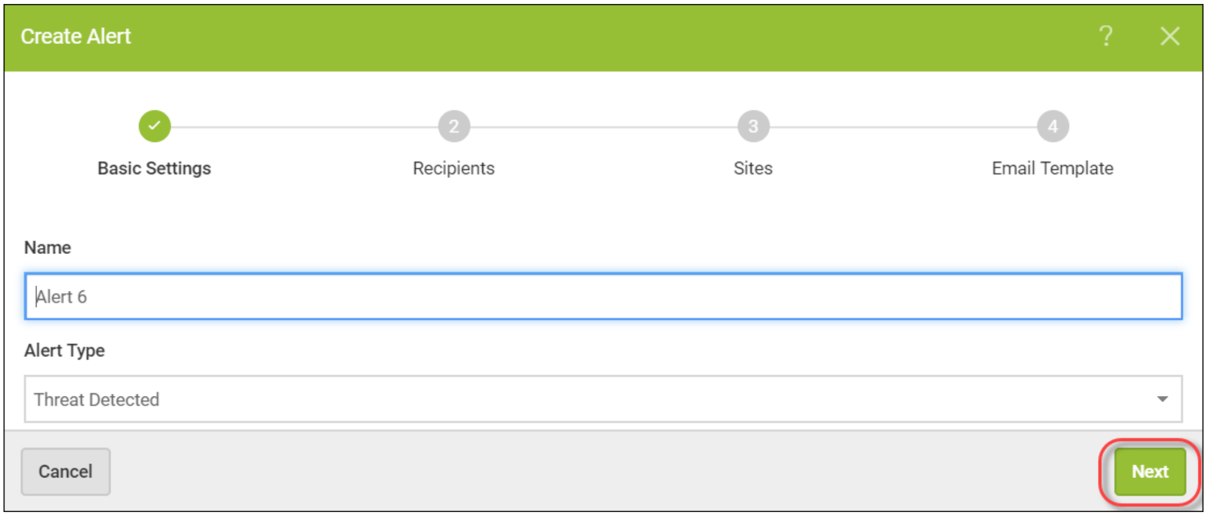
Name: Alert 6

Alert Type: Threat Detected

4. In the Name field, do either of the following:
   - Accept the system-generated name for the alert.
   - Enter a new name for the alert.

5. From the Alert Type drop-down menu, select one of the following to determine the type of alert:
   - **Infection Detected**
   - **Endpoint Installed**
   - **Infection Summary**
   - **Installation Summary**

6. Click the **Next** button.



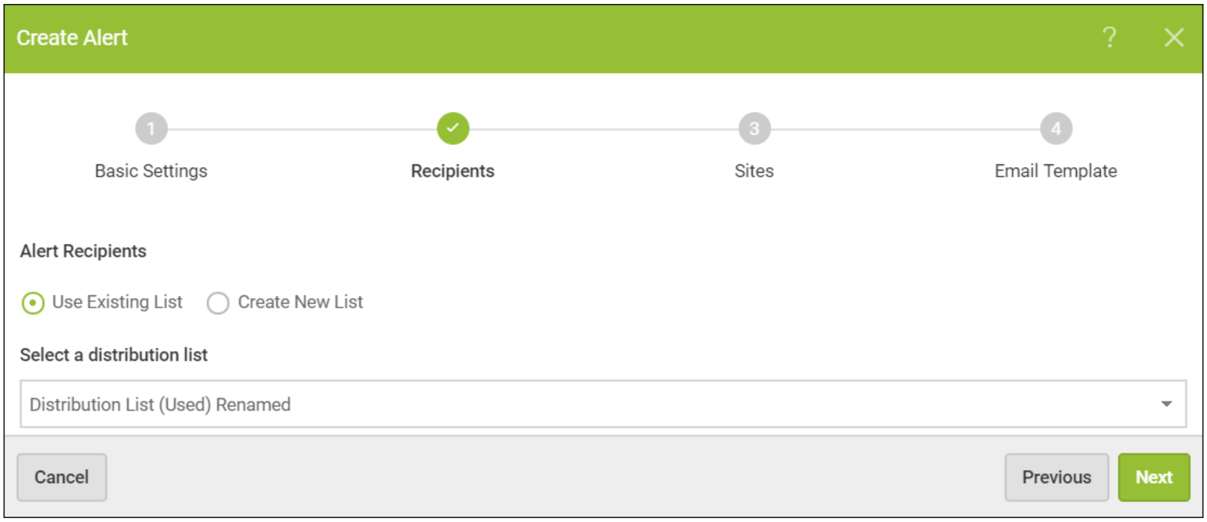
Name

Alert 6

Alert Type

Threat Detected

The system displays the Recipients panel.



Alert Recipients

● Use Existing List ○ Create New List

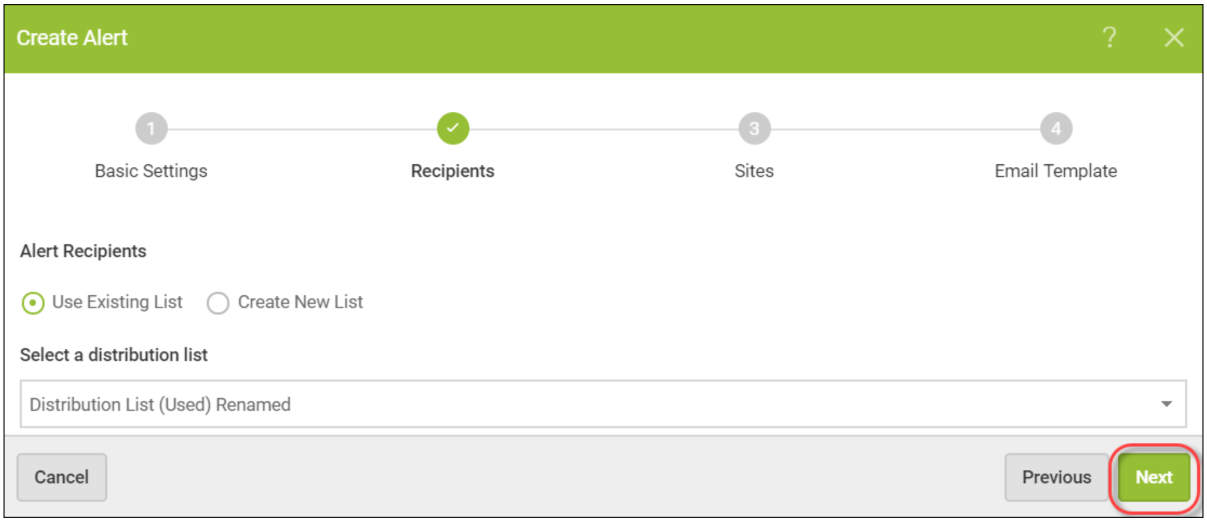
Select a distribution list

Distribution List (Used) Renamed

7. Select one of the following Alert Recipients radio buttons:
   - **Use Existing List**
   - **Create New List**

8. If you selected Create New List, do both of the following, otherwise continue with the next step.
   - In the Distribution List Name field, enter a name for the new distribution list.
   - In the Email Addresses field, enter the email addresses for the recipients of the new distribution list.
9. From the Select a distribution list drop-down menu, select from any of the distribution lists you previously created.

   For more information, see *Creating Distribution Lists* in the WSA Business Endpoint Protection Admin Guide.
10. Click the **Next** button.



Create Alert

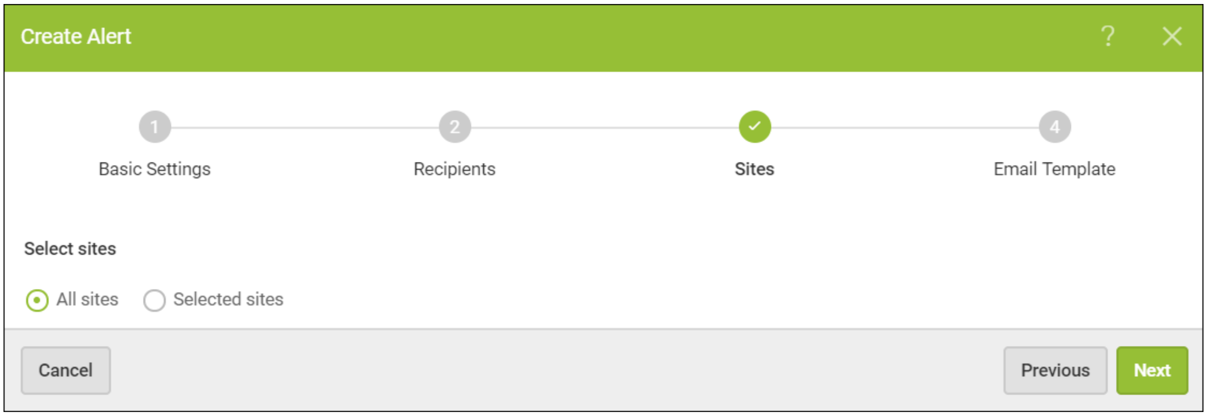
Alert Recipients

● Use Existing List ○ Create New List

Select a distribution list

Distribution List (Used) Renamed

The system displays the Sites panel.

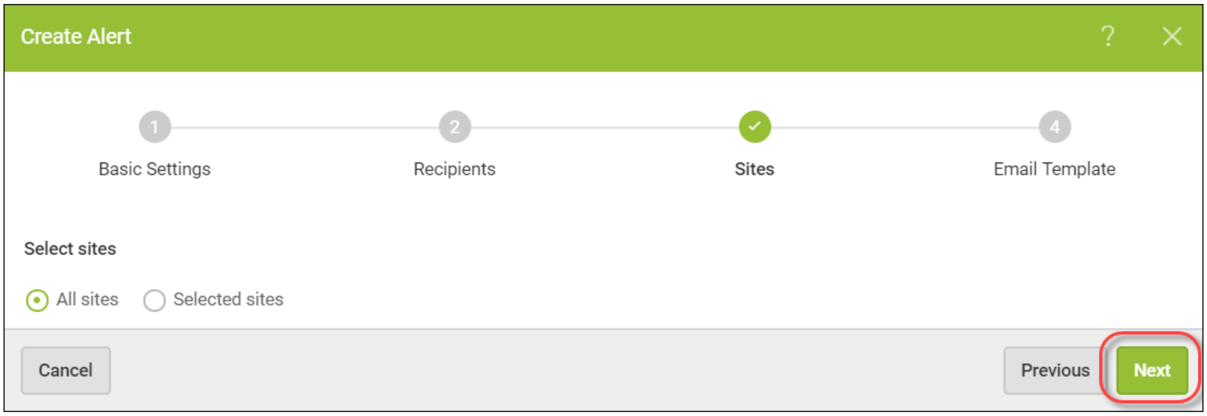


Create Alert

Select sites

● All sites ○ Selected sites

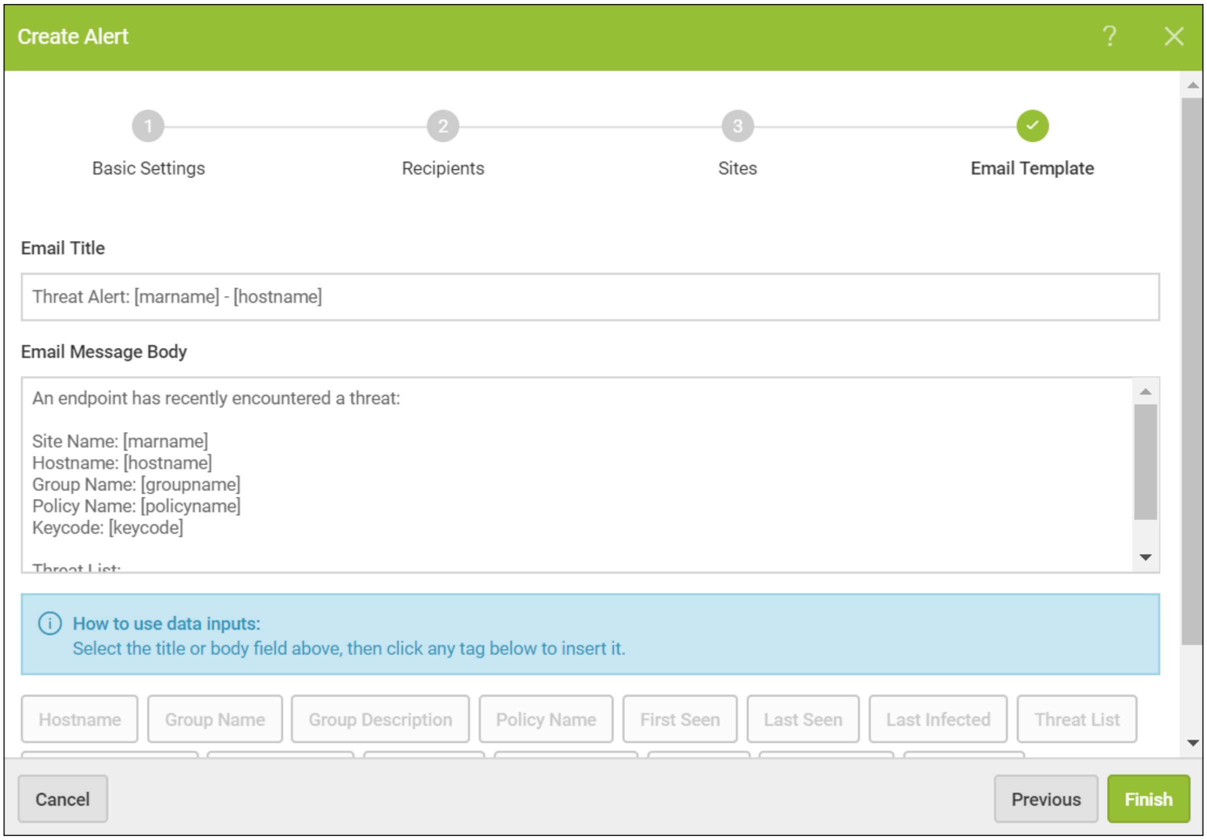
11. Select one of the following Sites to use this alert radio buttons:
    - **All Sites**
    - **Selected Sites**
12. Click the **Next** button.



Select sites

● All sites ○ Selected sites

The system displays the Email Template panel.



Email Title

Threat Alert: [marname] - [hostname]

Email Message Body

An endpoint has recently encountered a threat:

Site Name: [marname]
Hostname: [hostname]
Group Name: [groupname]
Policy Name: [policyname]
Keycode: [keycode]

Threat List:

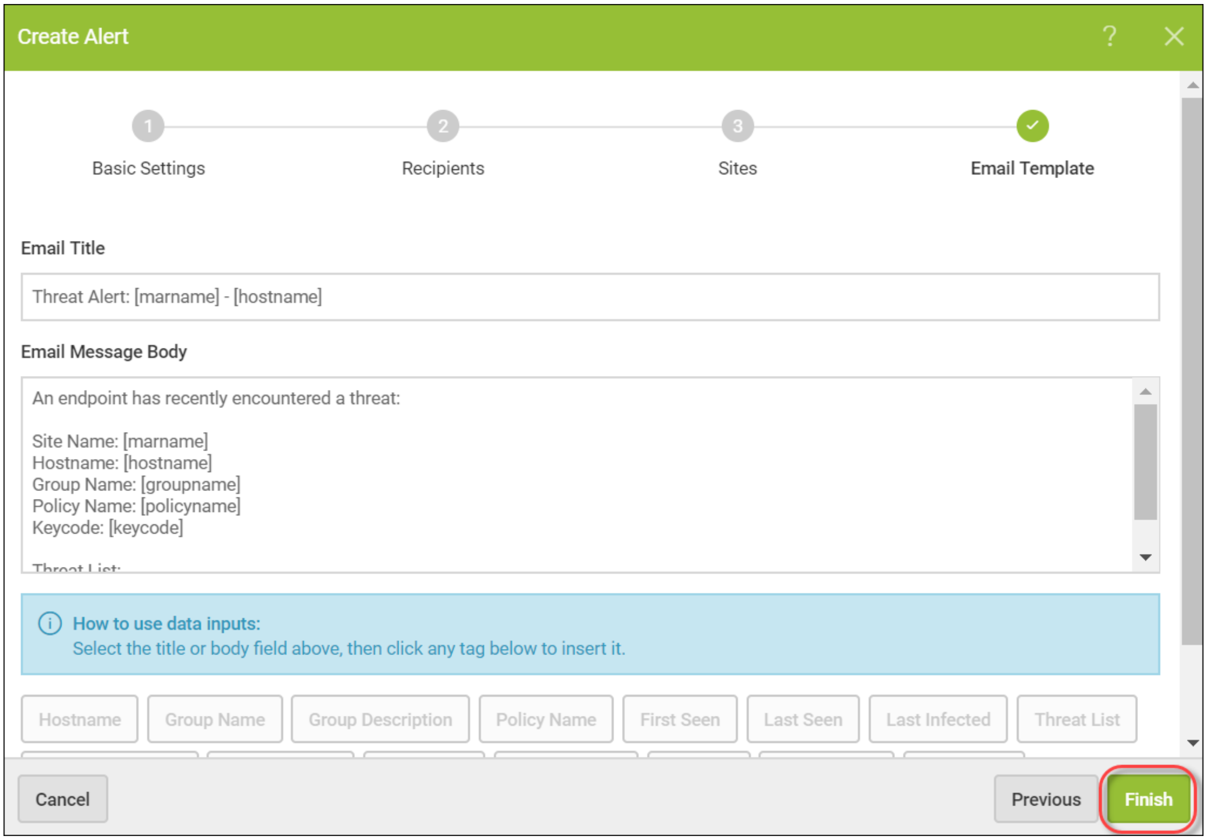
How to use data inputs:
Select the title or body field above, then click any tag below to insert it.

13. In the Email Title field, enter a name for the email.
14. In the Email Message Body field, enter the text that you want to send.
15. To use Data Inputs, place the cursor in the text, then click any of the tags to insert the data input at that point in the text.

    The following data points are unsupported in the Mac agent:

    - Workgroup
    - Active Directory

16. When you're done, click the **Finish** button.



Email Title

Threat Alert: [marname] - [hostname]

Email Message Body

An endpoint has recently encountered a threat:

Site Name: [marname]
Hostname: [hostname]
Group Name: [groupname]
Policy Name: [policyname]
Keycode: [keycode]

Threat List:

How to use data inputs:
Select the title or body field above, then click any tag below to insert it.

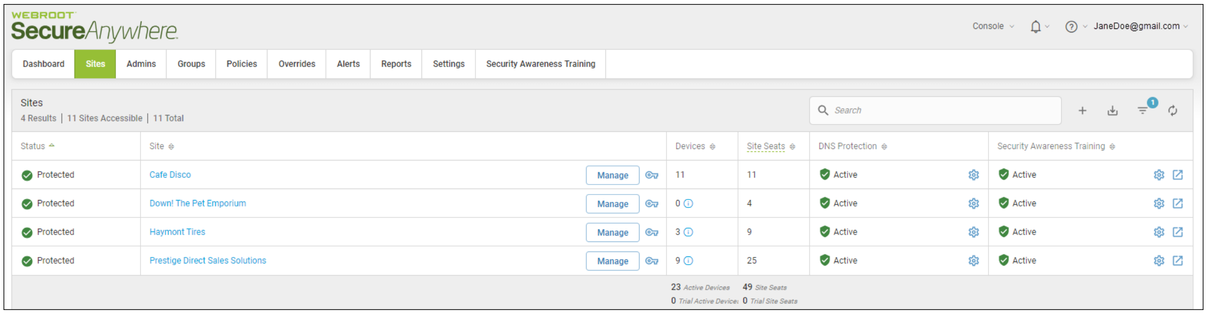
# Deleting Alerts

Follow this procedure to delete alerts.

### To delete an alert:

1. Log in to the management console.

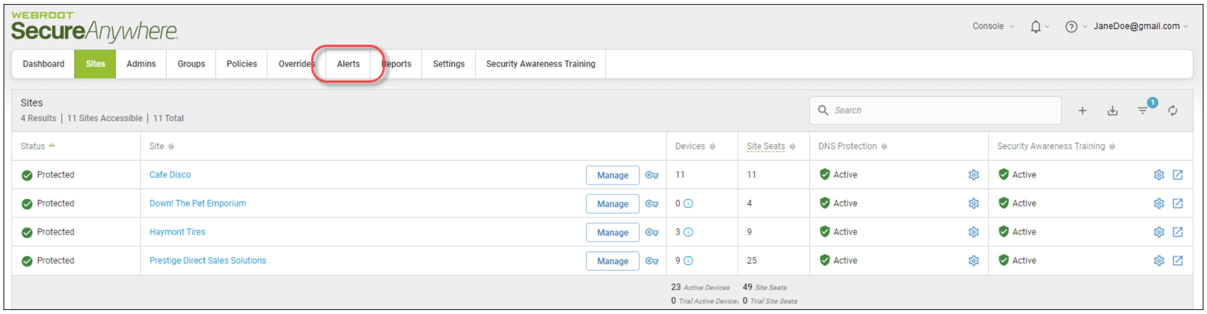
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

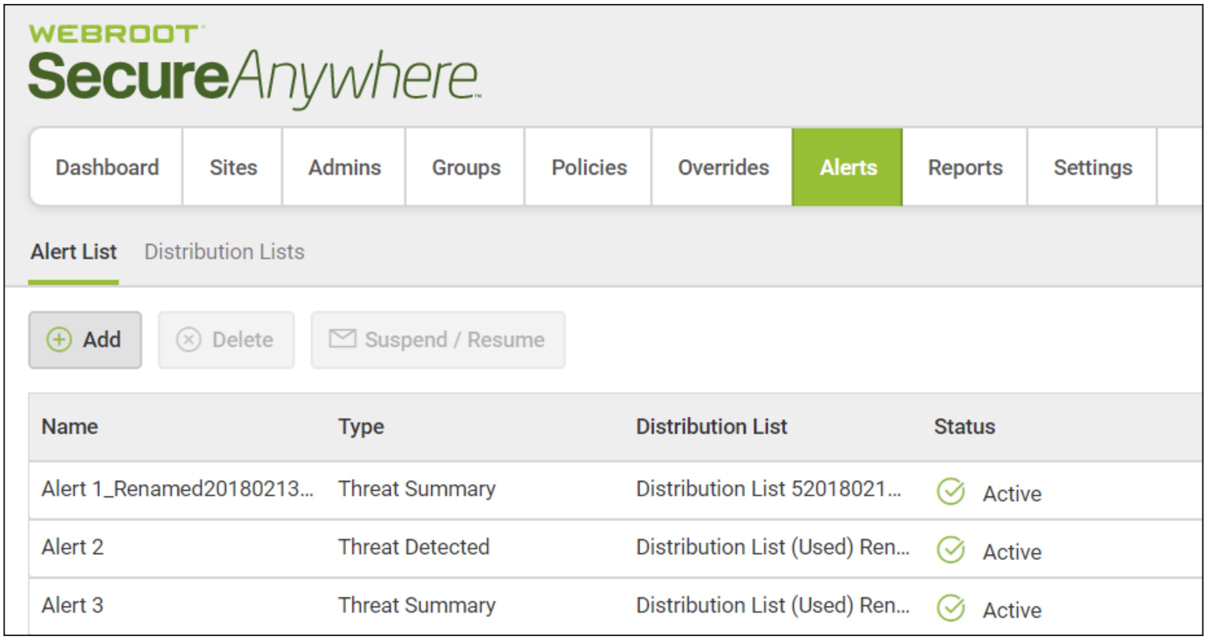
2. Click the **Alerts** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

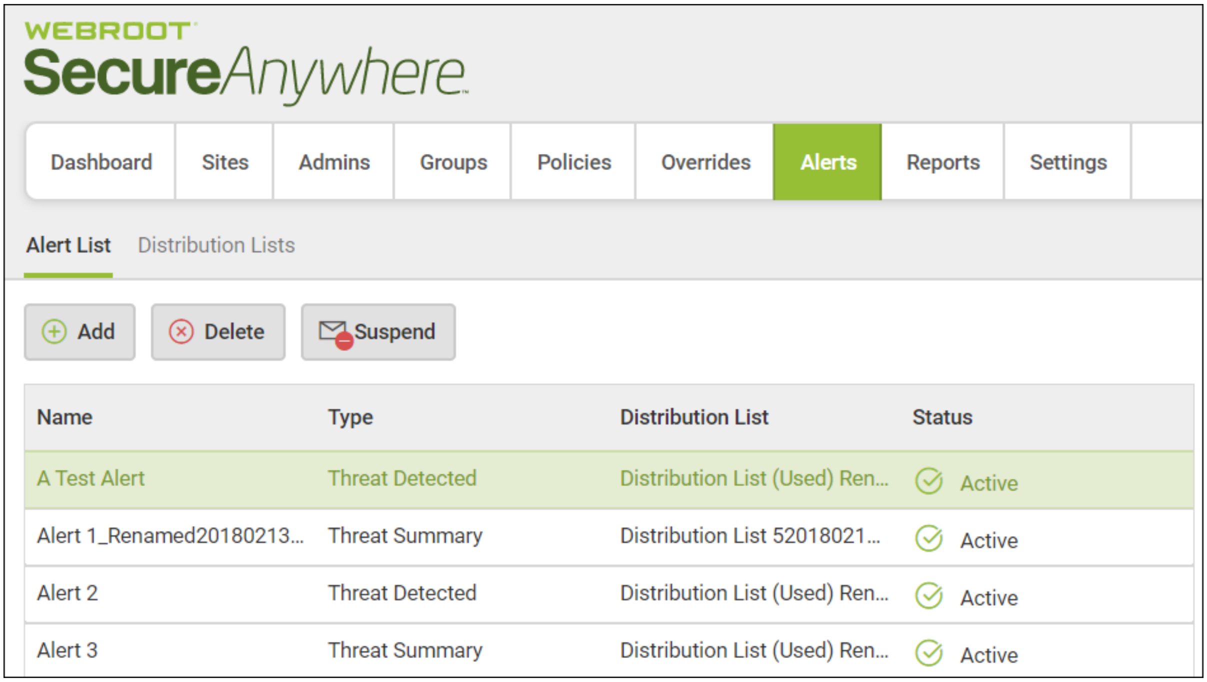
The system displays the Alerts tab, with the Alert List tab active.



| Name | Type | Distribution List | Status |
|---|---|---|---|
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

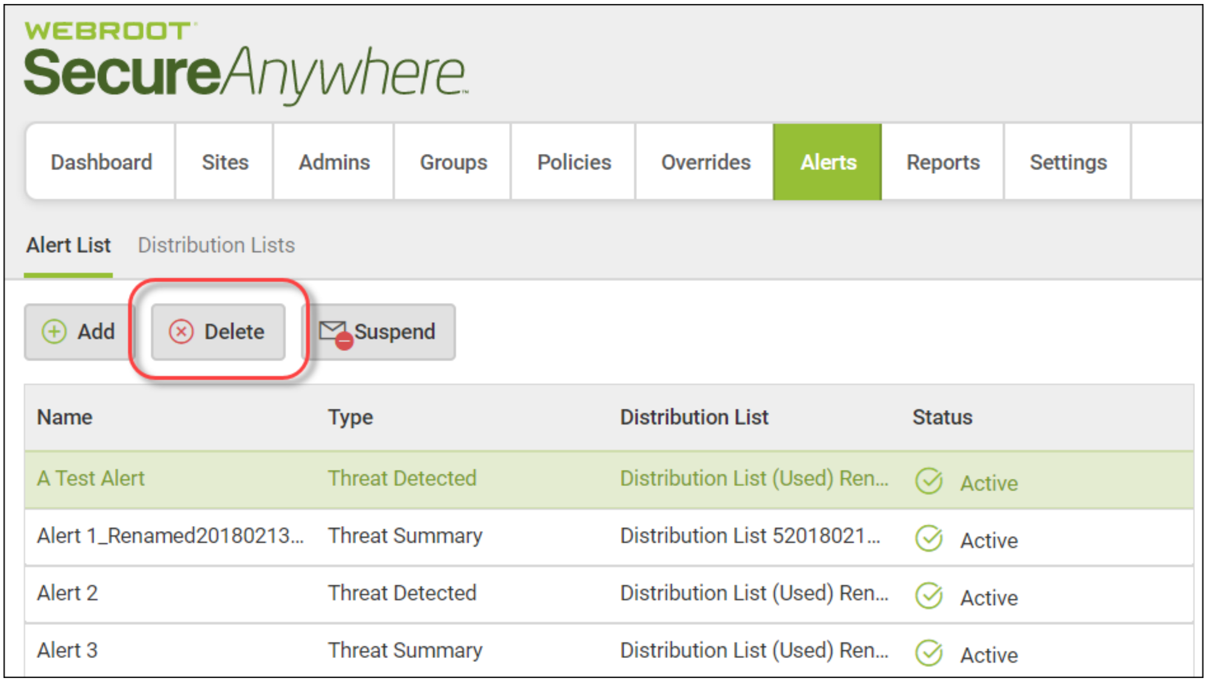
3. Click the alert you want to delete.

   The system displays information about that alert and the Delete button becomes active.



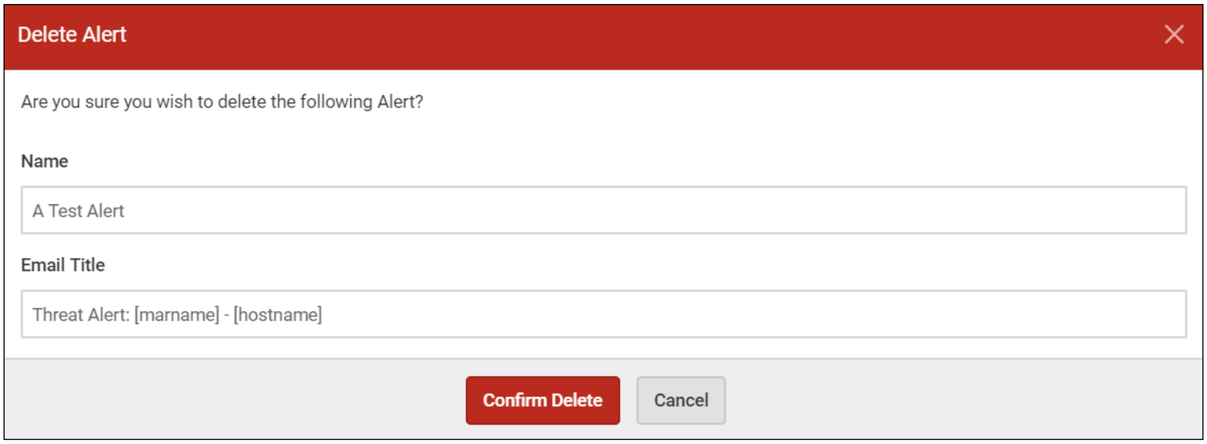
| Name | Type | Distribution List | Status |
|---|---|---|---|
| A Test Alert | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

4. Click the **Delete** button.



| Name | Type | Distribution List | Status |
|---|---|---|---|
| A Test Alert | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

The Delete Alert Message displays.



Are you sure you wish to delete the following Alert?

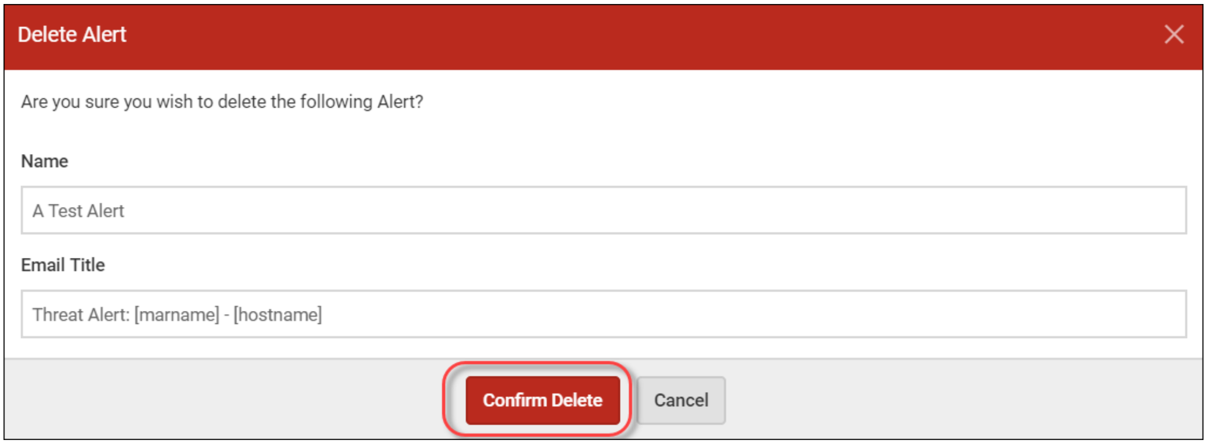
Name

A Test Alert

Email Title

Threat Alert: [marname] - [hostname]

5. Click the **Confirm Delete** button.



Delete Alert

Are you sure you wish to delete the following Alert?

Name

A Test Alert

Email Title

Threat Alert: [marname] - [hostname]

The system deletes the alert.

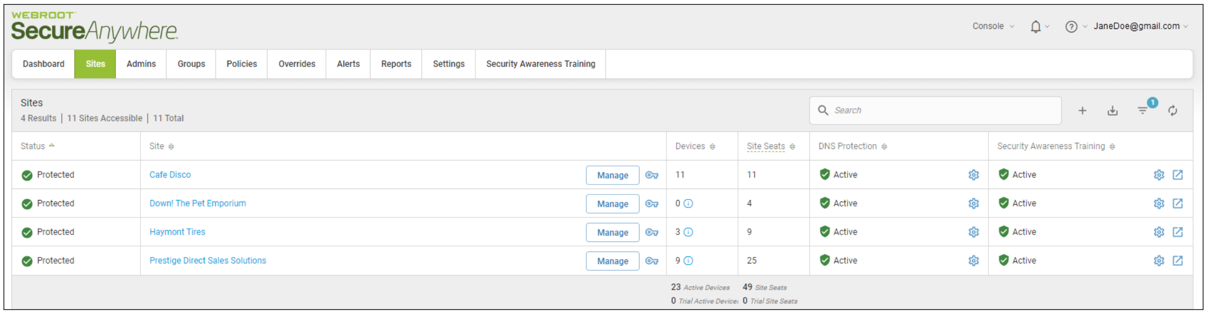
# Suspending or Resuming Alerts

Follow this procedure to suspend or resume an alert.

### To suspend or resume an alert:

1. Log in to the management console.

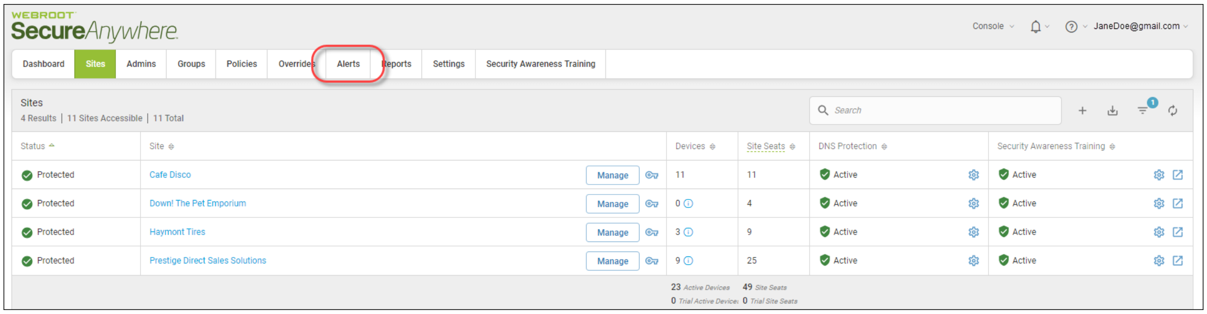
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

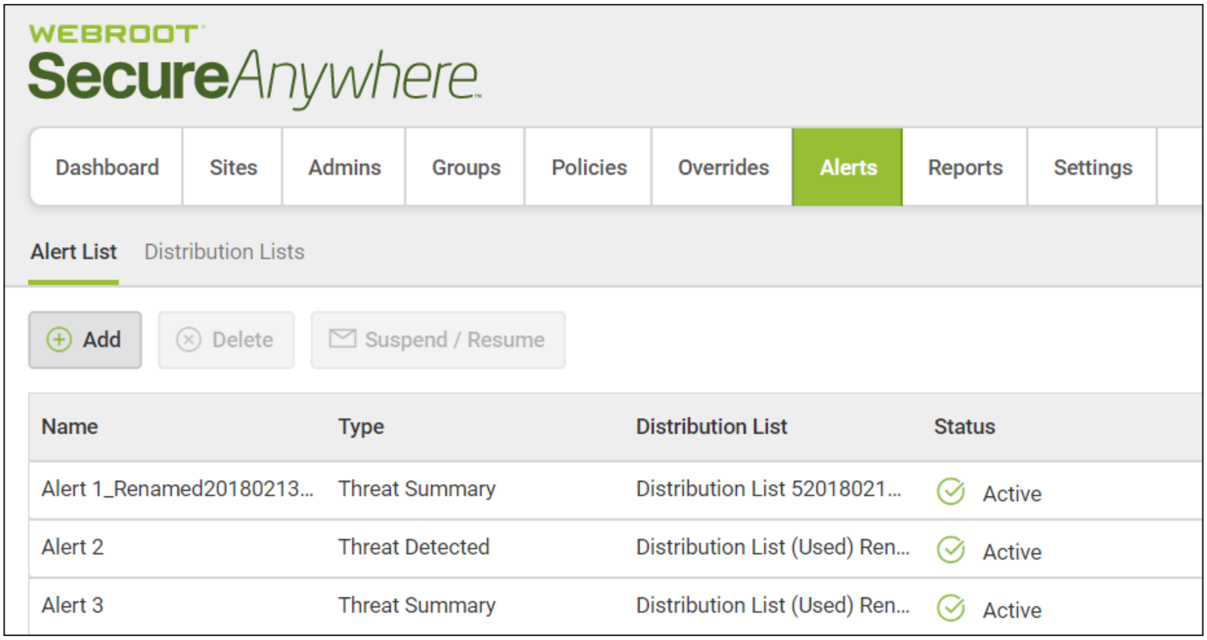
2. Click the **Alerts** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

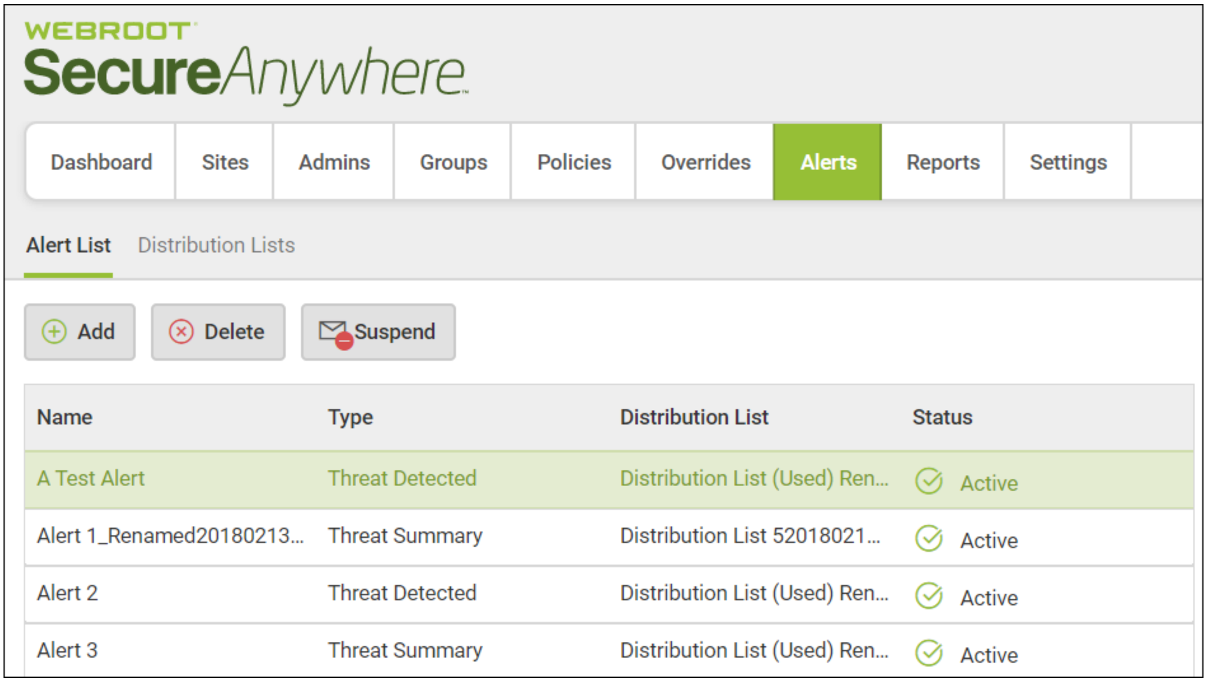
   The system displays the Alerts tab, with the Alert List tab active.



| Name | Type | Distribution List | Status |
|---|---|---|---|
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

3. Click the alert that you want to suspend or resume.

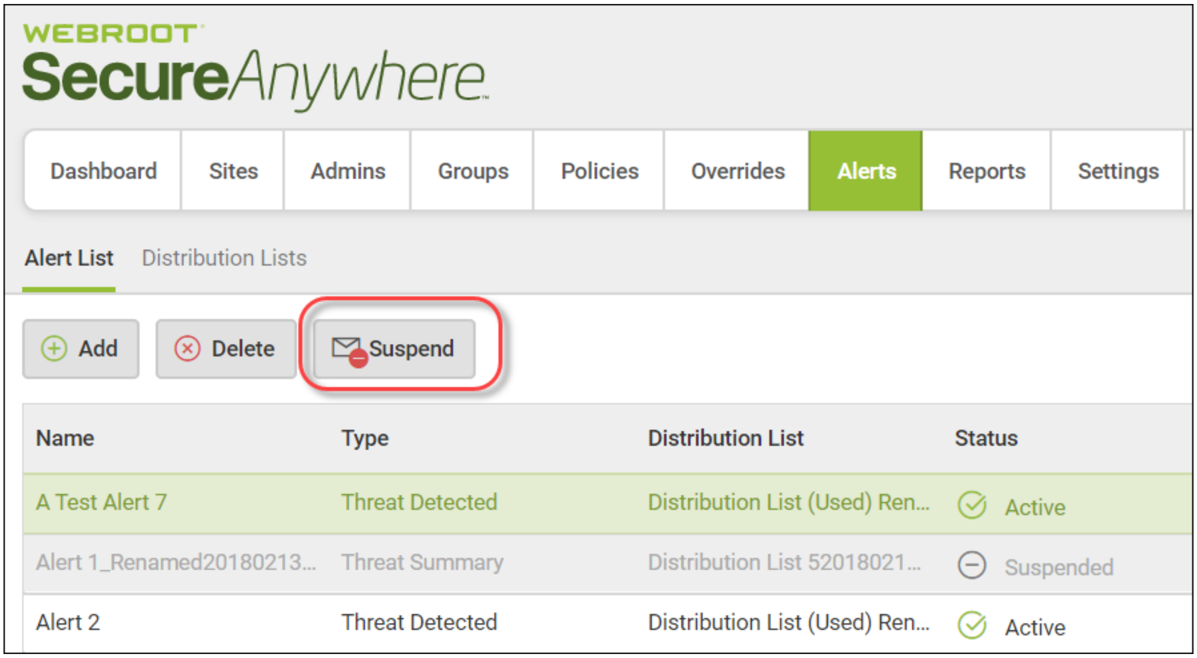
   The system displays information about that alert and the Suspend/Resume button becomes active.



| Name | Type | Distribution List | Status |
|---|---|---|---|
| A Test Alert | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

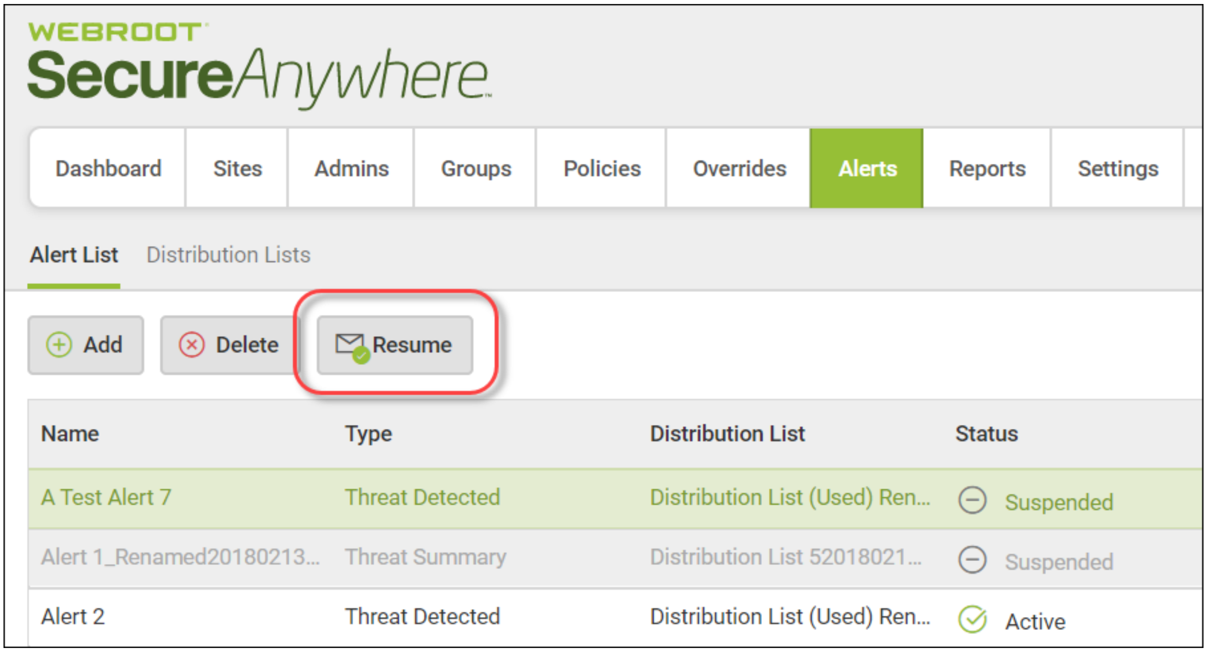
**Note:** If the alert is active, the button lets you suspend it. If the alert has been suspended, the button allows you to resume the alert.

4. Do either of the following:
   - Click the **Suspend** button to suspend the alert.



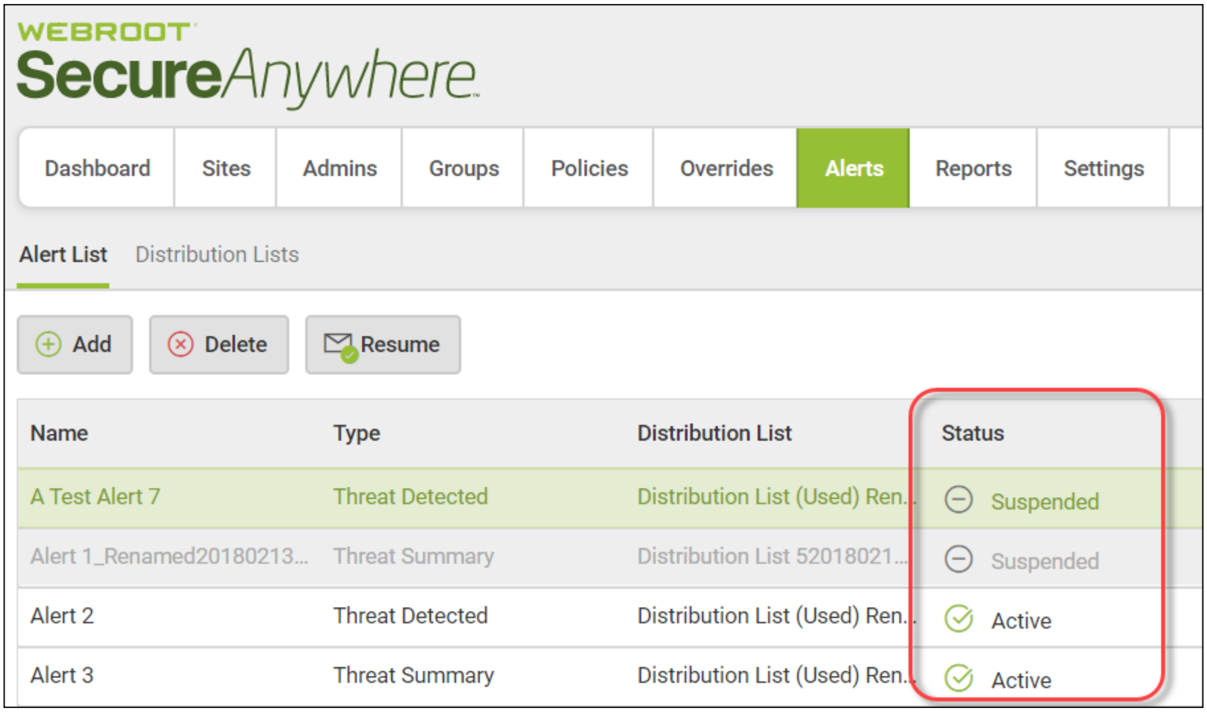
| Name | Type | Distribution List | Status |
|---|---|---|---|
| A Test Alert 7 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ⊖ Suspended |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |

- Click the **Resume** button to resume the alert.



| Name | Type | Distribution List | Status |
|---|---|---|---|
| A Test Alert 7 | Threat Detected | Distribution List (Used) Ren... | ⊖ Suspended |
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ⊖ Suspended |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |

The Status column reflects whether the alert is active or suspended.



| Name | Type | Distribution List | Status |
|---|---|---|---|
| A Test Alert 7 | Threat Detected | Distribution List (Used) Ren... | ⊖ Suspended |
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ⊖ Suspended |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

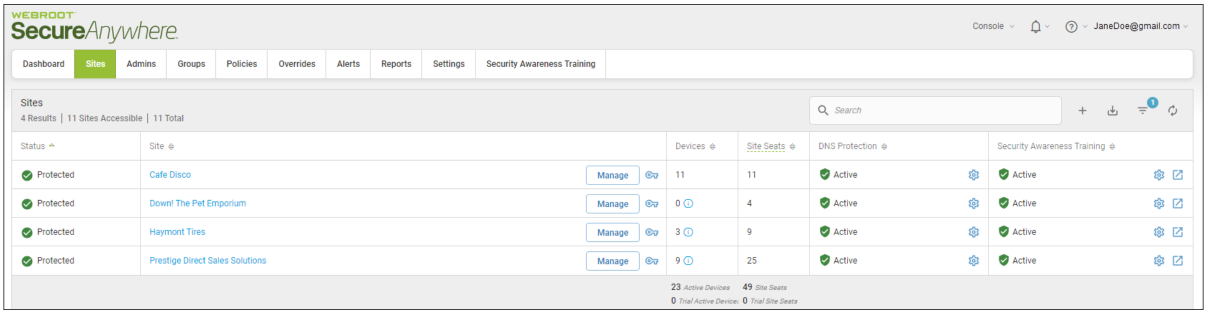
# Creating Distribution Lists

From the Alerts tab, you can create a distribution list of users who will receive alert messages. For example, you might want to create a list of administrators who need to respond to threat detections at a remote office.

**To create a distribution list:**

1. Log in to the [management console](management console).

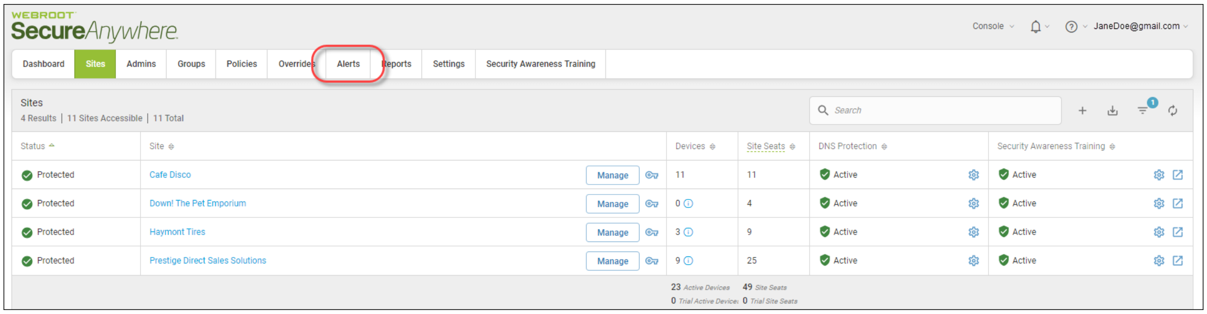
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

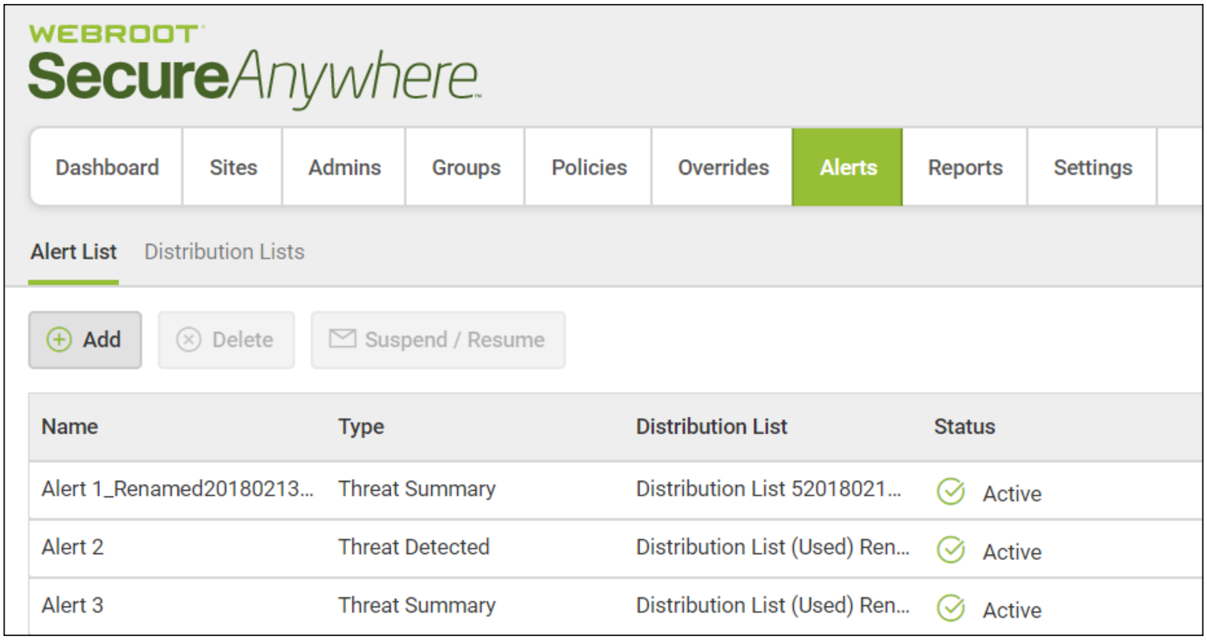
2. Click the **Alerts** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

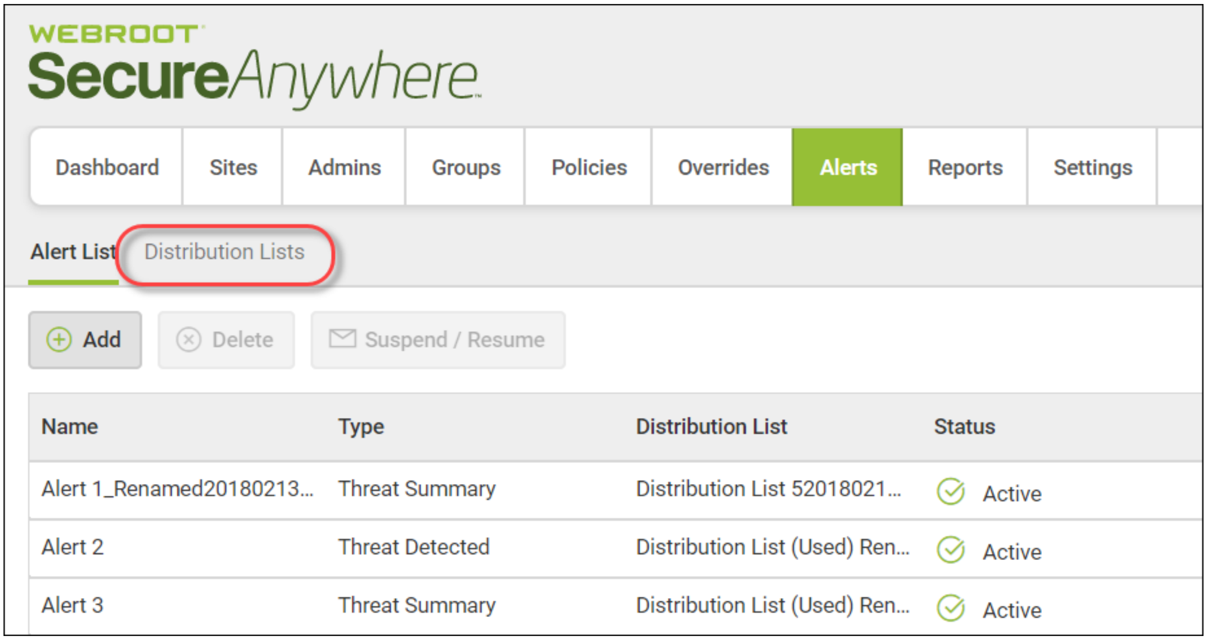
| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Devices* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

   The system displays the Alerts tab, with the Alert List tab active.



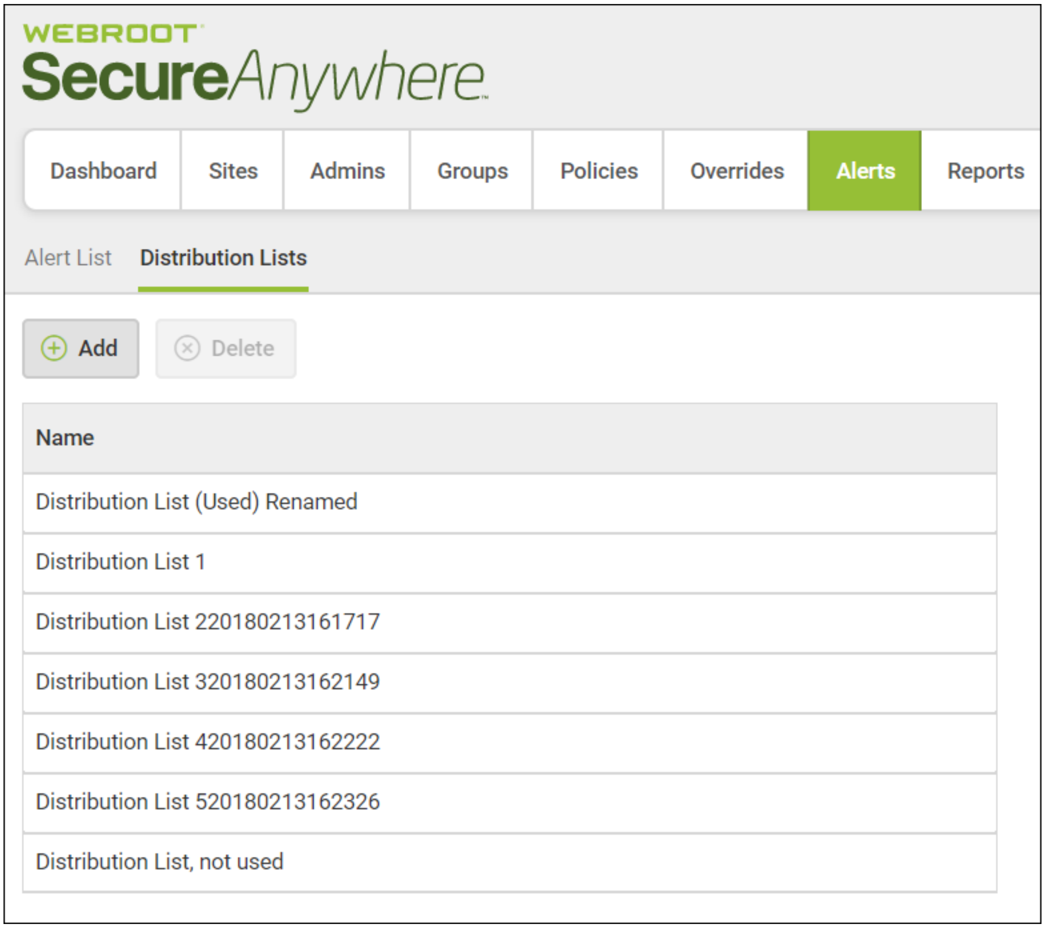
| Name | Type | Distribution List | Status |
|---|---|---|---|
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

3. Click the **Distribution Lists** tab.



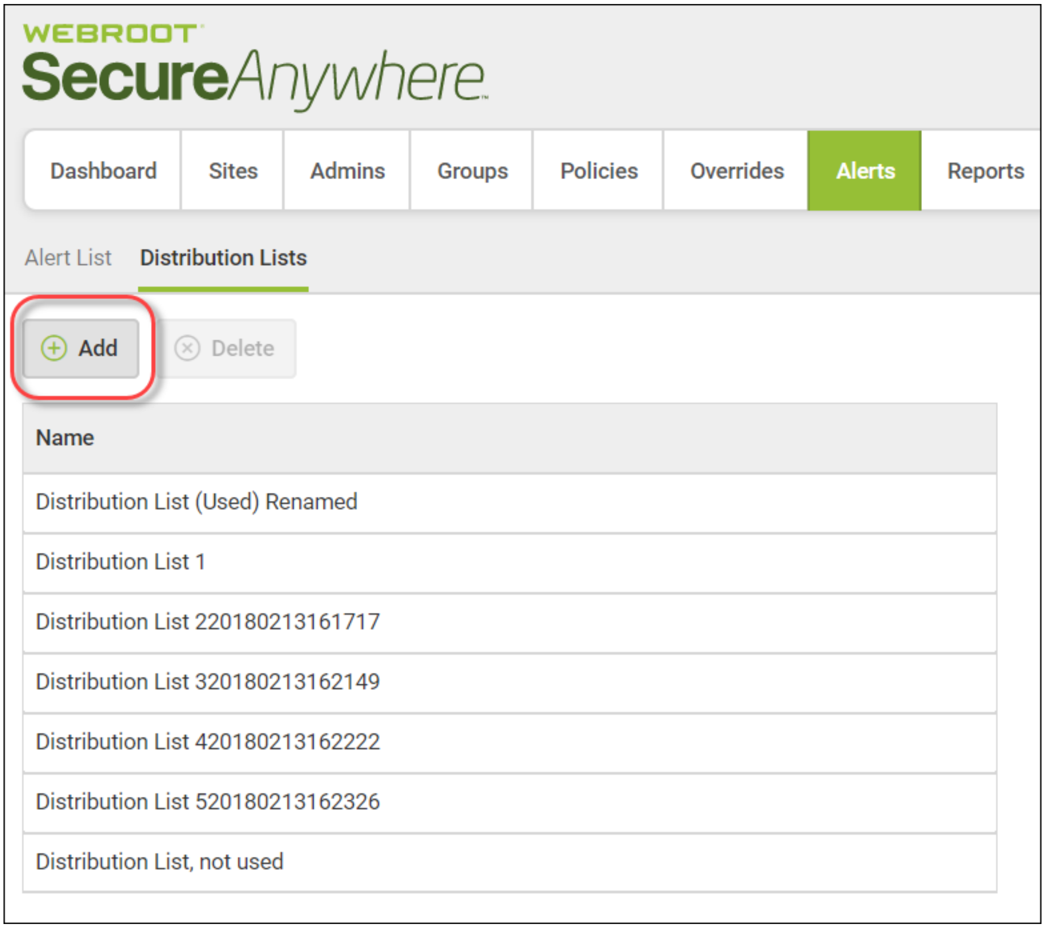
| Name | Type | Distribution List | Status |
|---|---|---|---|
| Alert 1_Renamed20180213... | Threat Summary | Distribution List 52018021... | ✓ Active |
| Alert 2 | Threat Detected | Distribution List (Used) Ren... | ✓ Active |
| Alert 3 | Threat Summary | Distribution List (Used) Ren... | ✓ Active |

The Distribution Lists tab displays.



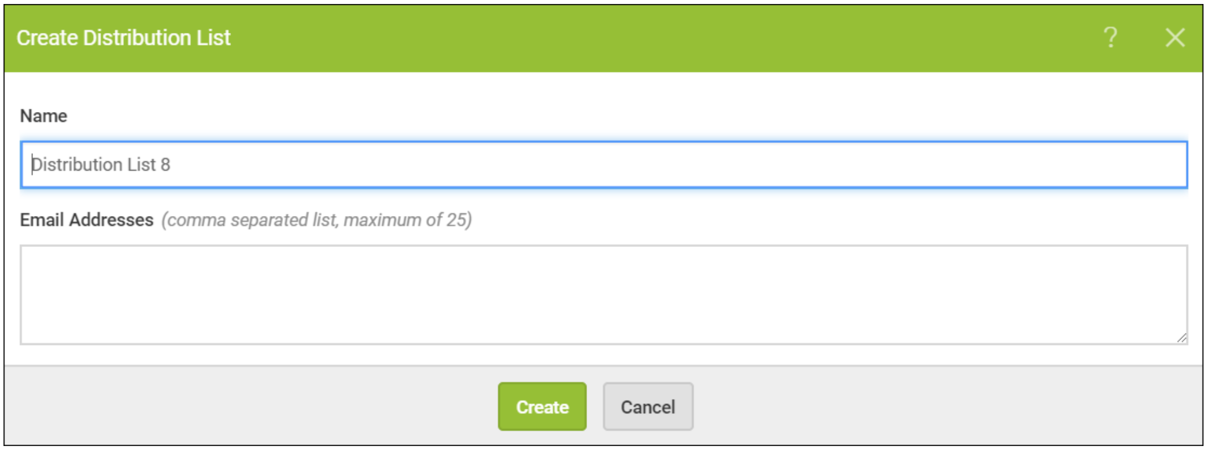
| Name |
|---|
| Distribution List (Used) Renamed |
| Distribution List 1 |
| Distribution List 220180213161717 |
| Distribution List 320180213162149 |
| Distribution List 420180213162222 |
| Distribution List 520180213162326 |
| Distribution List, not used |

4. Click the **Add** button.



| Name |
|---|
| Distribution List (Used) Renamed |
| Distribution List 1 |
| Distribution List 220180213161717 |
| Distribution List 320180213162149 |
| Distribution List 420180213162222 |
| Distribution List 520180213162326 |
| Distribution List, not used |

The Create Distribution List window displays.



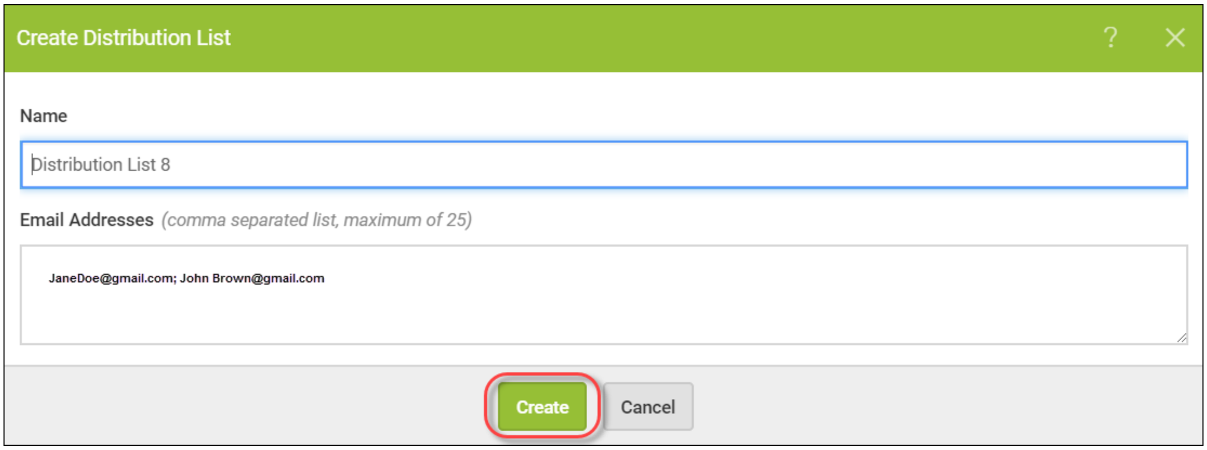
Create Distribution List

Name

Distribution List 8

Email Addresses *(comma separated list, maximum of 25)*

5. In the Name field, do either of the following:
   - Accept the system-generated name for the alert.
   - Enter a new name for the alert.
6. In the Email Addresses field, enter the email addresses for the recipients of the new distribution list.
7. When you're done, click the **Create** button.



Create Distribution List

Name

Distribution List 8

Email Addresses *(comma separated list, maximum of 25)*

JaneDoe@gmail.com; John Brown@gmail.com

# Chapter 10: Working With Reports

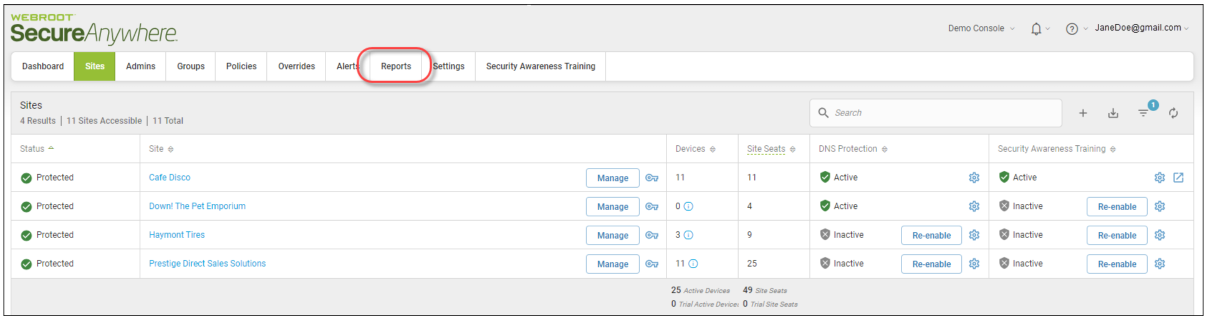
To work with reports, see the following topics:

# Global Site Manager Reports Overview

The management site console reports functionality can report on the health and performance of your individual sites or complete deployment with a granular set of tools to ensure you can report the information you want when it’s needed.

Schedule customized reports to run at recurring time periods or run them ad-hoc with content targeted to the individual requirements of the recipient. Scheduled Reports means you and your customers will never miss the information which is important to them.

All reporting functionality is located in the management site console, under the Reports tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | | Security Awareness Training | |
|---|---|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | | Active | |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | | Inactive | Re-enable |
| Protected | Haymont Tires | Manage | 3 | 9 | Inactive | Re-enable | Inactive | Re-enable |
| Protected | Prestige Direct Sales Solutions | Manage | 11 | 25 | Inactive | Re-enable | Inactive | Re-enable |
| | | | 25 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | | | |

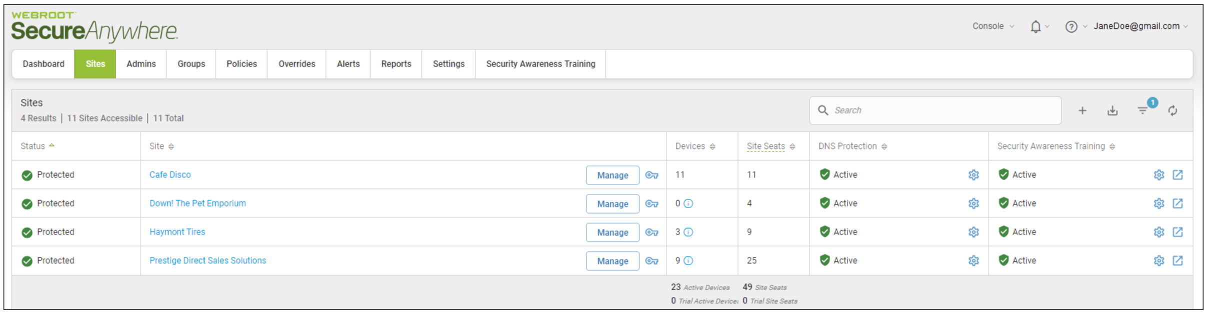
# Creating Reports

With its customizable data, scheduling, recipients and languages, Scheduled Reporting gives you the information and flexibility you need to keep your stakeholders in the know.

### To create a report:

1. Log in to the management console.

   The management console displays with the Sites tab active.

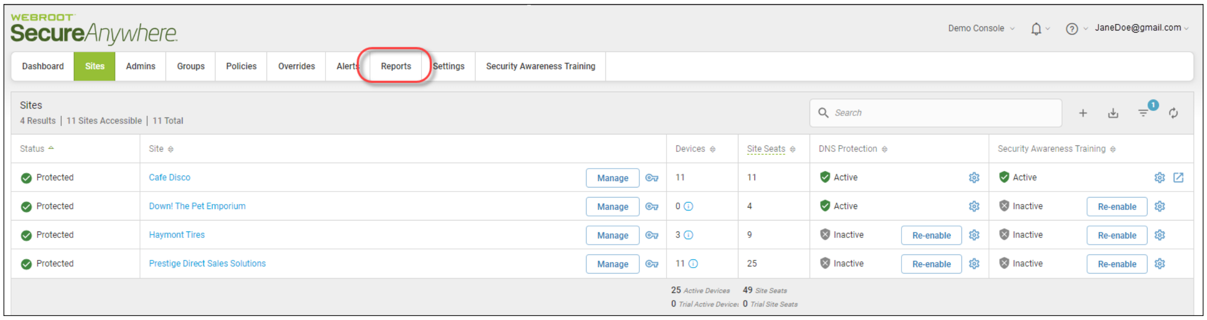


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |

23 Active Devices 49 Site Seats
0 Trial Active Device: 0 Trial Site Seats

2. Click the **Reports** tab.

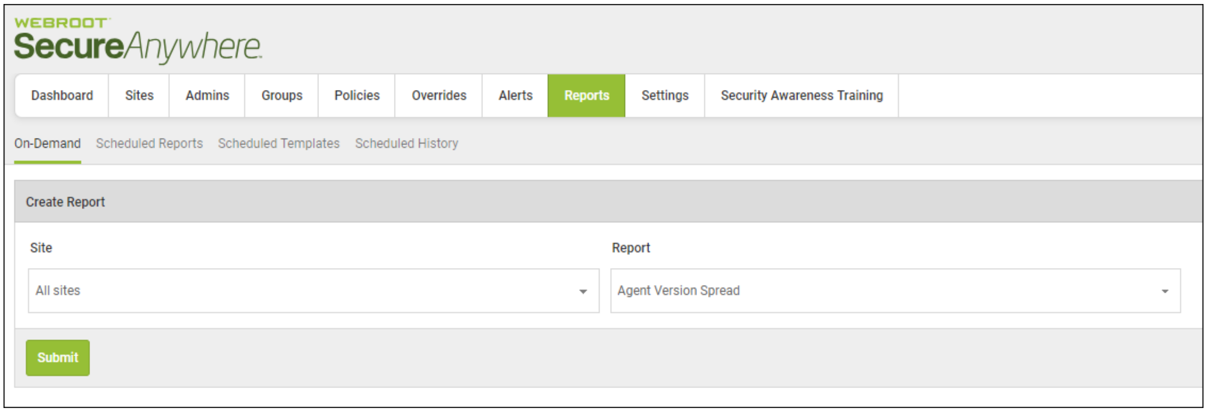


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Inactive |
| Protected | Haymont Tires | 3 | 9 | Inactive | Inactive |
| Protected | Prestige Direct Sales Solutions | 11 | 25 | Inactive | Inactive |

25 Active Devices 49 Site Seats
0 Trial Active Device: 0 Trial Site Seats

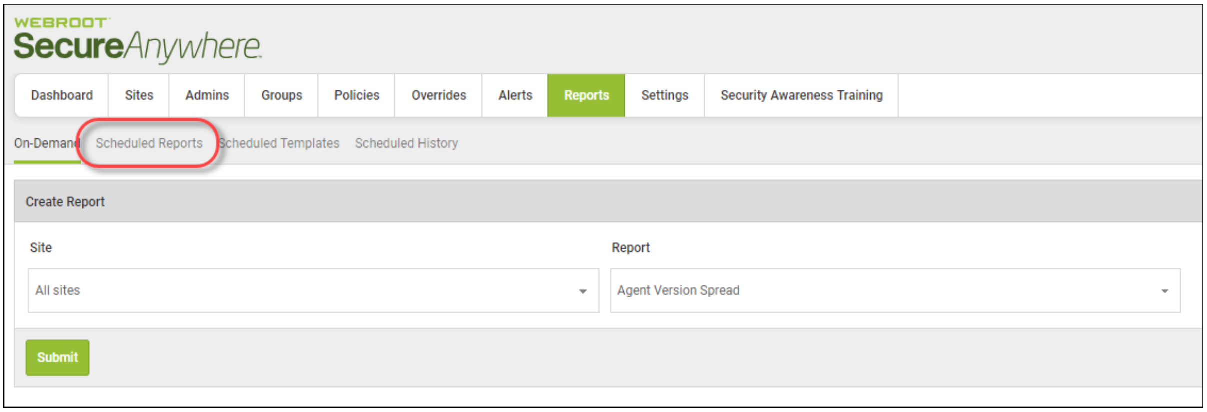
The system displays the Reports tab with the On-Demand tab active.



Site: All sites

Report: Agent Version Spread

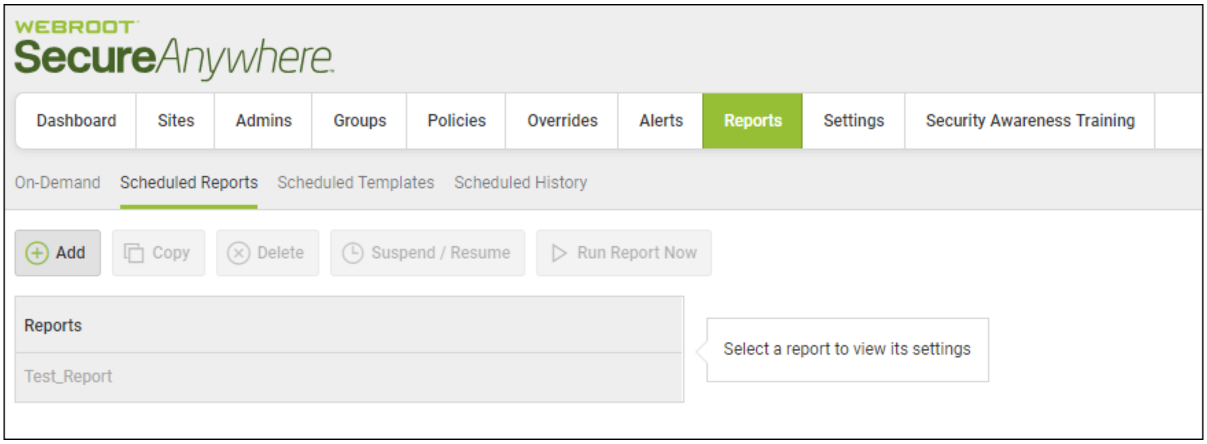
3. Click the **Scheduled Reports** tab.



Site: All sites

Report: Agent Version Spread

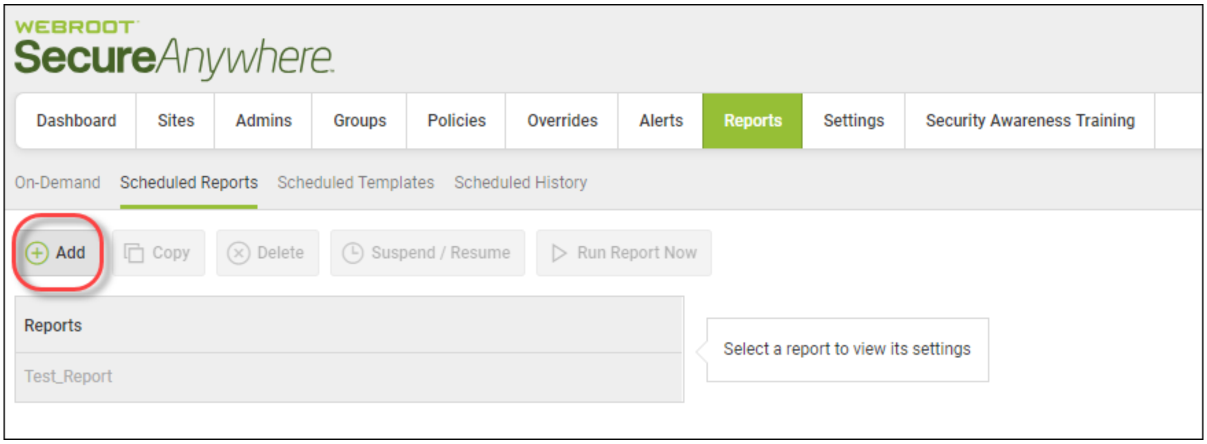
The Scheduled Reports tab displays.



| Reports |
|---|
| Test_Report |

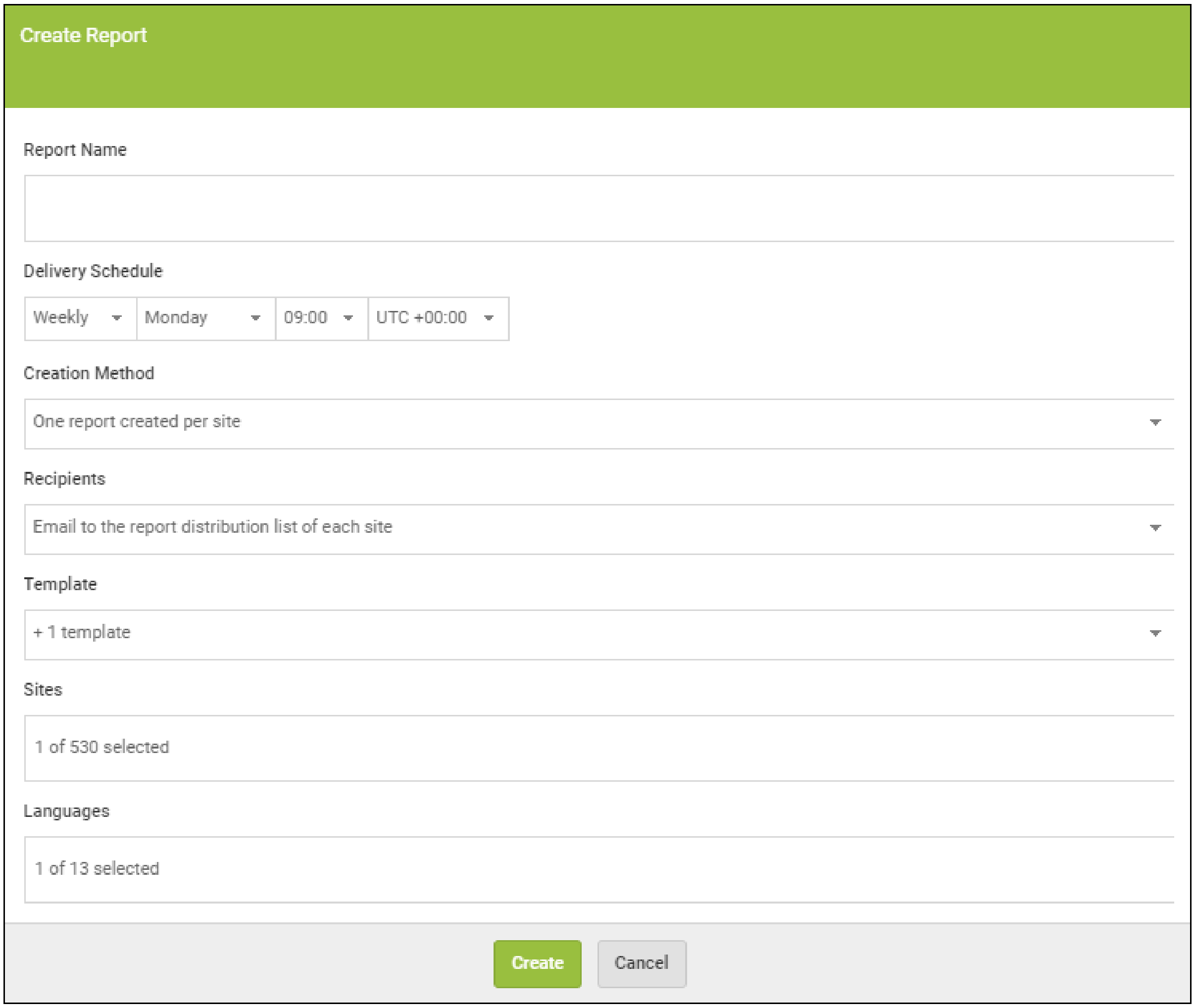
Select a report to view its settings

4. Click the **Add** button.



Select a report to view its settings

The Create Report window displays.



Create Report

Report Name

Delivery Schedule

Weekly ▾ Monday ▾ 09:00 ▾ UTC +00:00 ▾

Creation Method

One report created per site ▾

Recipients

Email to the report distribution list of each site ▾

Template

+ 1 template ▾

Sites

1 of 530 selected

Languages

1 of 13 selected

5. In the Report Name field, enter an identifier for the report, for example, *Weekly Summary Report*.
6. From the Delivery Schedule drop-down menus, create a schedule to run reports at regular intervals and deliver to the inbox of stakeholders or run a report as the information is needed and distribute accordingly.
   - **Daily** — Runs ever day at the time you specify.
   - **Weekly** — Runs weekly at the day and time you specify.
   - **Monthly** — Runs monthly at the date and time you specify.

**Note:** The time selected for the schedule is in UTC and not relative to the user time zone.

7. In the Creating Method field, create reports to deliver the information to targeted recipients either as an aggregate of selected sites from your deployment, or on an individual site basis. Select one of the following:
   - **Create one report for each selected site**
   - **Create one report containing combined data from all selected sites**
8. From the Recipients drop-down menu, select one of the following to set up a list of regular site recipients or add specific email addresses to deliver to:
   - **Mail to the report distribution list of each site**
   - **Mail to static email addresses provided manually**
   - **Mail to both options above**

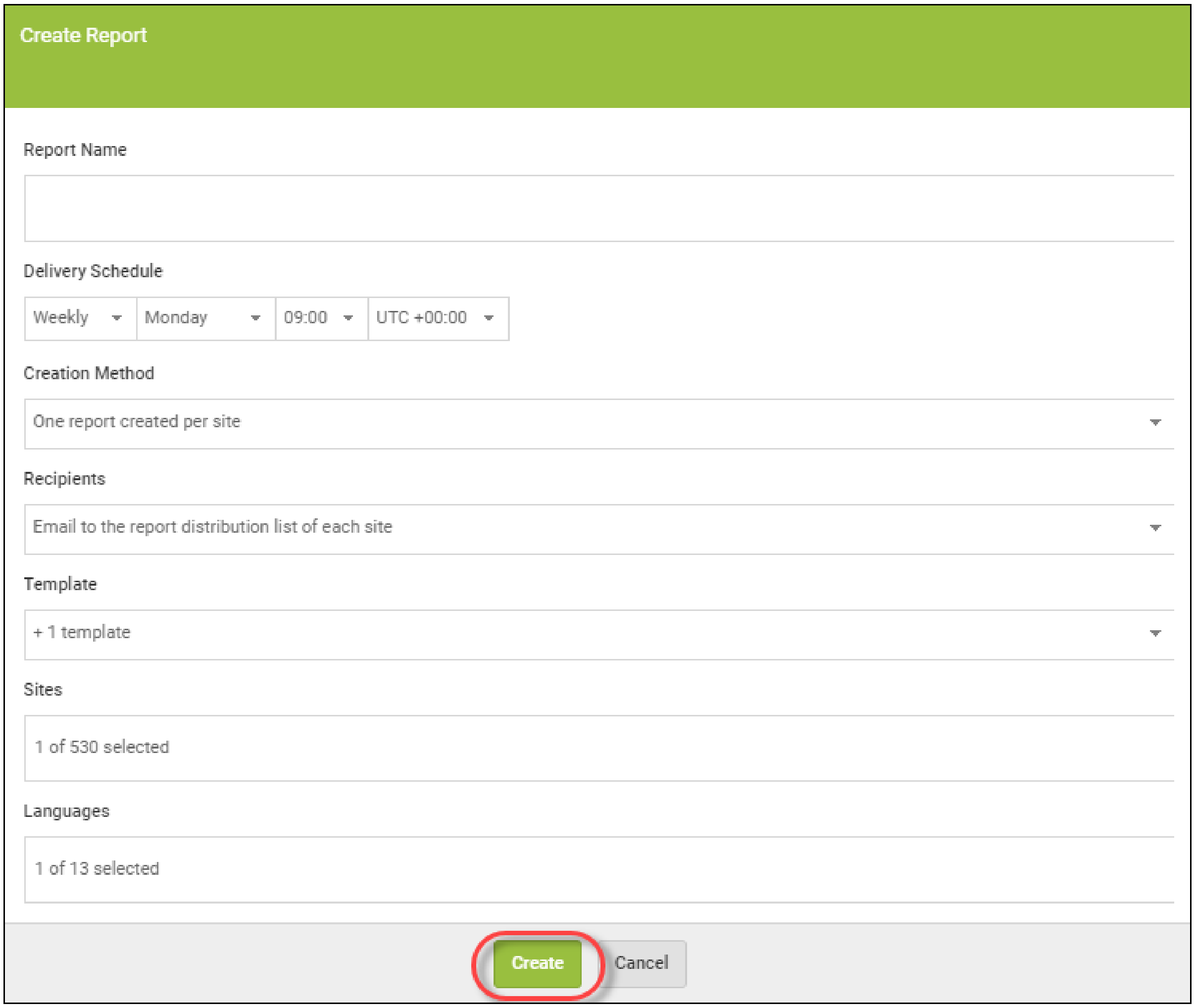
> **Note:** Report Distribution List is a new field which can be modified by selecting to edit site against each site on the sites page. All existing sites have been pre-populated with the emails of all admins already present on that site.

9. From the Templates drop-down menu, select the data template to be included in the report.
10. In the Sites field, click in the field and select the sites to be included in the report.
11. In the Languages field, click in the field and select the languages for the reports to be created in.

    Any default text, such as graph axes and chart titles will be provided in the selected language. If multiple languages are selected, then one report per language will be created. In addition to English, the language options are:

| | | |
|---|---|---|
| German | Turkish | Spanish |
| French | Italian | Japanese |
| Korean | Dutch | Portuguese |
| Russian | Chinese (Simplified) | Chinese (Traditional) |

12. When you're done, click the **Create** button.



Create Report

Report Name

Delivery Schedule

Weekly | Monday | 09:00 | UTC +00:00

Creation Method

One report created per site

Recipients

Email to the report distribution list of each site

Template

+ 1 template

Sites

1 of 530 selected

Languages

1 of 13 selected

# Generating Reports

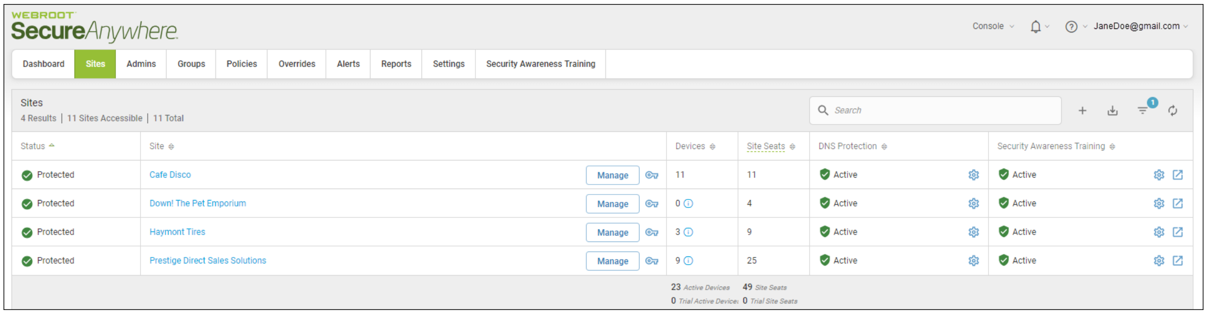
At any time you can access a report outside of the set schedule by using the Run report now tool. This tool offers instant report scheduling with the ability to apply one-off overrides to the creation method and distribution list.

You can change the report to aggregate information across sites or report on individual sites and customize the recipients — without permanent changes to the ongoing schedule. Alternatively, you can run the report exactly as it would have on schedule.

**To generate a report:**

1. Log in to the management console.

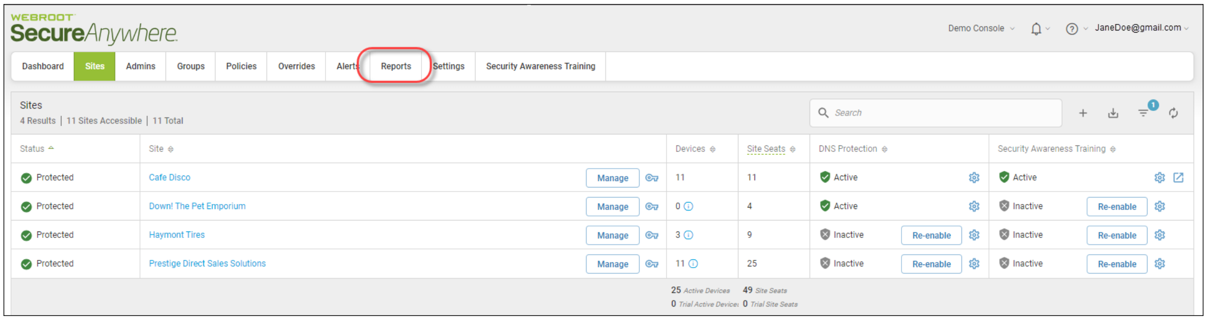
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

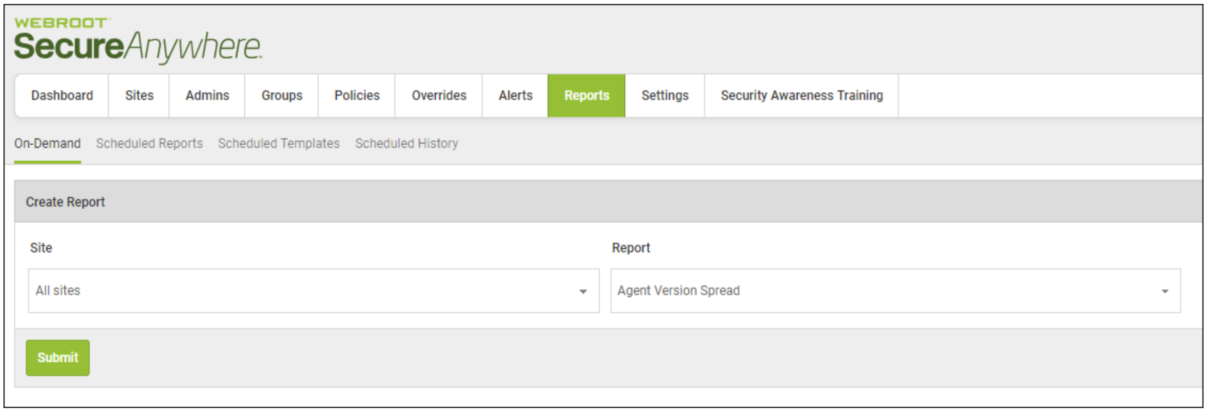
2. Click the **Reports** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Inactive |
| Protected | Haymont Tires | 3 | 9 | Inactive | Inactive |
| Protected | Prestige Direct Sales Solutions | 11 | 25 | Inactive | Inactive |
| | | 25 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

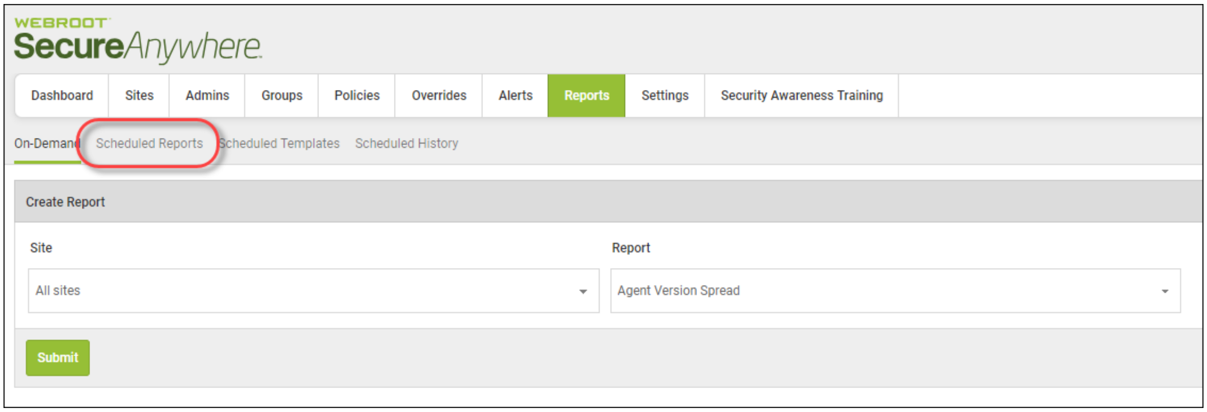
   The system displays the Reports pane with the On-Demand tab active.



Site: All sites

Report: Agent Version Spread

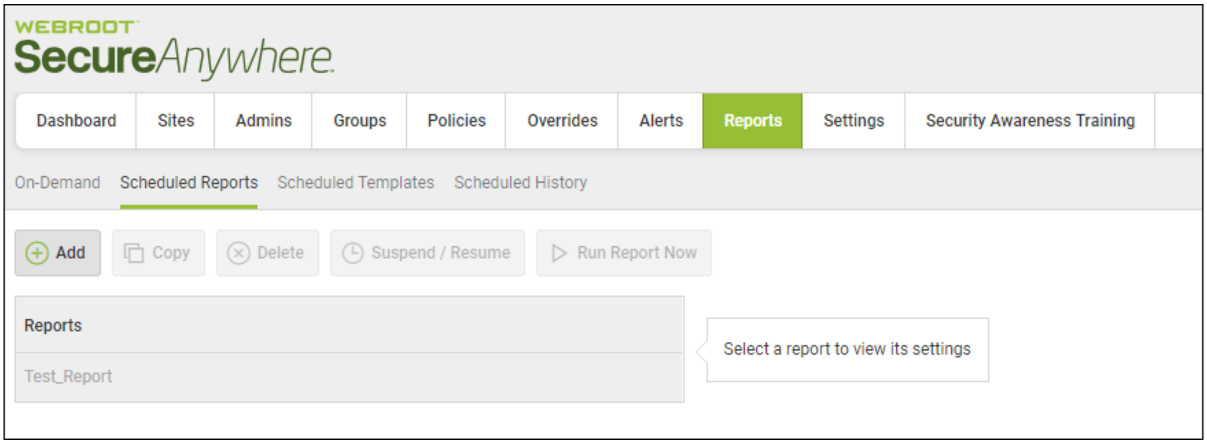
3. Click the **Scheduled Reports** tab.



Site: All sites

Report: Agent Version Spread

The Scheduled Reports tab displays.

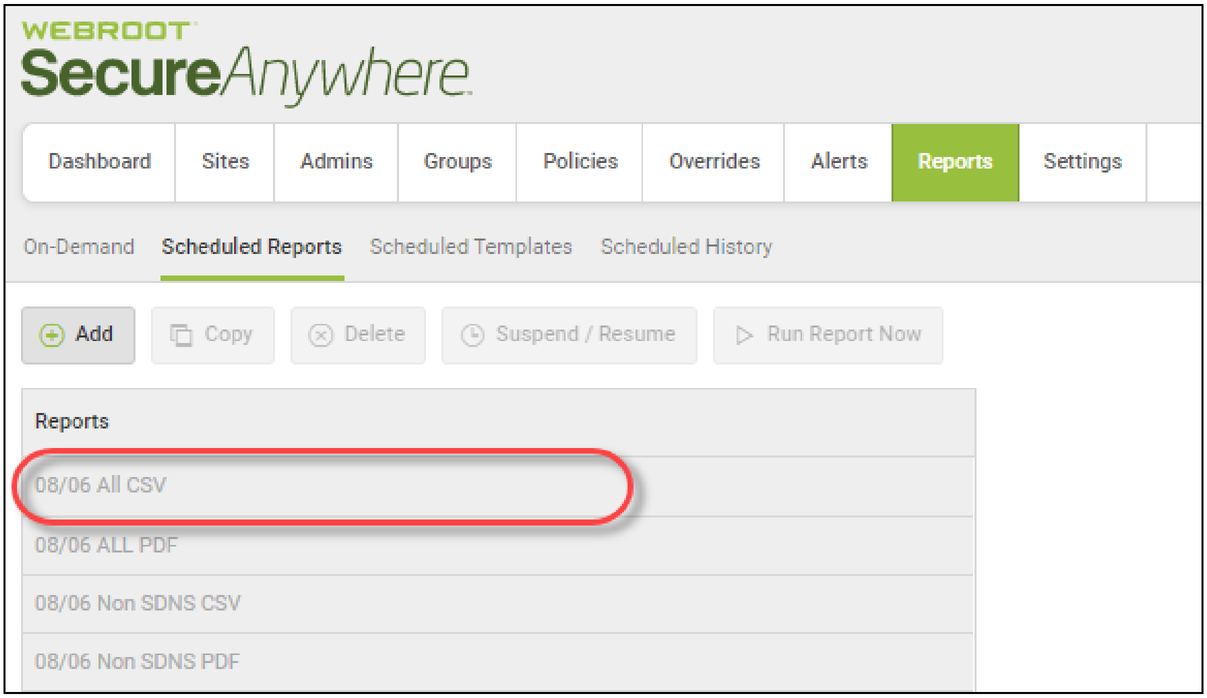


Reports

Test_Report

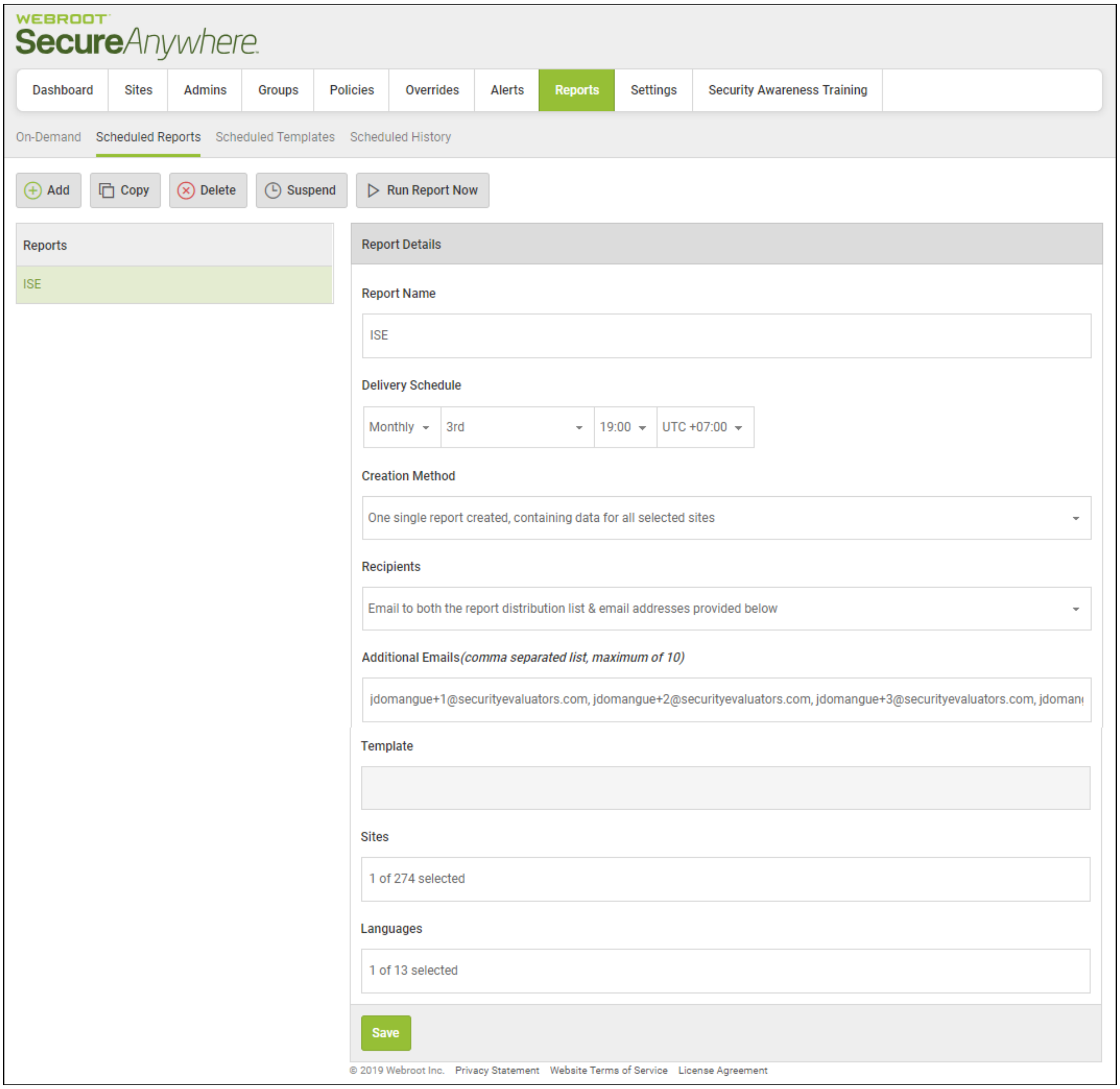
Select a report to view its settings

4. Click the name of the report that you want to run.



| Reports |
|---|
| 08/06 All CSV |
| 08/06 ALL PDF |
| 08/06 Non SDNS CSV |
| 08/06 Non SDNS PDF |

The Report Details pane displays.



Report Name

ISE

Delivery Schedule

Monthly | 3rd | 19:00 | UTC +07:00

Creation Method

One single report created, containing data for all selected sites

Recipients

Email to both the report distribution list & email addresses provided below

Additional Emails*(comma separated list, maximum of 10)*

jdomangue+1@securityevaluators.com, jdomangue+2@securityevaluators.com, jdomangue+3@securityevaluators.com, jdomang

Template

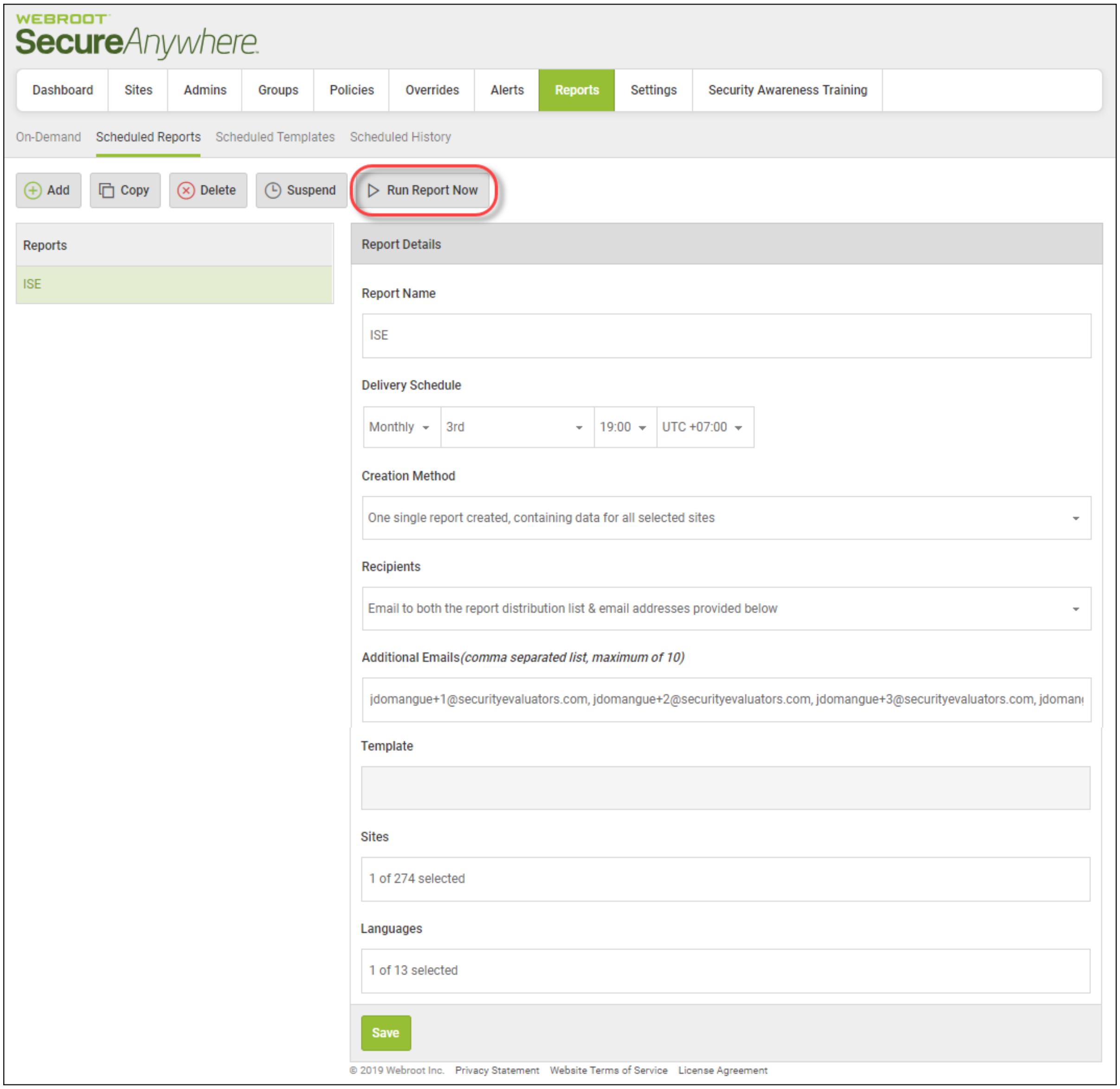
Sites

1 of 274 selected

Languages

1 of 13 selected

5. Update report details as needed, then click the **Run Report Now** button.



Report Name: ISE

Delivery Schedule: Monthly | 3rd | 19:00 | UTC +07:00

Creation Method: One single report created, containing data for all selected sites

Recipients: Email to both the report distribution list & email addresses provided below

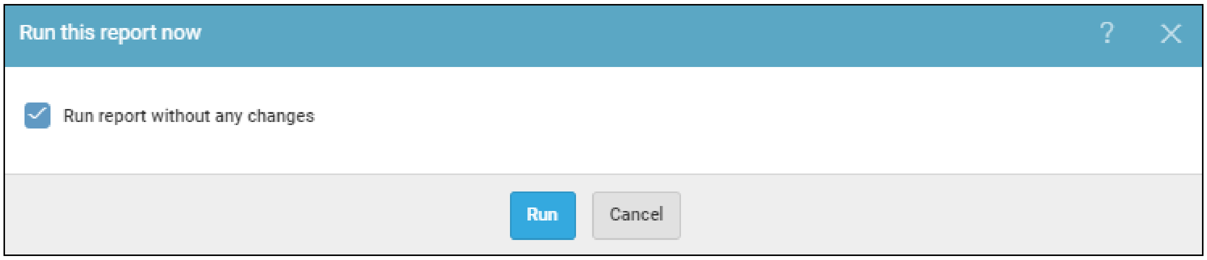
Additional Emails *(comma separated list, maximum of 10)*: jdomangue+1@securityevaluators.com, jdomangue+2@securityevaluators.com, jdomangue+3@securityevaluators.com, jdomang

Template:

Sites: 1 of 274 selected

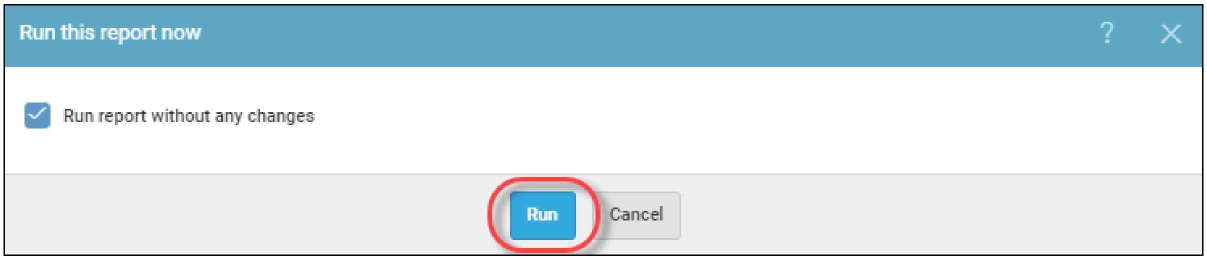
Languages: 1 of 13 selected

The Run this report now window displays.



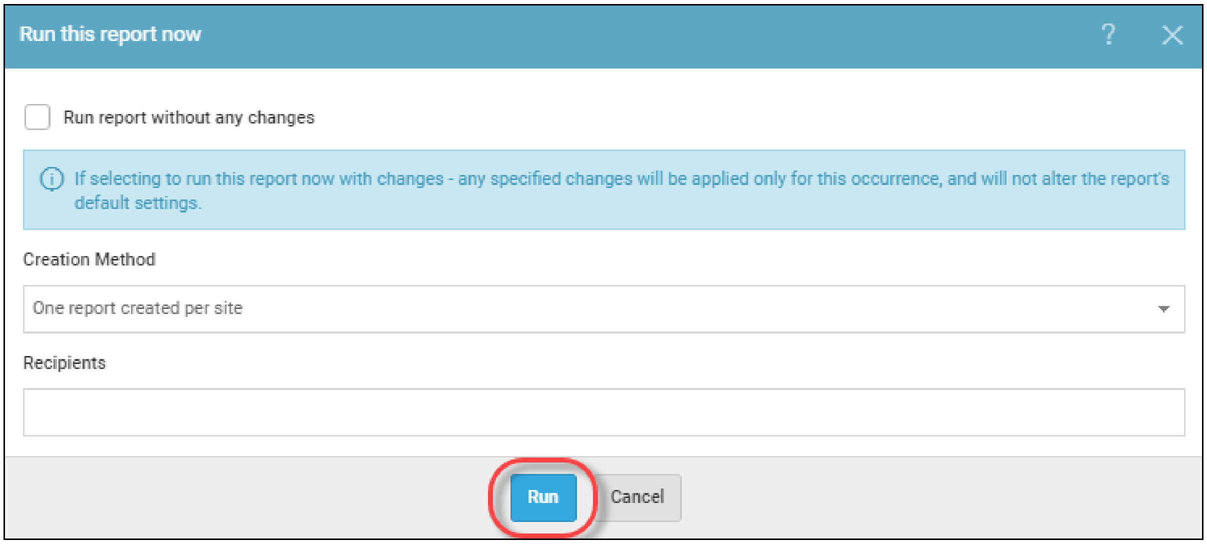
☑ Run report without any changes

6. Do one of the following:
   - To run the report without any changes, click the **Run** button.



☑ Run report without any changes

   - To run the report with changes, deselect the **Run report without any changes** checkbox, select the creation method, and enter the name of any recipients for the report, then click the **Run** button



□ Run report without any changes

ⓘ If selecting to run this report now with changes - any specified changes will be applied only for this occurrence, and will not alter the report's default settings.

Creation Method

One report created per site

Recipients

# Generating On-Demand Reports

If you want to run a report and display the information on your screen while you're in the management console, then follow this procedure to generate an on-demand report.

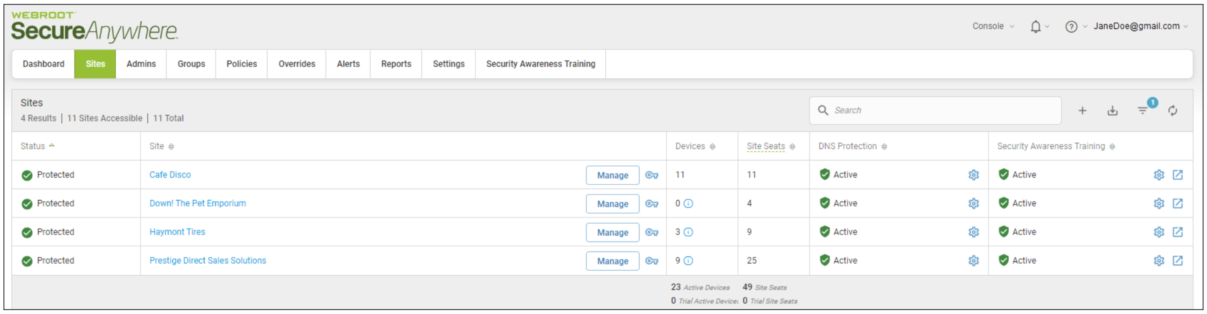
To generate a report and create a CSV file or a PDF, see *Generating Reports on page 448*.

**Note:** Limited Admins can run On Demand Reports for the sites that have access to.

**To generate an on-demand report:**

1. Log in to the management console.

   The management console displays with the Sites tab active.

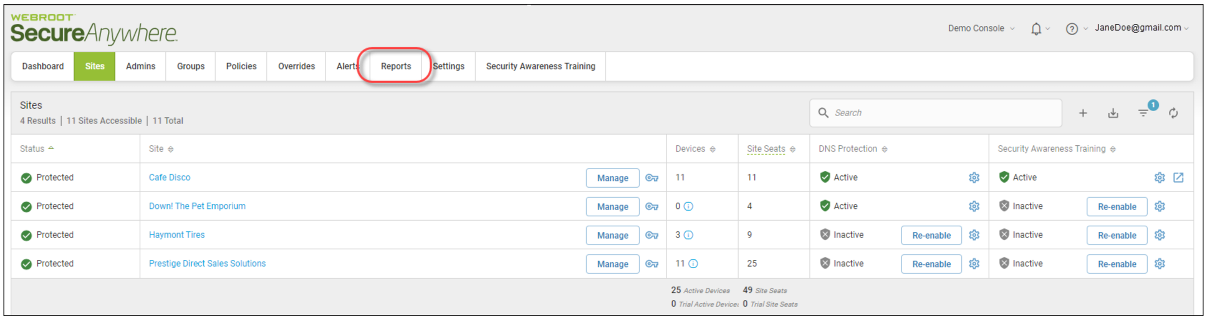


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |

23 Active Devices 49 Site Seats
0 Trial Active Device: 0 Trial Site Seats

2. Click the **Reports** tab.

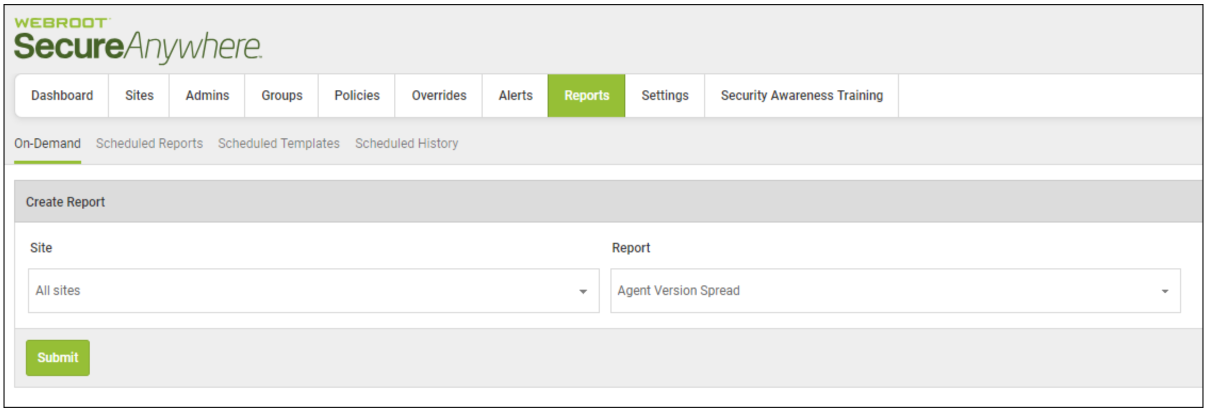


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Inactive Re-enable |
| Protected | Haymont Tires | 3 | 9 | Inactive Re-enable | Inactive Re-enable |
| Protected | Prestige Direct Sales Solutions | 11 | 25 | Inactive Re-enable | Inactive Re-enable |

25 Active Devices 49 Site Seats
0 Trial Active Device: 0 Trial Site Seats

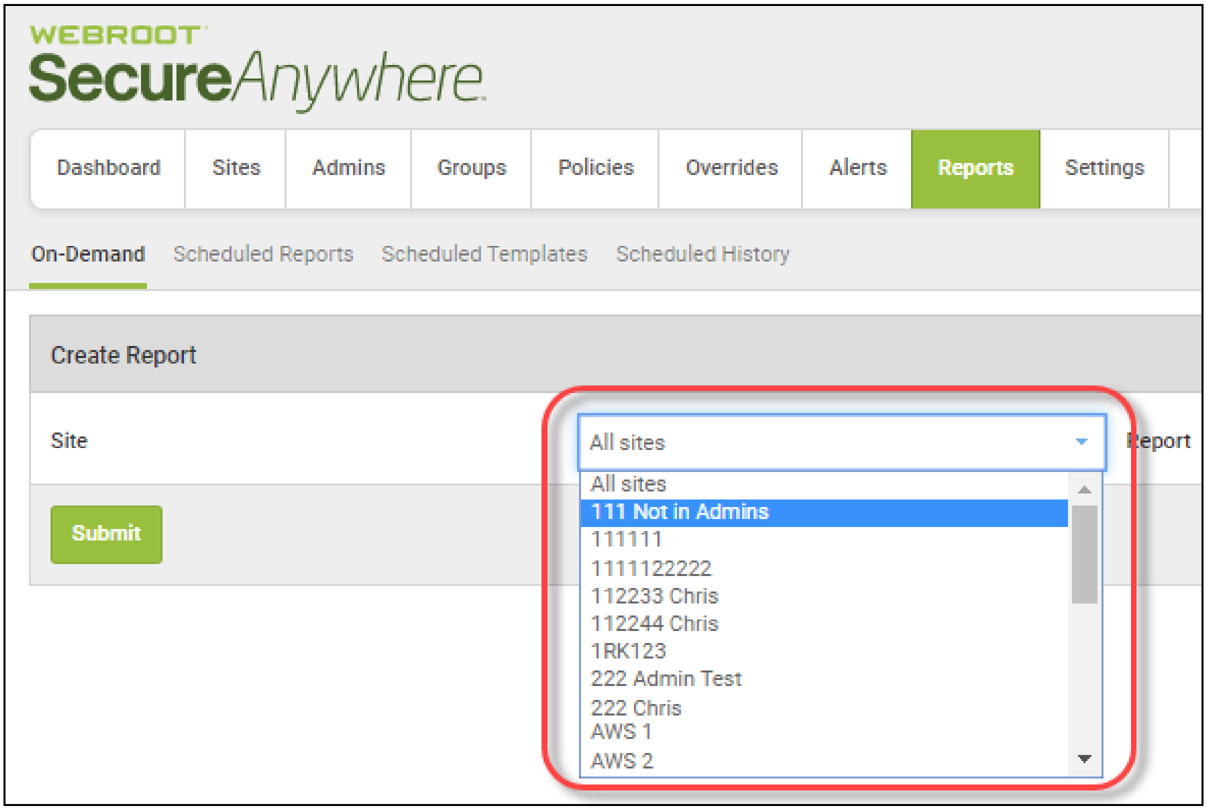
The system displays the Reports pane with the On-Demand tab active.



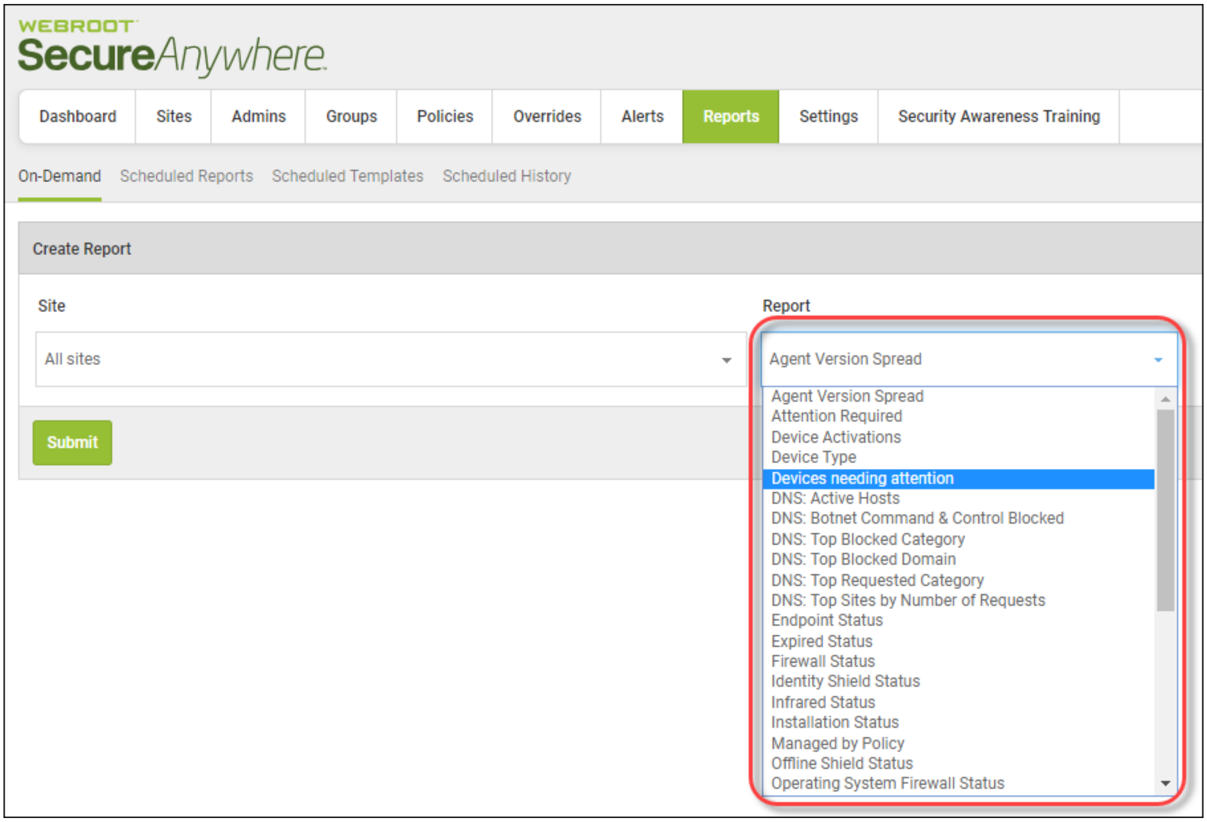
Site: All sites

Report: Agent Version Spread

3. From the Sites drop-down menu, select the site for which you want to generate the report.



4. From the Report drop-down menu, select the report you want to generate.



The following table describes all the reporting options.

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Agent Version Spread** | Shows which version of the Webroot Secure Anywhere agent each Endpoint device is using. | Bar, Column, Pie | N/A |
| **All Threats Seen** | Locates detected threats. This report lists threats by file name, along with when and where SecureAnywhere detected them. | Spreadsheet | Use the Date Picker from the Period drop-down menu to select a date range anywhere from the last seven days to the last 90 days. Additionally, you can create a custom date range. |
| **All Undetermined Software Seen** | Locates files classified as Undetermined, which displays legitimate, but also exhibits questionable behavior, typically executable files, that cannot be classified as either safe or as malware. | Spreadsheet | Use the Date Picker from the Period drop-down menu to select a date range anywhere from the last seven days to the last 90 days. Additionally, you can create a custom date range. |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Attention Required** | Provides a list of all Endpoint devices that have been determined as secure, and a list of those that require attention. | Bar, Column, Pie | N/A |
| **Device Activations** | Provides a list of all Endpoint devices that have been activated during the time period that you selected. | Area, Area Spline, Bar, Column, Line, Spline | 24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days,<br>90 days |
| **Device Type** | Provides a list of the number of Endpoint devices that are PCs or Macs. | Bar, Column, Pie | N/A |
| **Devices Needing Attention** | Displays a list of devices that have the status of Needs Attention. | List | 24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days,<br>90 days |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Devices With Threats Seen On Last Scan** | Displays threats by endpoint location. From the report, you can change the endpoint's policy, run a scan, create an override for a file, or restore a file from quarantine. | Spreadsheet | Use the Date Picker from the Period drop-down menu to select a date range anywhere from the last seven days to the last 90 days. Additionally, you can create a custom date range. |
| **Devices With Undetermined Software On Last Scan** | Locates devices with files classified as Undetermined, which displays legitimate, but also exhibits questionable behavior, typically executable files, that cannot be classified as either safe or as malware. | Spreadsheet | Use the Date Picker from the Period drop-down menu to select a date range anywhere from the last seven days to the last 90 days. Additionally, you can create a custom date range. |
| **Endpoint Status** | Shows the number of clean Endpoint devices, and the number of infected Endpoint devices on your sites. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Evasion Shield - Script Detections** | Locates detected threats. This report lists threats by name, along with when and where Webroot detected them. | Spreadsheet | 24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days,<br>90 days |
| **Evasion Shield - Script Protection Status** | Shows which of your Endpoint Devices have the Script Protection option:<br>• Detect and Remediate<br>• Detect and Report<br>• Off<br>• Unsupported | Bar with drill-down to sites and endpoints | N/A |
| **Expired Status** | Shows the number of Endpoint devices that are Active, and the number of Endpoint devices that have an Expired state. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT<br>DESCRIPTIO N | CHART TYPE S | TIME PERIOD S |
|---|---|---|---|
| **Firewall Status** | Shows which of your Endpoint Devices have the Firewall option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Identity Shield Status** | Shows how many of your Endpoint Devices have the Identity Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTIO N | CHART TYPE S | TIME PERIOD S |
|---|---|---|---|
| **Infrared Status** | Shows which of your Endpoint devices have the Enable Webroot Infrared option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Installation Status** | Shows which of your Endpoint devices have the Webroot Secure Anywhere product installed and which ones have had the product uninstalled. | Bar, Column, Pie | N/A |
| **Managed by Policy** | Shows how many of your Endpoint devices are being managed by a policy you have created and how many are in an unmanaged state. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT<br>DESCRIPTIO N | CHART TYPE S | TIME PERIOD S |
|---|---|---|---|
| **Offline Shield Status** | Shows how many of your Endpoint devices have the Offline Shield option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Operating System Firewall Status** | Shows which of your Endpoint devices have an operating system Firewall option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Operating System Language** | Shows which Operating system language your Endpoint devices are using. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Operating System Platform** | Shows which Operating system platform, from 32 bit, 64 bit, or Unknown, that your Endpoint devices are using. | Bar, Column, Pie | N/A |
| **Phishing Shield Status** | Shows how many of your Endpoint devices have the Phishing Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |
| **Primary Browser** | Shows the Primary Web Browser used by each of your Endpoint devices. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Realtime Shield Status** | Shows how many of your Endpoint devices have the Realtime Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |
| **Remediation Status** | Shows how many of your Endpoint devices have the Remediation status:<br>• Disabled<br>• Enabled<br>To disable the Remediation status, the **Automatically quarantine previously blocked files** option, must be turned off. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Report Summary** | Provides a number of overall counts that effectively summarize site or deployment information:<br>• Number of active devices<br>• Number of available seats Endpoints currently needing attention<br>• Endpoints which encountered threats (Last ‘n’ days)<br>• Total Threats seen (Last ‘n’ days)<br>• Number of Endpoints Seen (Last ‘n’ days)<br>• Number of Endpoints Not Seen (Last ‘n’ days)<br>• Number of Endpoints Seen | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT<br>DESCRIPTIO<br>N | CHART TYPE<br>S | TIME PERIOD<br>S |
|---|---|---|---|
| | (All Time) | | |
| **Rootkit Shield Status** | Shows how many of your Endpoint devices have the Rootkit Shield option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Scheduled Scans Status** | Shows how many of your Endpoint devices have a Scheduled Scan:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Silent Mode** | Shows how many of your Endpoint devices have the Silent Audit option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Threat Detection History** | Shows the history over your selected time period, of all threats that have been detected on your Endpoint devices. | Area, Area Spline, Bar, Column, Line, Spline | 24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days |
| **USB Shield Status** | Shows how many of your Endpoint devices have the USB Shield option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |

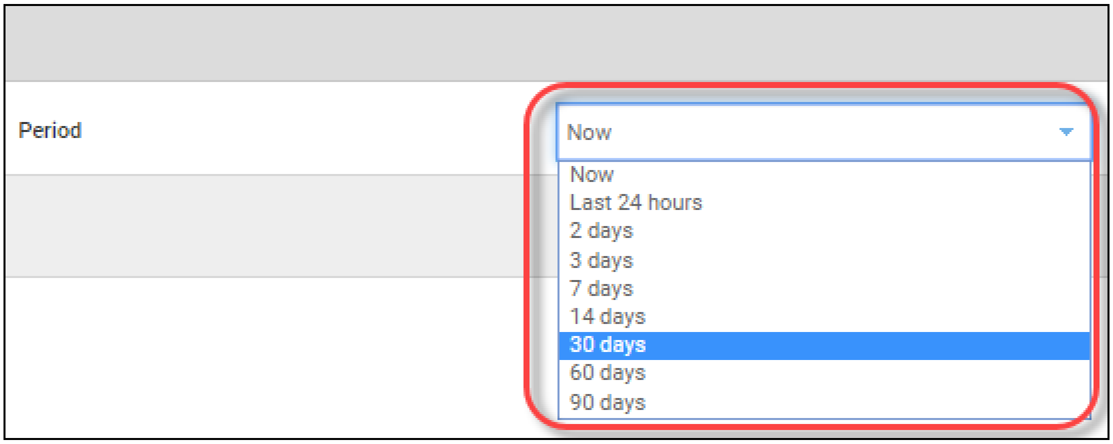
| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Virtual Machine** | Shows how many of your Endpoint devices have been classified as Virtual Machines (VMs). | Bar, Column, Pie | N/A |
| **Web Threat Shield Blocked URL History** | Displays a history of the URLs that have been blocked by Webroot's Web Threat Shield. | Spreadsheet | Use the Date Picker from the Period drop-down menu to select a date range anywhere from the last seven days to the last 90 days. Additionally, you can create a custom date range. |

| DATA FIELD | REPORT<br>DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Web Threat Shield Blocked URLs** | Displays a list of of the URLs that have been blocked by Webroot's Web Threat Shield. | Spreadsheet | Use the Date Picker from the Period drop-down menu to select a date range anywhere from the last seven days to the last 90 days. Additionally, you can create a custom date range. |
| **Web Threat Shield Status** | Shows how many of your Endpoint devices have the Web Threat Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |

5. If the report allows you to select a period during which the report should be generated, from the Period drop-down menu, select one of the following periods:

- Last 24 hours
- 2 days
- 3 days
- 7 days
- 14 days
- 30 days

- 60 days
- 90 days

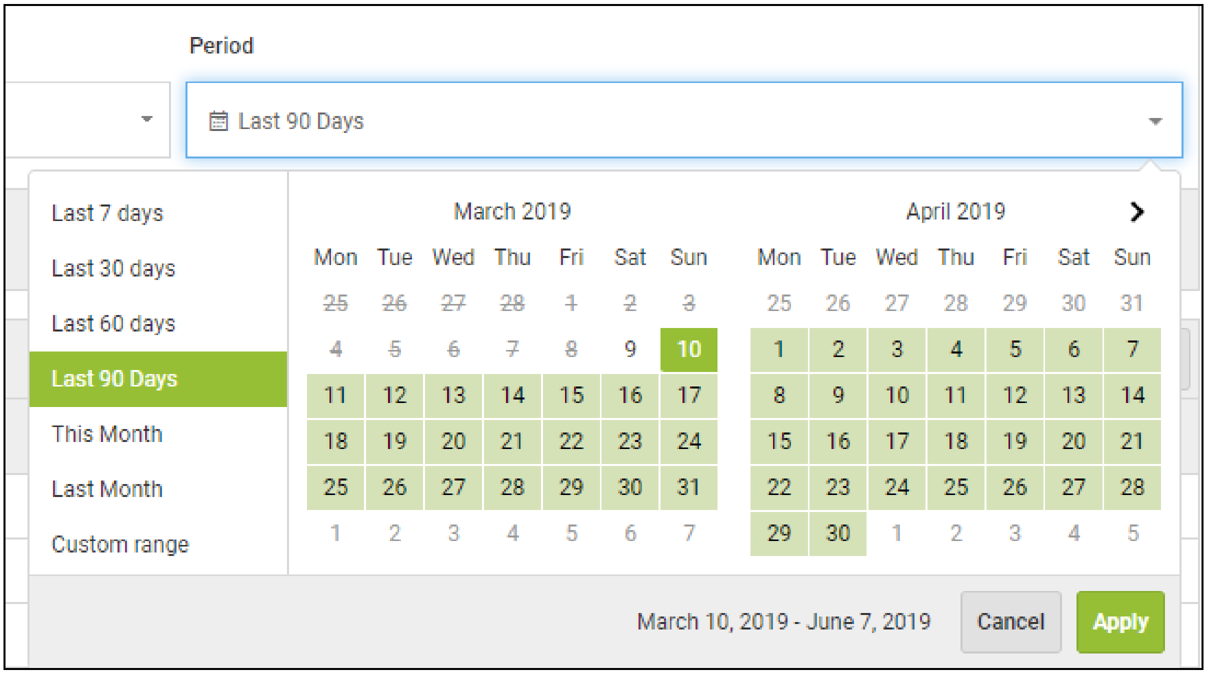


Period

Now

- Now
- Last 24 hours
- 2 days
- 3 days
- 7 days
- 14 days
- 30 days
- 60 days
- 90 days

6. If the report allows you to use the Date Picker function, from the Period drop-down menu, select one of the following date ranges and click the **Apply** button:



Period

Last 90 Days

- Last 7 days
- Last 30 days
- Last 60 days
- Last 90 Days
- This Month
- Last Month
- Custom range

March 2019

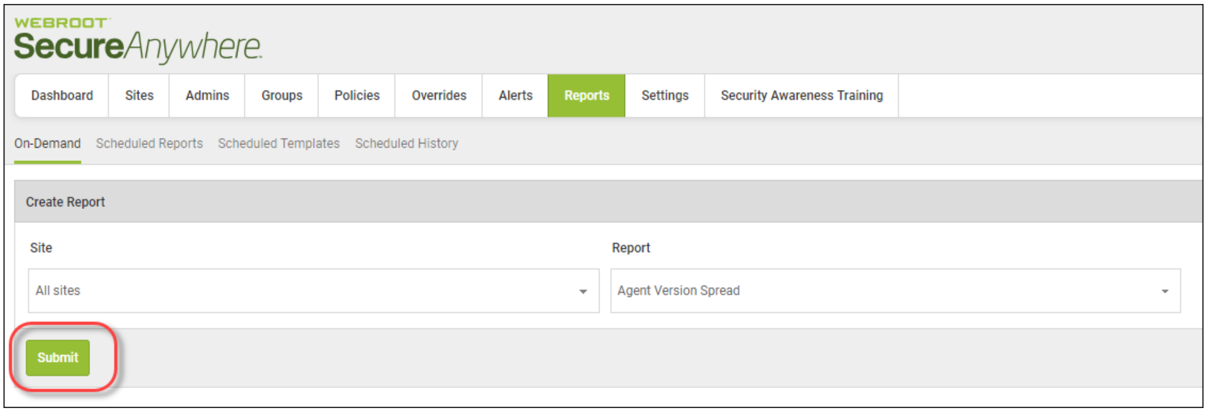
| Mon | Tue | Wed | Thu | Fri | Sat | Sun |
|---|---|---|---|---|---|---|
| ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | ~~1~~ | ~~2~~ | ~~3~~ |
| ~~4~~ | ~~5~~ | ~~6~~ | ~~7~~ | ~~8~~ | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

April 2019

| Mon | Tue | Wed | Thu | Fri | Sat | Sun |
|---|---|---|---|---|---|---|
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 1 | 2 | 3 | 4 | 5 |

March 10, 2019 - June 7, 2019

7. When you're done, click the **Submit** button.

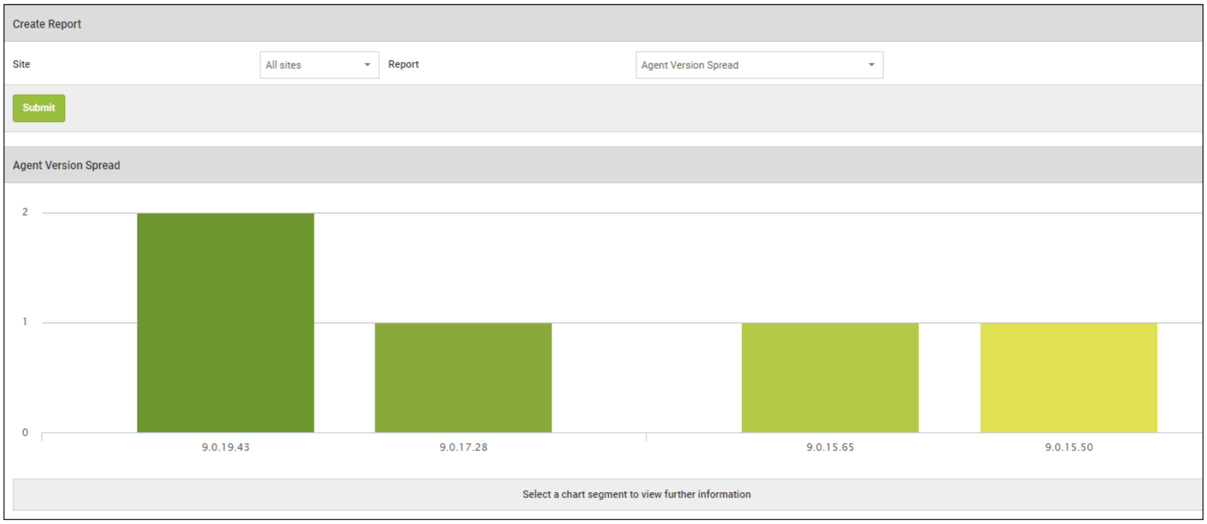


Create Report

Site: All sites

Report: Agent Version Spread

The system displays the report in the console in a graphic format.



Create Report

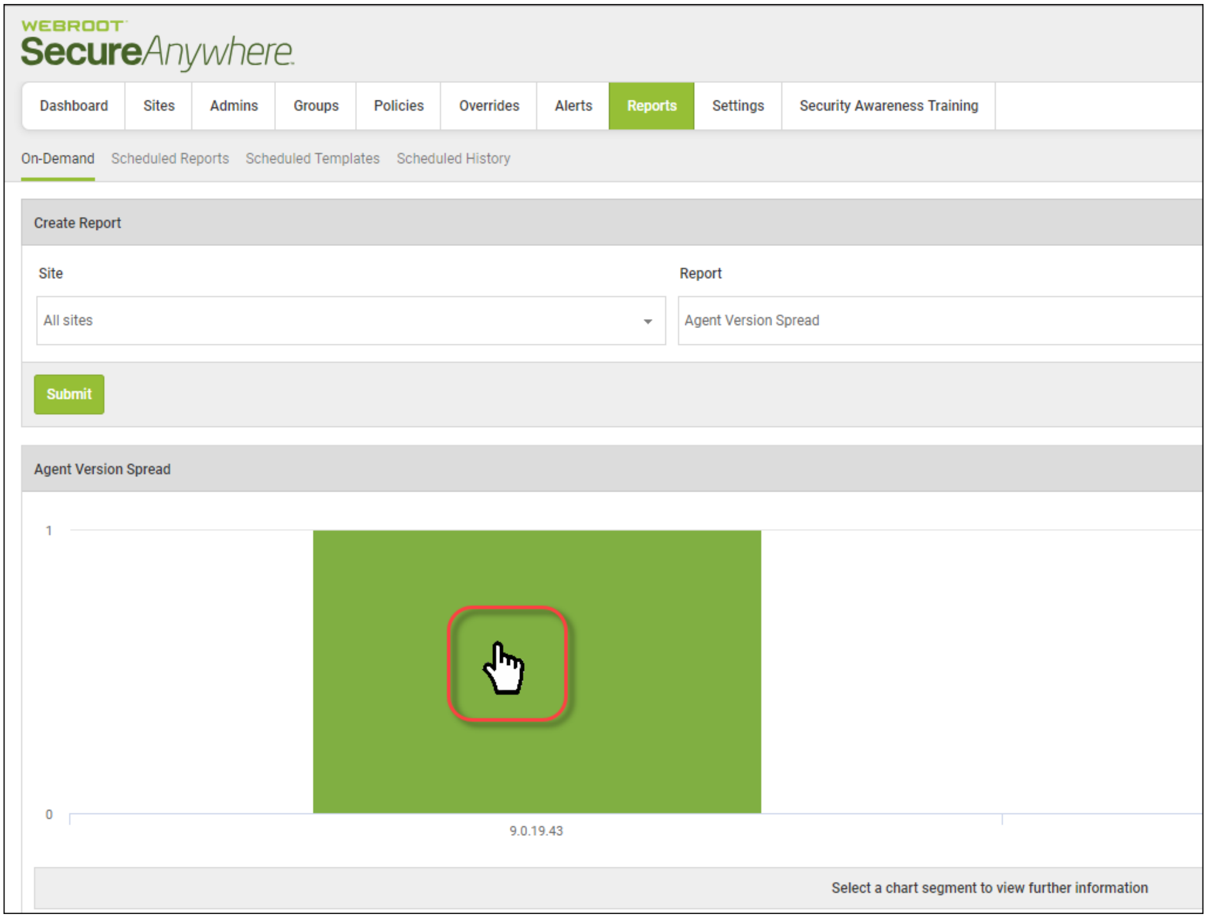
Site: All sites

Report: Agent Version Spread

Agent Version Spread

Select a chart segment to view further information

8. To display information about the report, click on any of the segments.

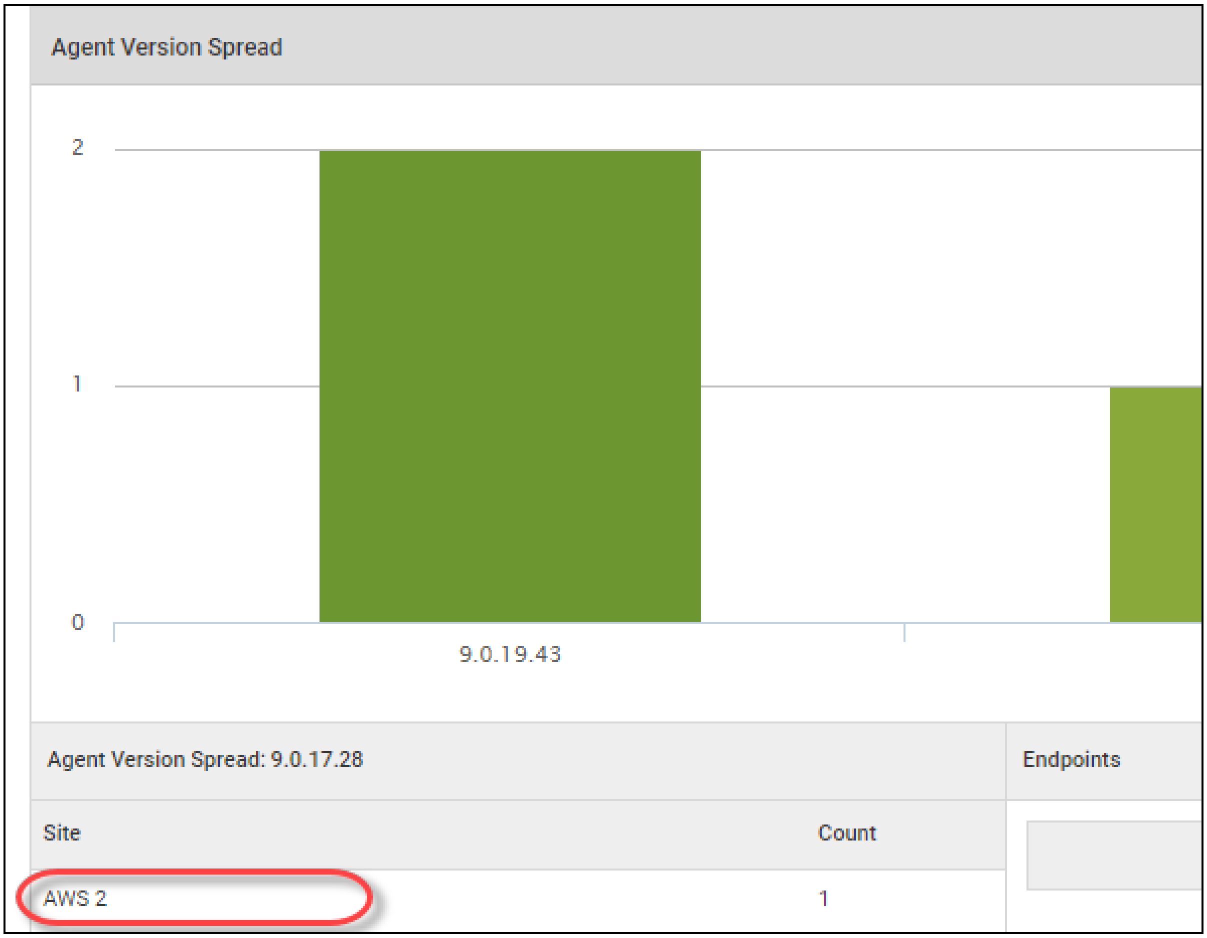


Site: All sites

Report: Agent Version Spread

Select a chart segment to view further information

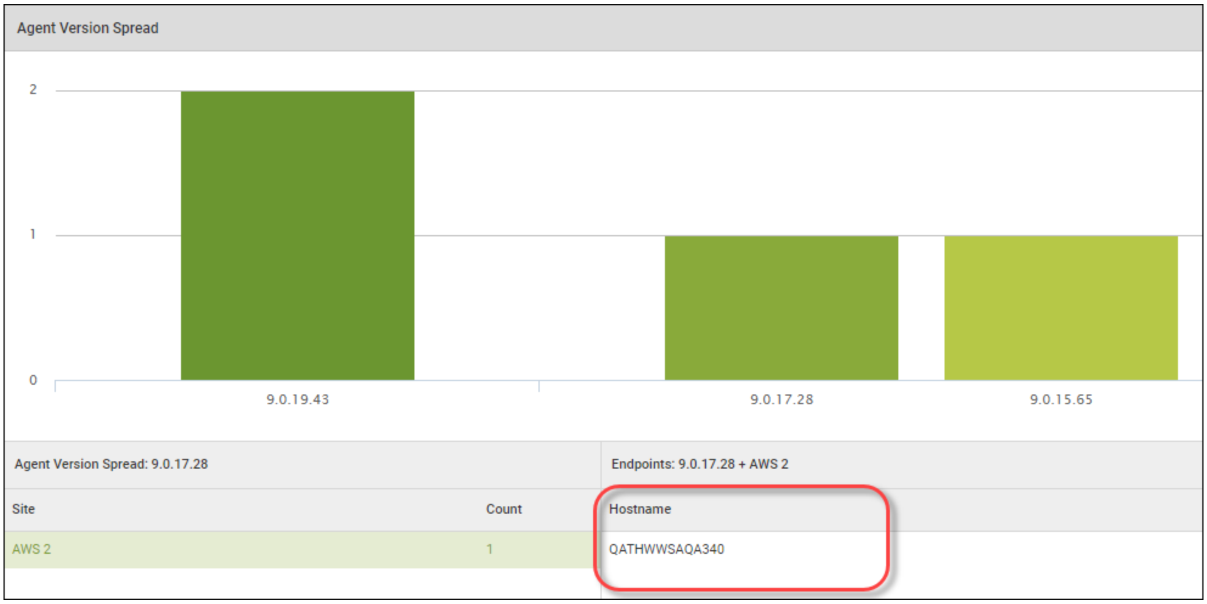
9. In the left panel, click on any site to display additional information about a particular site.



Agent Version Spread: 9.0.17.28

| Site | Count |
|---|---|
| AWS 2 | 1 |

The system displays additional information about that site.



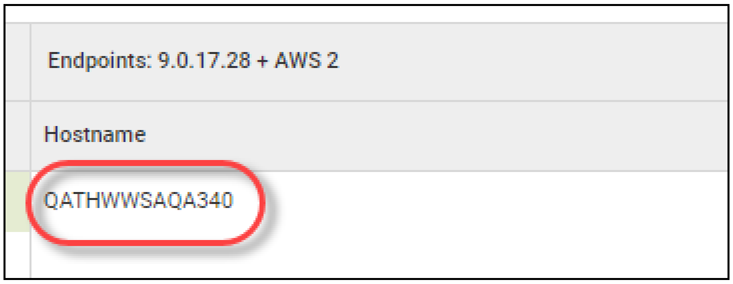
Agent Version Spread: 9.0.17.28

| Site | Count |
|---|---|
| AWS 2 | 1 |

Endpoints: 9.0.17.28 + AWS 2

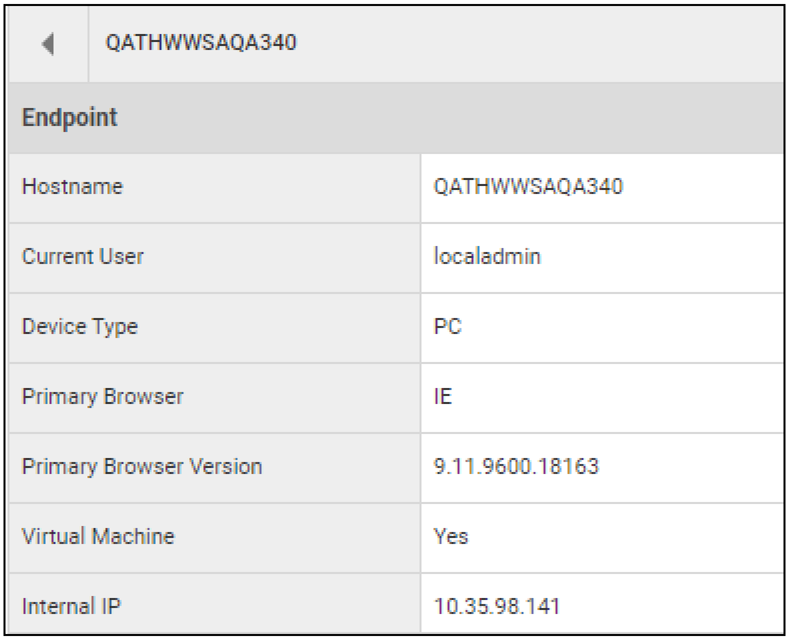
| Hostname |
|---|
| QATHWWSAQA340 |

10. Click on any of the names in the Hostename column to display additional and more specific information about that hostname. Use the scrollbar on the right to view all of the information.



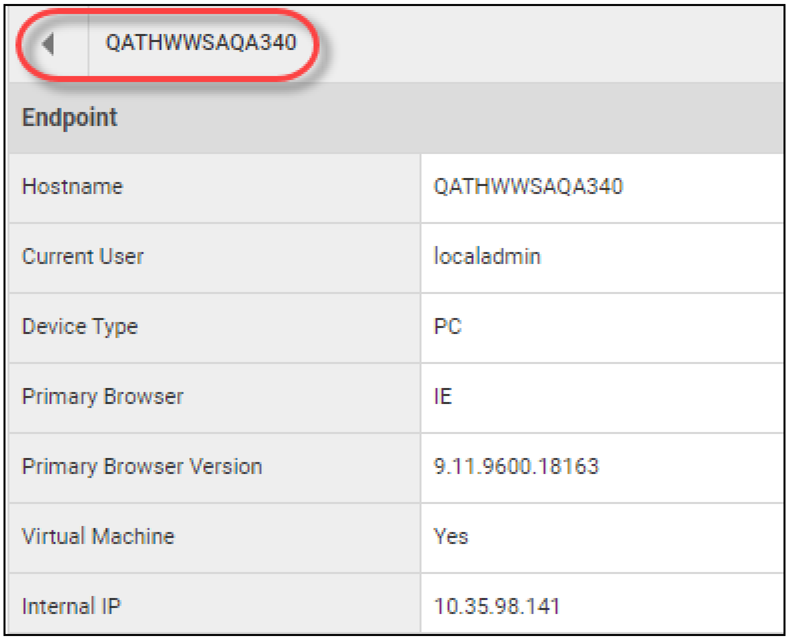
Endpoints: 9.0.17.28 + AWS 2

| Hostname |
|---|
| QATHWWSAQA340 |



| QATHWWSAQA340 | |
|---|---|
| **Endpoint** | |
| Hostname | QATHWWSAQA340 |
| Current User | localadmin |
| Device Type | PC |
| Primary Browser | IE |
| Primary Browser Version | 9.11.9600.18163 |
| Virtual Machine | Yes |
| Internal IP | 10.35.98.141 |

11. When you're done, you can click the **Left** arrow to return to the previous view.



| QATHWWSAQA340 | |
|---|---|
| **Endpoint** | |
| Hostname | QATHWWSAQA340 |
| Current User | localadmin |
| Device Type | PC |
| Primary Browser | IE |
| Primary Browser Version | 9.11.9600.18163 |
| Virtual Machine | Yes |
| Internal IP | 10.35.98.141 |

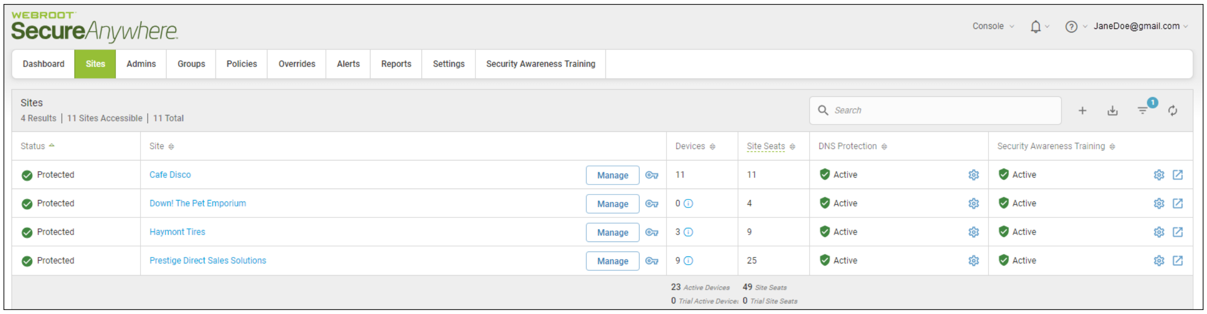
# Creating Report Templates

This scheduled reports feature utilizes a customizable template approach. Easily add or remove pages, select data and time periods to build up a report with the content you need. Default templates will be included which can be modified, copied or deleted as needed. New templates can also be created.

### To create a report template:

1. Log in to the management console.

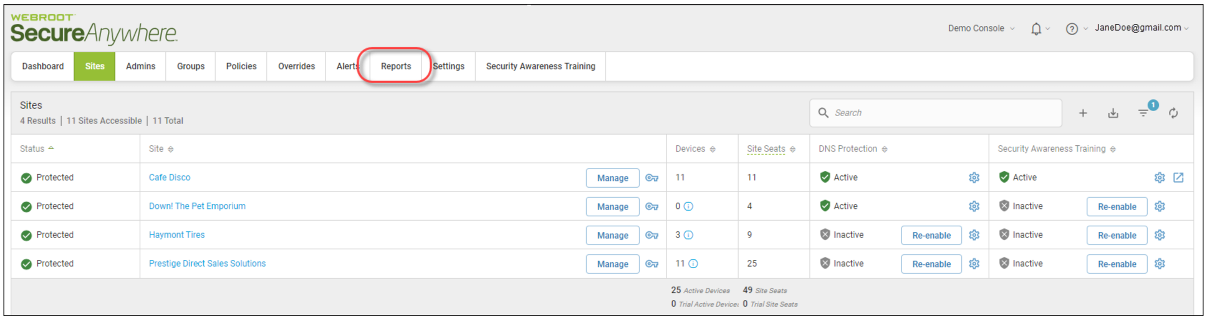
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

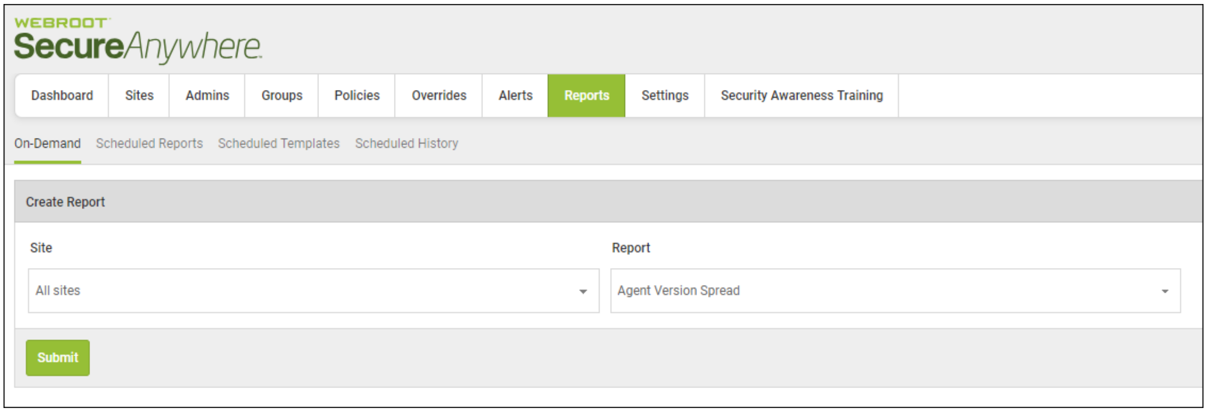
2. Click the **Reports** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Inactive Re-enable |
| Protected | Haymont Tires | 3 | 9 | Inactive Re-enable | Inactive Re-enable |
| Protected | Prestige Direct Sales Solutions | 11 | 25 | Inactive Re-enable | Inactive Re-enable |
| | | 25 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

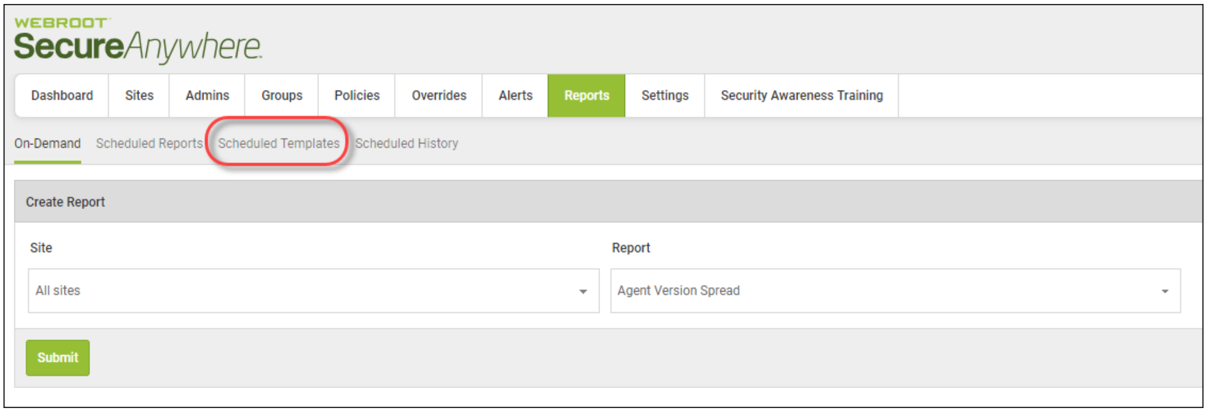
The system displays the Reports pane with the On-Demand tab active.



Site: All sites

Report: Agent Version Spread

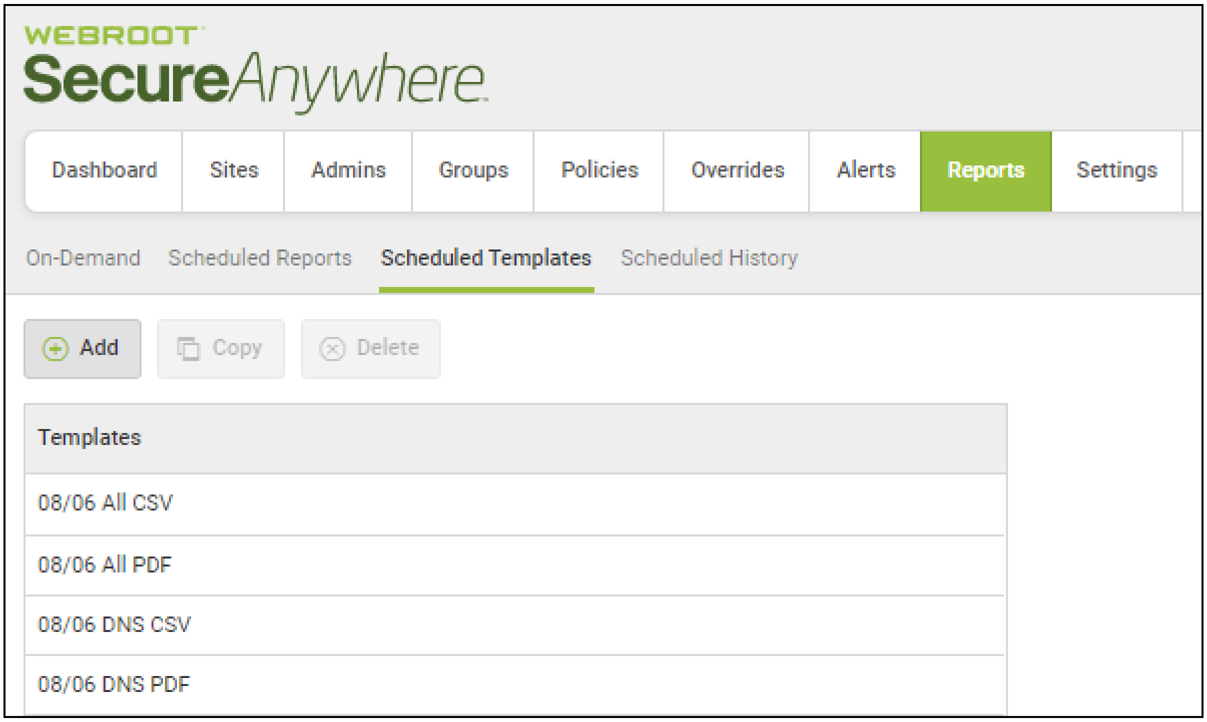
3. Click the **Scheduled Templates** tab.



Site: All sites

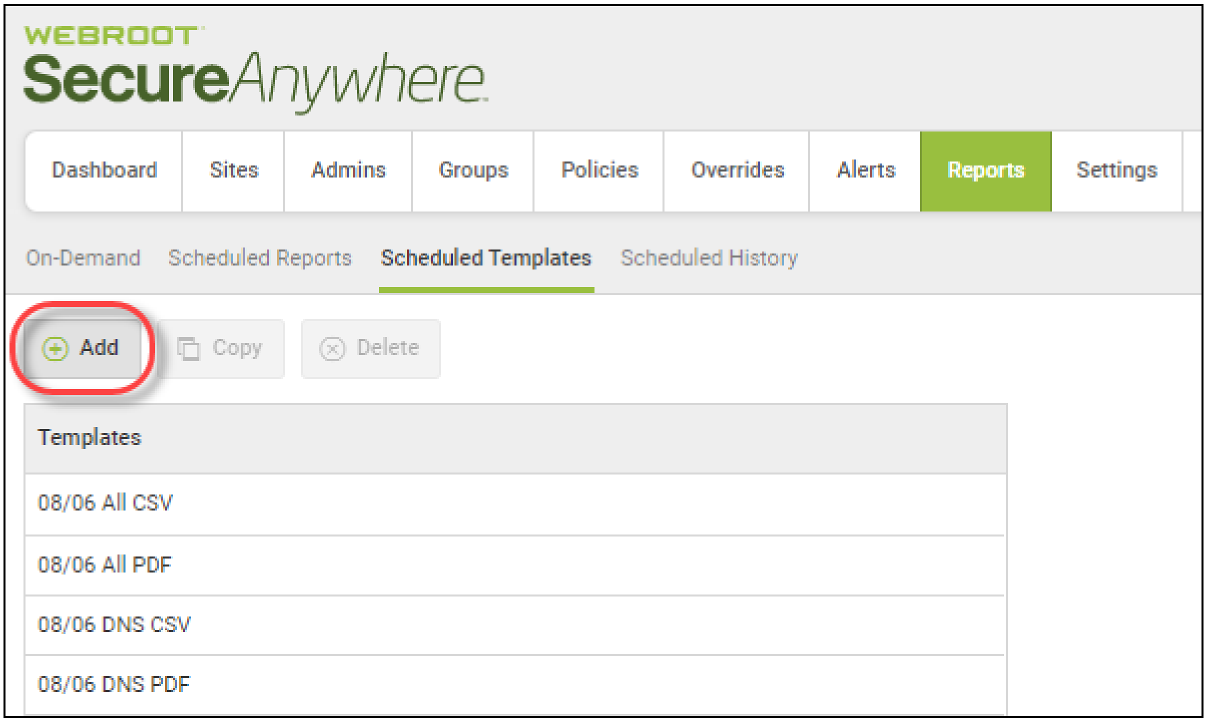
Report: Agent Version Spread

The Scheduled Templates tab displays.



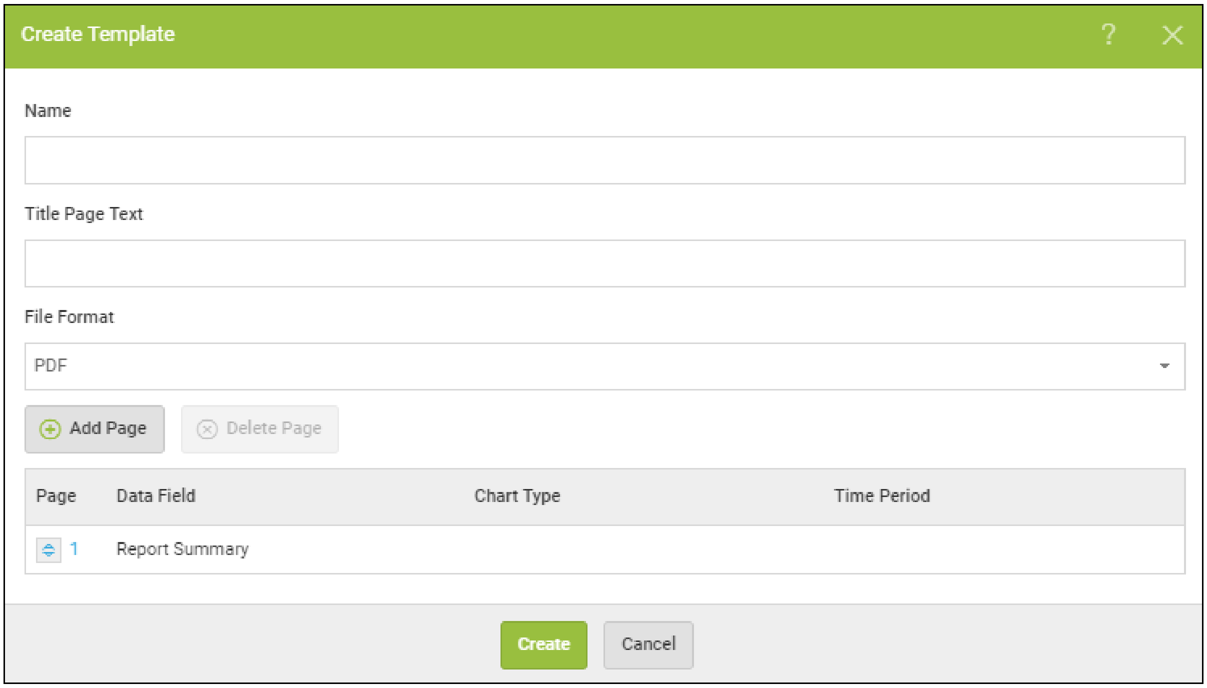
| Templates |
|---|
| 08/06 All CSV |
| 08/06 All PDF |
| 08/06 DNS CSV |
| 08/06 DNS PDF |

4. Click the **Add** button.



| Templates |
|---|
| 08/06 All CSV |
| 08/06 All PDF |
| 08/06 DNS CSV |
| 08/06 DNS PDF |

The Create Template window displays.



File Format

PDF

| Page | Data Field | Chart Type | Time Period |
|---|---|---|---|
| 1 | Report Summary | | |

5. In the Name field, enter an identifier for the template, for example, *Summary Template*.
6. In the Title Page Text field, enter the text that displays on the cover page of the report.
7. In the File Format field, from the drop down menu, select one of the following formats:
   - **PDF**
   - **CSV**
8. In the Page column, use the **Up** and **Down** arrows to determine how many pages should be included in the template.
9. In the Data Field column, from the drop-down menu, select the type of data that should be included on each page.
10. In the Chart Type column, select the type of chart that the report results should display in. For example, select *Bar*, *Column*, or *Pie*.

    For the Device Activations and Threat Detection History, additional chart types are available.

11. In the Time Period column, if needed, select the time period that should be used for the report.

> **Note:** Specific time periods are only available for the Device Activations and Threat Detection History data types.

12. The following table describes all the reporting options.

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Agent Version Spread** | Shows which version of the Webroot Secure Anywhere agent each Endpoint device is using. | Bar, Column, Pie | N/A |
| **Attention Required** | Provides a list of all Endpoint devices that have been determined as secure, and a list of those that require attention. | Bar, Column, Pie | N/A |
| **Device Activations** | Provides a list of all Endpoint devices that have been activated during the time period that you selected. | Area, Area Spline, Bar, Column, Line, Spline | 24h, 1 day, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Device Type** | Provides a list of the number of Endpoint devices that are PCs or Macs. | Bar, Column, Pie | N/A |
| **Endpoint Status** | Shows the number of clean Endpoint devices, and the number of infected Endpoint devices on your sites. | Bar, Column, Pie | N/A |
| **Expired Status** | Shows the number of Endpoint devices that are Active, and the number of Endpoint devices that have an Expired state. | Bar, Column, Pie | N/A |
| **Firewall Status** | Shows which of your Endpoint Devices have the Firewall option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Identity Shield Status** | Shows how many of your Endpoint Devices have the Identity Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |
| **Infrared Status** | Shows which of your Endpoint devices have the Enable Webroot Infrared option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Installation Status** | Shows which of your Endpoint devices have the Webroot Secure Anywhere product installed and which ones have had the product uninstalled. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Managed by Policy** | Shows how many of your Endpoint devices are being managed by a policy you have created and how many are in an unmanaged state. | Bar, Column, Pie | N/A |
| **Offline Shield Status** | Shows how many of your Endpoint devices have the Offline Shield option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Operating System Firewall Status** | Shows which of your Endpoint devices have an operating system Firewall option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Operating System Language** | Shows which Operating system language your Endpoint devices are using. | Bar, Column, Pie | N/A |
| **Operating System Platform** | Shows which Operating system platform, from 32 bit, 64 bit, or Unknown, that your Endpoint devices are using. | Bar, Column, Pie | N/A |
| **Phishing Shield Status** | Shows how many of your Endpoint devices have the Phishing Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |
| **Primary Browser** | Shows the Primary Web Browser used by each of your Endpoint devices. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Realtime Shield Status** | Shows how many of your Endpoint devices have the Realtime Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |
| **Remediation Status** | Shows how many of your Endpoint devices have the Remediation status:<br>• Disabled<br>• Enabled<br>To disable the Remediation status, the **Automatically quarantine previously blocked files** option must be turned off. | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Report Summary** | Provides a number of overall counts that effectively summarize site or deployment information:<br>• Number of active devices<br>• Number of available seats Endpoints currently needing attention<br>• Endpoints which encountered threats (Last 'n' days)<br>• Total Threats seen (Last 'n' days)<br>• Number of Endpoints Seen (Last 'n' days)<br>• Number of Endpoints Not Seen (Last 'n' days)<br>• Number of Endpoints Seen (All Time) | Bar, Column, Pie | N/A |

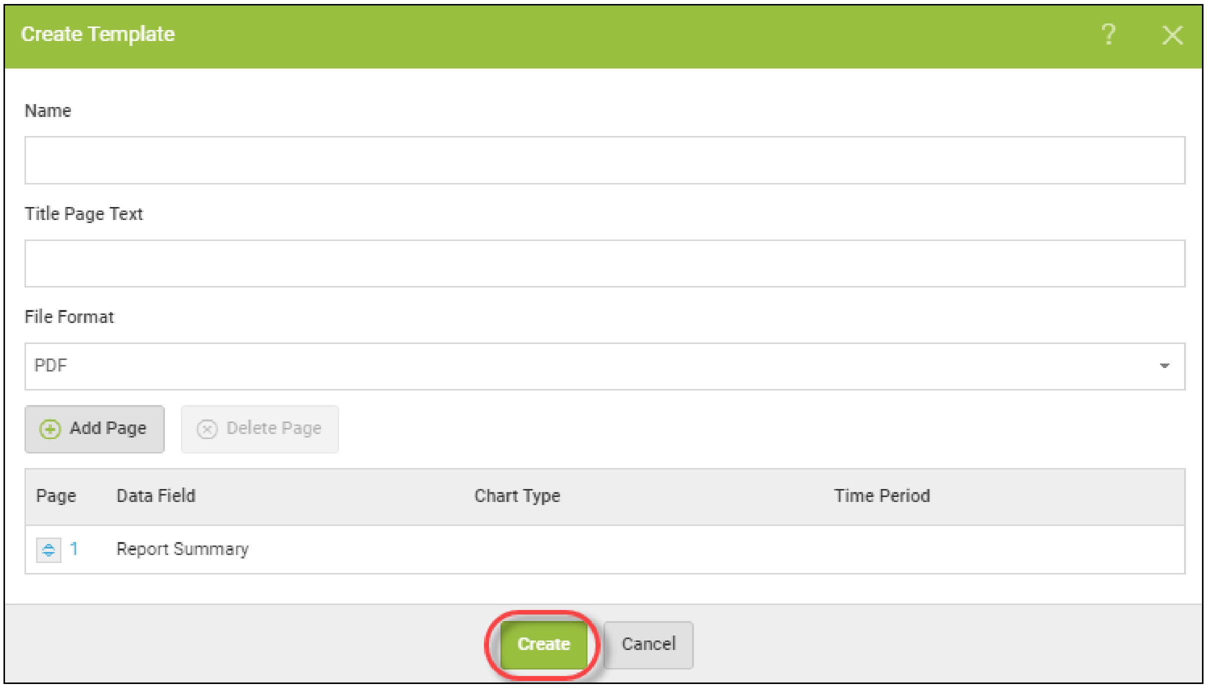
| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Rootkit Shield Status** | Shows how many of your Endpoint devices have the Rootkit Shield option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Scheduled Scans Status** | Shows how many of your Endpoint devices have a Scheduled Scan:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |
| **Silent Mode** | Shows how many of your Endpoint devices have the Silent Audit option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |

| DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS |
|---|---|---|---|
| **Threat Detection History** | Shows the history over your selected time period, of all threats that have been detected on your Endpoint devices. | Area, Area Spline, Bar, Column, Line, Spline | 24h, 1 day, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days |
| **USB Shield Status** | Shows how many of your Endpoint devices have the USB Shield option:<br>• Disabled<br>• Enabled<br>• Unsupported | Bar, Column, Pie | N/A |
| **Virtual Machine** | Shows how many of your Endpoint devices have been classified as Virtual Machines (VMs). | Bar, Column, Pie | N/A |
| **Web Threat Shield Status** | Shows how many of your Endpoint devices have the USB Shield option:<br>• Disabled<br>• Enabled | Bar, Column, Pie | N/A |

For reports that collate stats from multiple sites into one report, this will also include the following:

- Total Number of sites
- Active sites
- Trial sites
- Suspended sites
- Deactivated sites
- Expired sites
- Sites expiring in the next 14 days
- Sites with endpoints needing attention

13. When you're done, click the **Create** button.



File Format: PDF

| Page | Data Field | Chart Type | Time Period |
|---|---|---|---|
| 1 | Report Summary | | |

# Accessing Report Histories

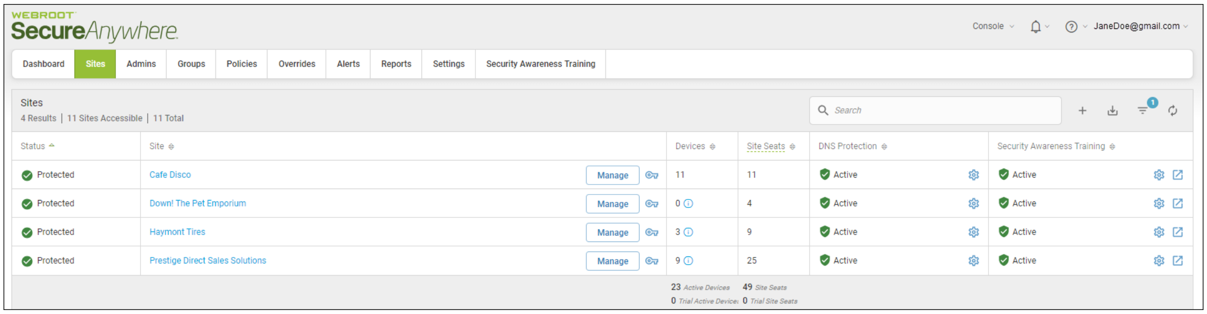
Access a historical record of all report runs over the last 90 days including the requested date, recipient summary, and ability to download exactly what was sent as part of the schedule. Requesting a download will allow you to select from the templates, sites and languages which were included in the original generation so you can see exactly what was sent to stakeholders on the distribution list.

**Note**: Reports are available only in PDF format. Reports available through history for download for 90 day period. Links provided in emails to download reports valid for 48 hours only.

**To access a report's history:**

1. Log in to the management console.

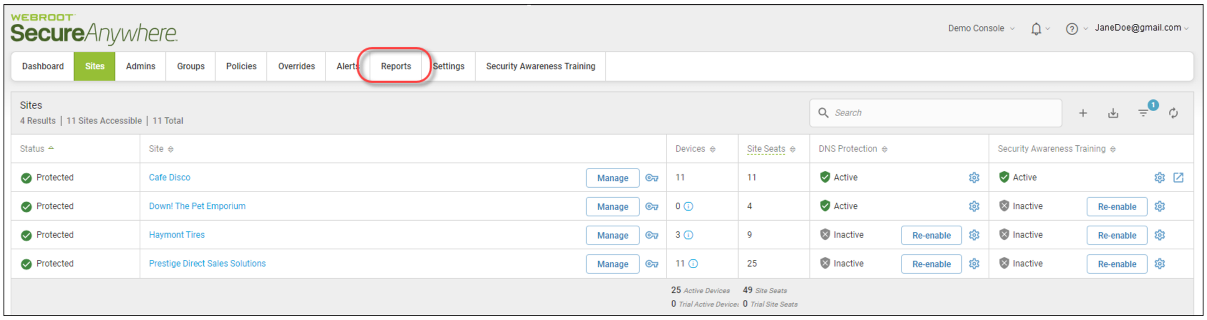
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

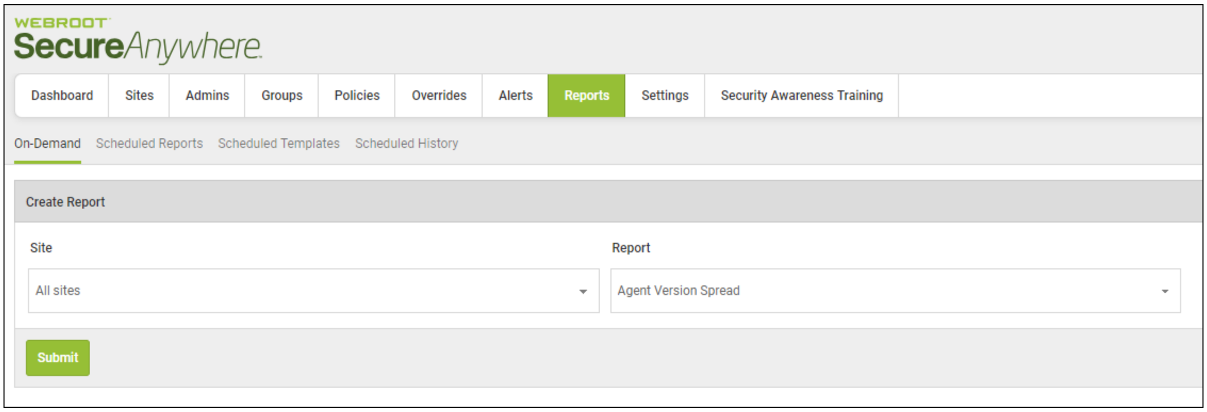
2. Click the **Reports** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Inactive |
| Protected | Haymont Tires | 3 | 9 | Inactive | Inactive |
| Protected | Prestige Direct Sales Solutions | 11 | 25 | Inactive | Inactive |
| | | 25 Active Devices<br>0 Trial Active Devices | 49 Site Seats<br>0 Trial Site Seats | | |

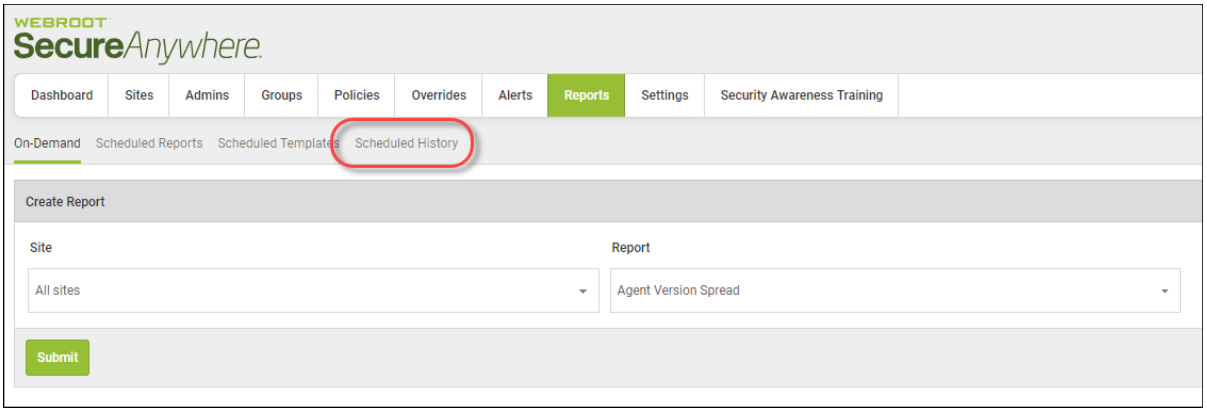
   The system displays the Reports tab with the On-Demand tab active.



Site: All sites

Report: Agent Version Spread

3. Click the **Scheduled History** tab.

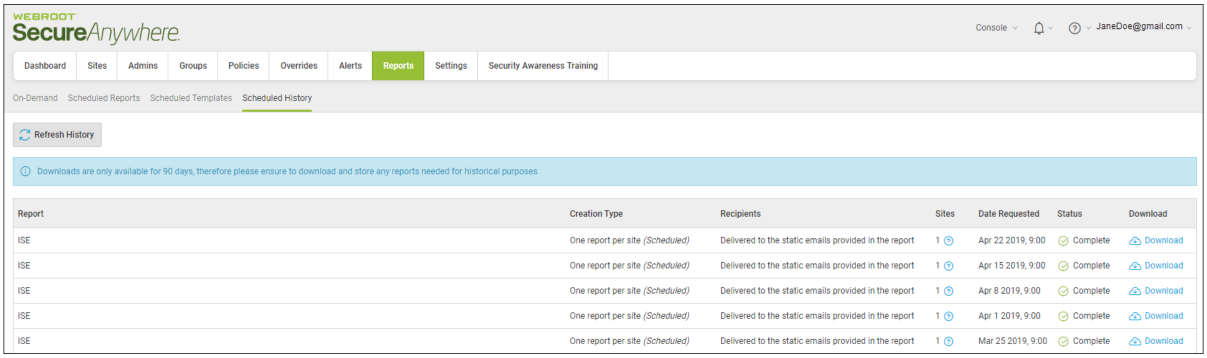


Site: All sites

Report: Agent Version Spread

The History pane displays with the following information:

- Report Name
- Creation Type
- Recipients
- Sites
- Date Requested
- Status
- Download PDF



ⓘ Downloads are only available for 90 days, therefore please ensure to download and store any reports needed for historical purposes

| Report | Creation Type | Recipients | Sites | Date Requested | Status | Download |
|---|---|---|---|---|---|---|
| ISE | One report per site *(Scheduled)* | Delivered to the static emails provided in the report | 1 | Apr 22 2019, 9:00 | ✓ Complete | Download |
| ISE | One report per site *(Scheduled)* | Delivered to the static emails provided in the report | 1 | Apr 15 2019, 9:00 | ✓ Complete | Download |
| ISE | One report per site *(Scheduled)* | Delivered to the static emails provided in the report | 1 | Apr 8 2019, 9:00 | ✓ Complete | Download |
| ISE | One report per site *(Scheduled)* | Delivered to the static emails provided in the report | 1 | Apr 1 2019, 9:00 | ✓ Complete | Download |
| ISE | One report per site *(Scheduled)* | Delivered to the static emails provided in the report | 1 | Mar 25 2019, 9:00 | ✓ Complete | Download |

# Downloading Reports

For reports that display in a spreadsheet format, you can export the report to a CSV format.

The reports that you can do this for are as follows:

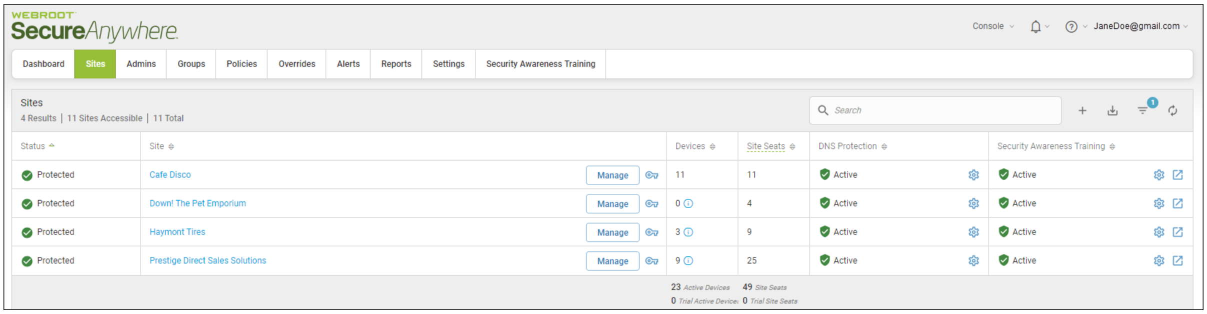
- All Threats Seen
- All Undetermined Software Seen
- Devices With Threats Seen On Last Scan
- Devices With Undetermined Software On Last Scan
- Web Threat Shield Blocked URL History
- Web Threat shield Blocked URLs

For more information, see *Generating On-Demand Reports on page 454*.

**To download reports:**

1. Log in to the management console.

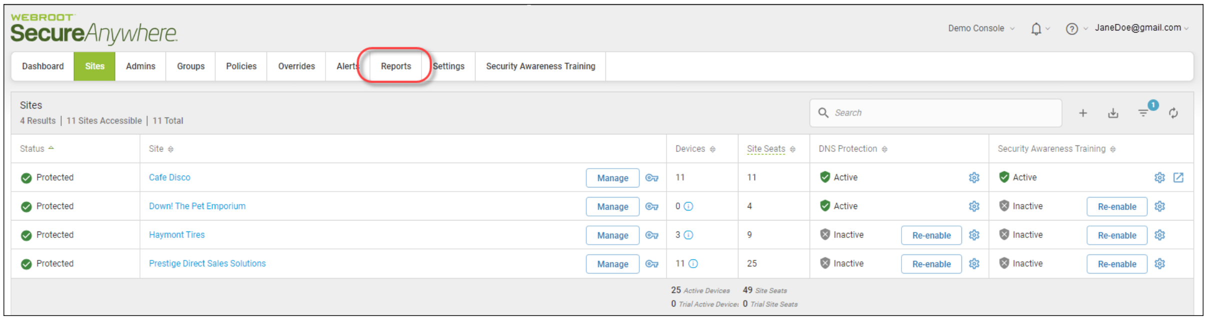
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

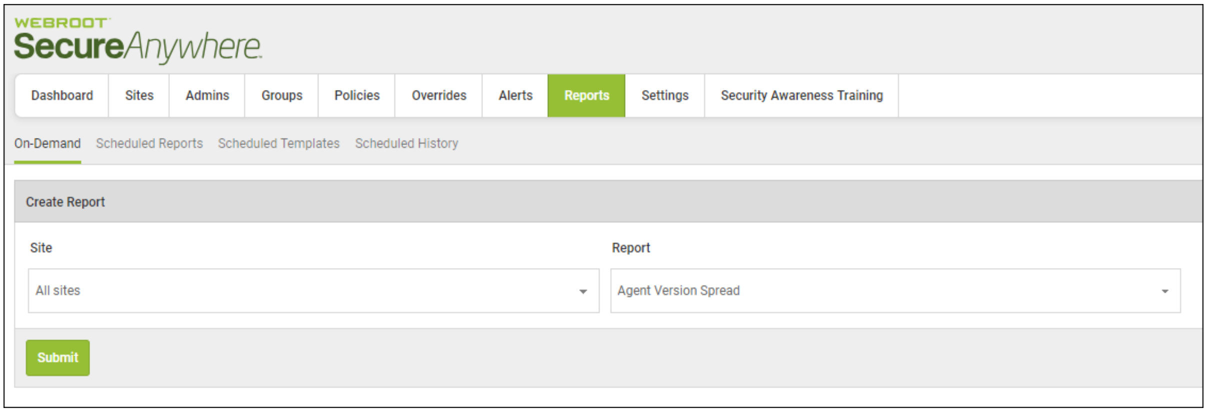
2. Click the **Reports** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | | Security Awareness Training | |
|---|---|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | | Active | |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | | Inactive | Re-enable |
| Protected | Haymont Tires | Manage | 3 | 9 | Inactive | Re-enable | Inactive | Re-enable |
| Protected | Prestige Direct Sales Solutions | Manage | 11 | 25 | Inactive | Re-enable | Inactive | Re-enable |
| | | | 25 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | | | |

The system displays the Reports pane with the On-Demand tab active.

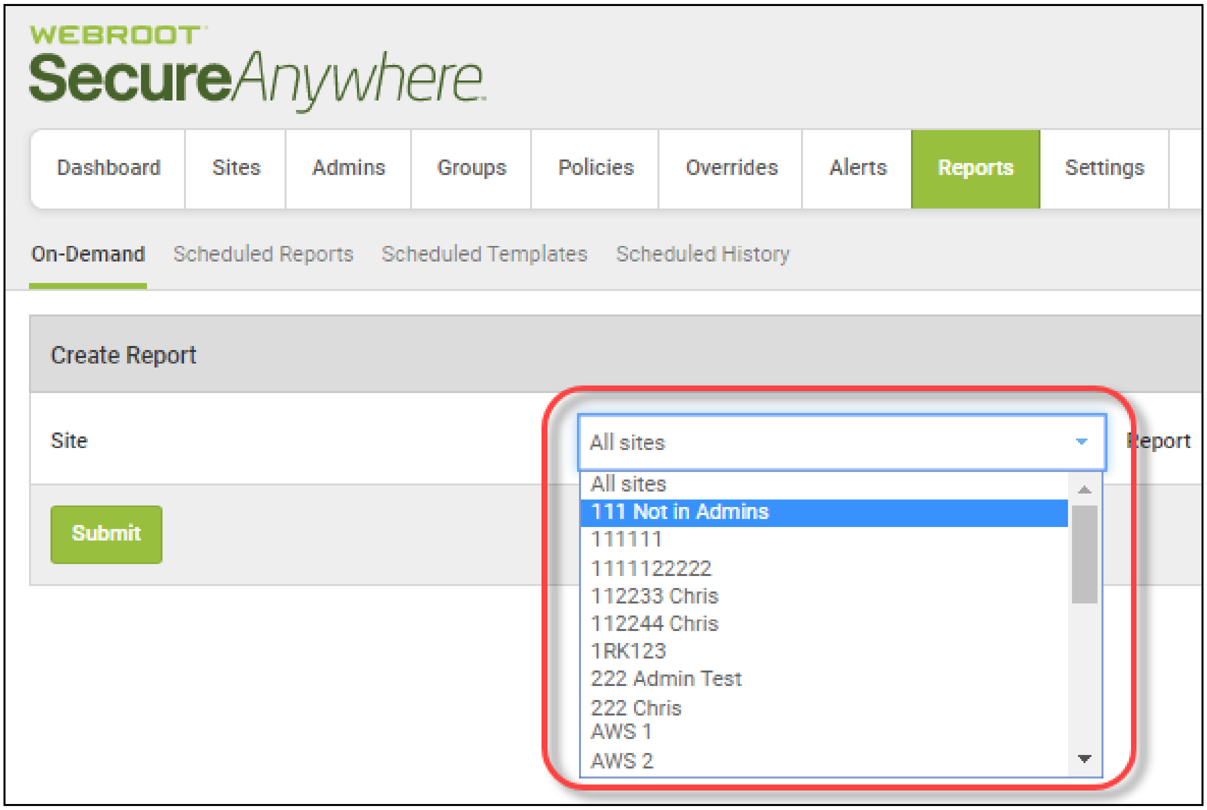


Create Report

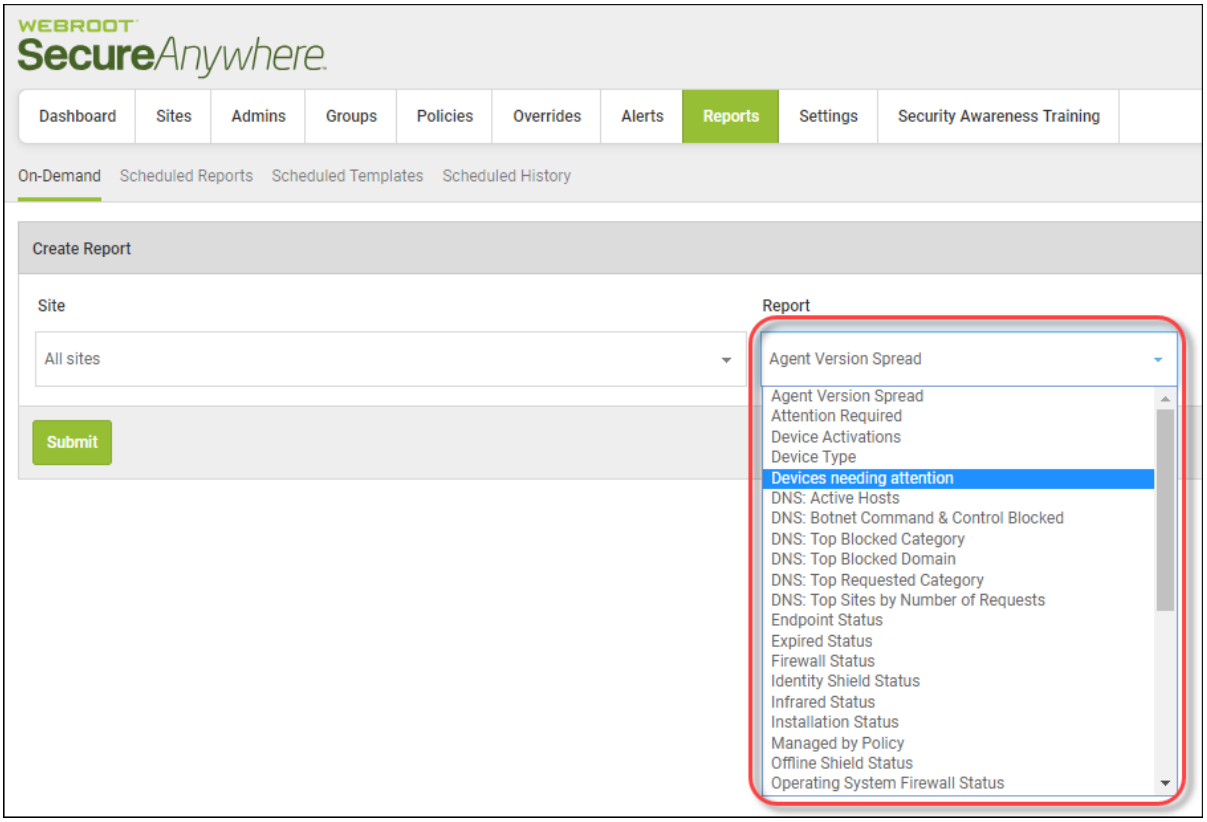
Site: All sites

Report: Agent Version Spread

3. From the Sites drop-down menu, select the site for which you want to generate the report.



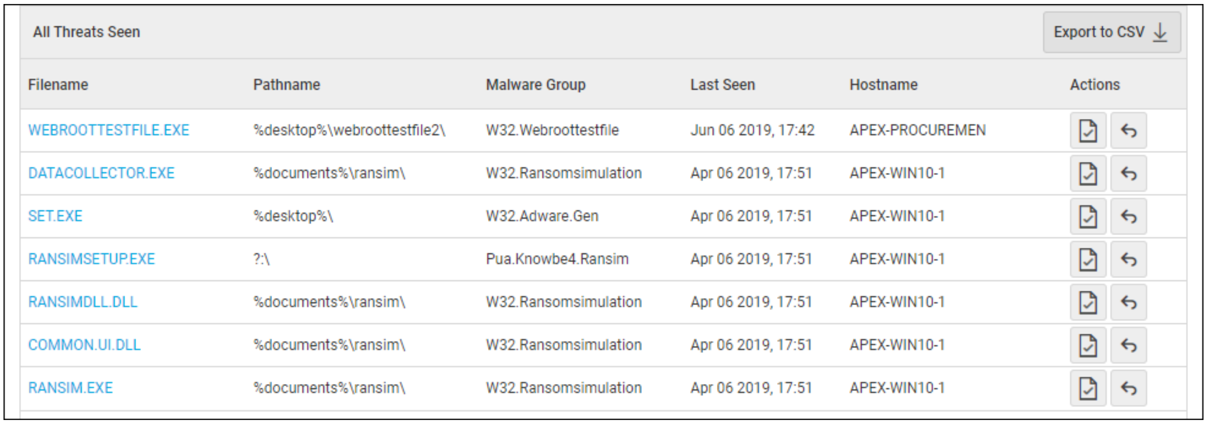
4. From the Report drop-down menu, select the report you want to generate.



Site: All sites

Report: Agent Version Spread

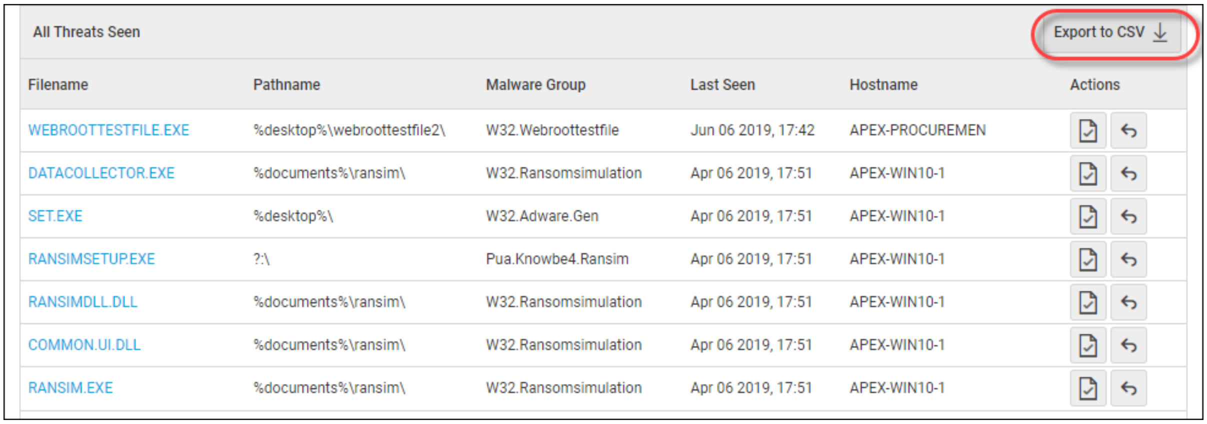
The report displays in a spreadsheet format.


All Threats Seen

Export to CSV

| Filename | Pathname | Malware Group | Last Seen | Hostname | Actions |
|---|---|---|---|---|---|
| WEBROOTTESTFILE.EXE | %desktop%\webroottestfile2\ | W32.Webroottestfile | Jun 06 2019, 17:42 | APEX-PROCUREMEN | |
| DATACOLLECTOR.EXE | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | |
| SET.EXE | %desktop%\ | W32.Adware.Gen | Apr 06 2019, 17:51 | APEX-WIN10-1 | |
| RANSIMSETUP.EXE | ?:\ | Pua.Knowbe4.Ransim | Apr 06 2019, 17:51 | APEX-WIN10-1 | |
| RANSIMDLL.DLL | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | |
| COMMON.UI.DLL | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | |
| RANSIM.EXE | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | |

5. Click the **Export to CSV** button.

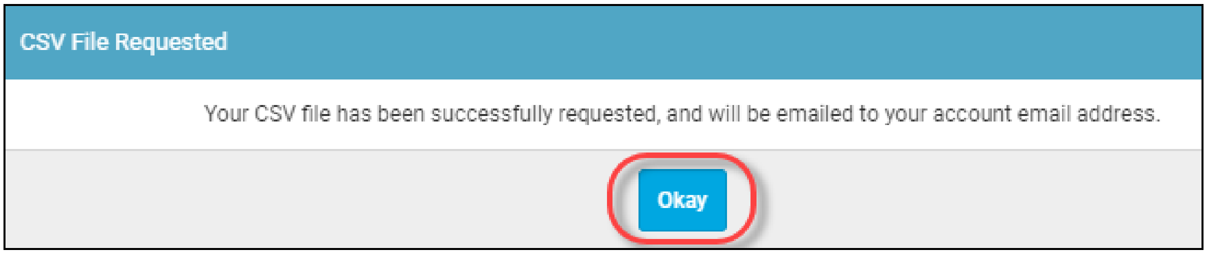


All Threats Seen

| Filename | Pathname | Malware Group | Last Seen | Hostname | Actions |
|---|---|---|---|---|---|
| WEBROOTTESTFILE.EXE | %desktop%\webroottestfile2\ | W32.Webroottestfile | Jun 06 2019, 17:42 | APEX-PROCUREMEN | 🗎 ↶ |
| DATACOLLECTOR.EXE | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | 🗎 ↶ |
| SET.EXE | %desktop%\ | W32.Adware.Gen | Apr 06 2019, 17:51 | APEX-WIN10-1 | 🗎 ↶ |
| RANSIMSETUP.EXE | ?:\ | Pua.Knowbe4.Ransim | Apr 06 2019, 17:51 | APEX-WIN10-1 | 🗎 ↶ |
| RANSIMDLL.DLL | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | 🗎 ↶ |
| COMMON.UI.DLL | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | 🗎 ↶ |
| RANSIM.EXE | %documents%\ransim\ | W32.Ransomsimulation | Apr 06 2019, 17:51 | APEX-WIN10-1 | 🗎 ↶ |

The following message displays: *Your CSV file has been successfully requested, and will be emailed to your account email address*.

6. Click the **Okay** button to return to the report spreadsheet.



CSV File Requested

Your CSV file has been successfully requested, and will be emailed to your account email address.

# Chapter 11: Working With Settings

To work with settings, see the following topics:

# Settings Overview

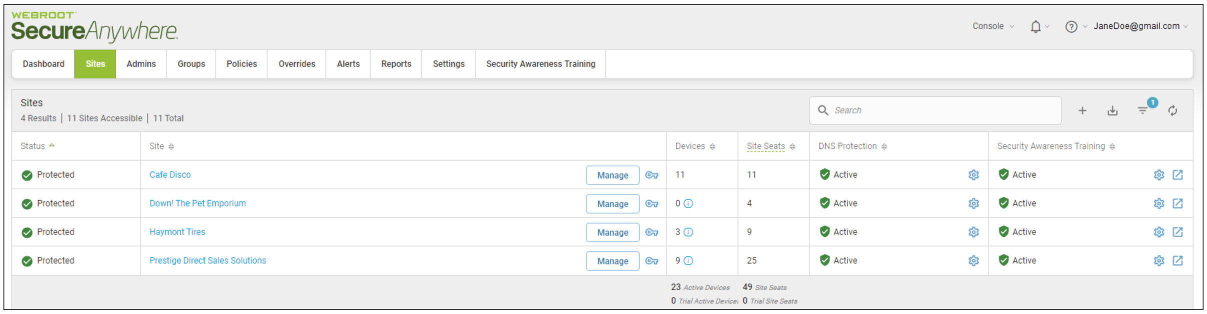
The Settings tab has the following functionality:

- Activating Subscriptions for DNS Protection
- Activating Subscriptions for Security Awareness Training
- Viewing Account Information
- Setting GSM-Level Data Filters on page 521
- Creating API Client Credentials on page 528

**To access the Settings tab:**

1. Log in to the management console.

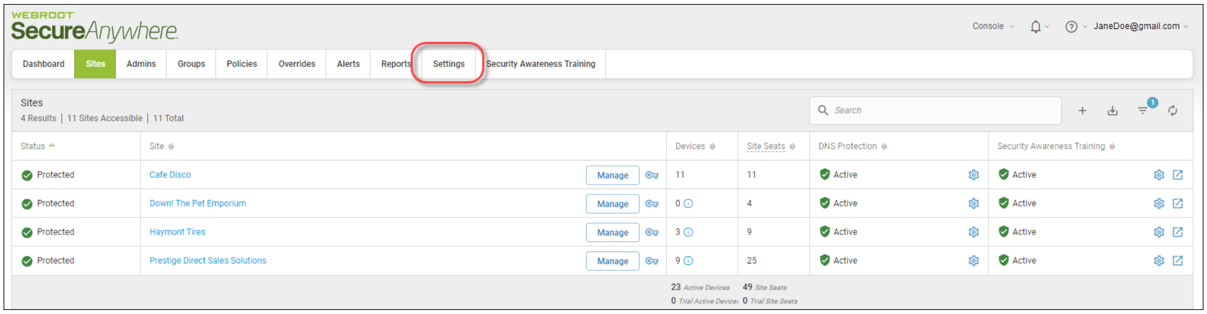
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

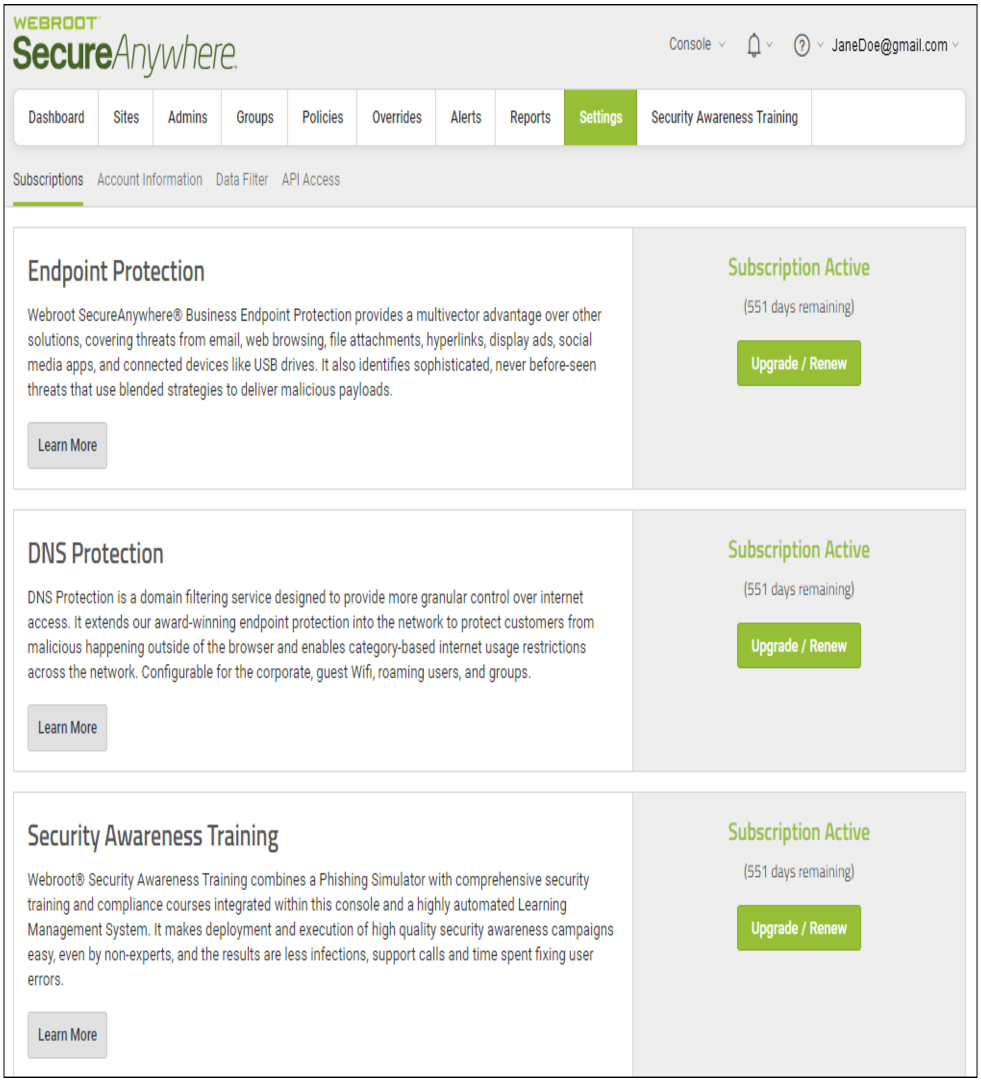
2. Click the **Settings** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

The system displays the Settings tab, with the Subscriptions tab active.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

DNS Protection

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.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

3. For more information on what functionality is available on the Settings tab, see any of the following:
    - *Activating Subscriptions for DNS Protection*
    - *Activating Subscriptions for Security Awareness Training*
    - *Setting GSM-Level Data Filters on page 521*
    - *Viewing Account Information on page 503*
    - *Creating API Client Credentials on page 528*

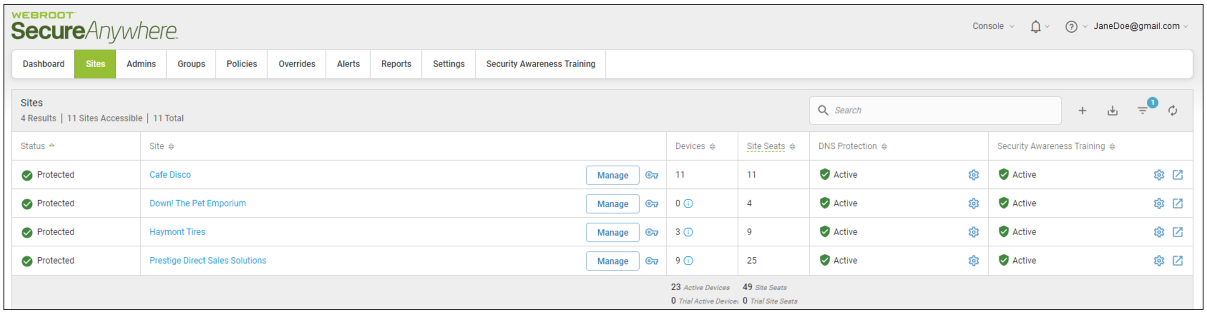
# Viewing Account Information

You can view information about different accounts, including the point of contact and the billing cycle.

**To view account information:**

1. Log in to the management console.

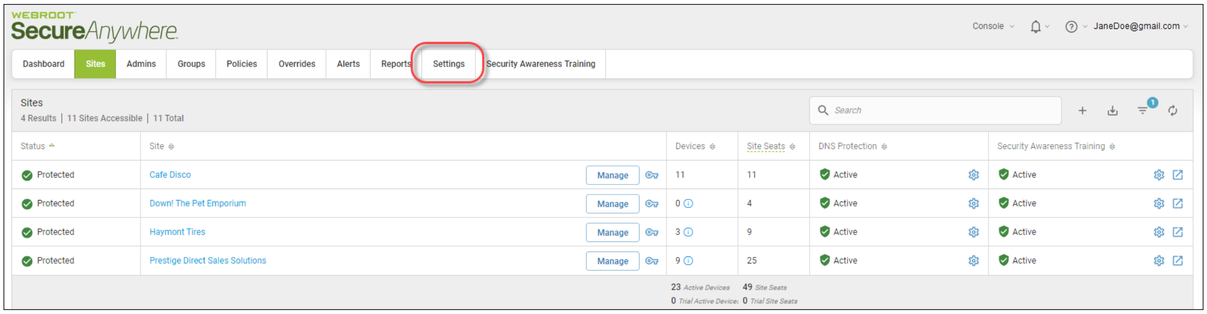
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

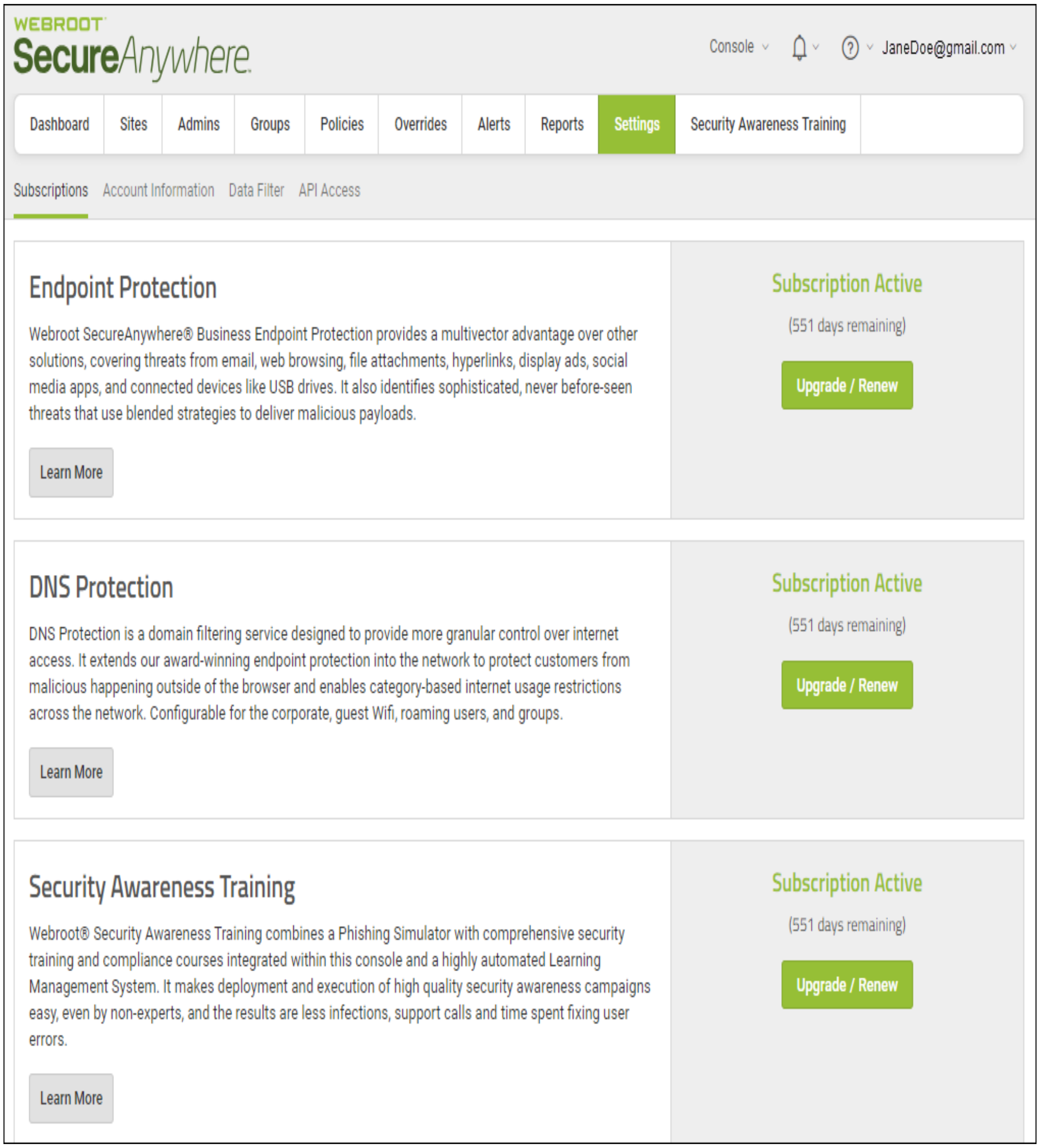
2. Click the **Settings** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|
| Protected | Cafe Disco | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | 0 | 4 | Active | Active |
| Protected | Haymont Tires | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | 9 | 25 | Active | Active |
| | | 23 *Active Devices*<br>0 *Trial Active Device:* | 49 *Site Seats*<br>0 *Trial Site Seats* | | |

   The system displays the Settings tab, with the Subscriptions tab active.



## Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

## DNS Protection

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.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

## Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

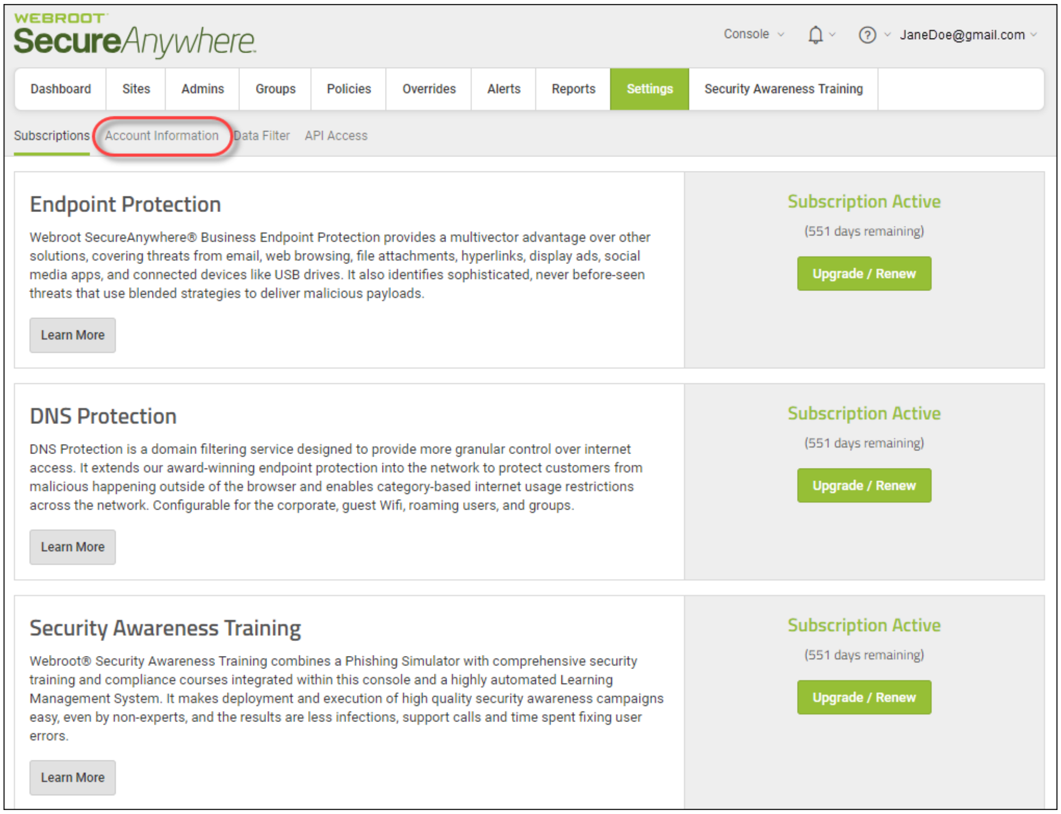
Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

3. Click the **Account Information** tab.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Subscription Active

(551 days remaining)

DNS Protection

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.

Subscription Active

(551 days remaining)

Security Awareness Training

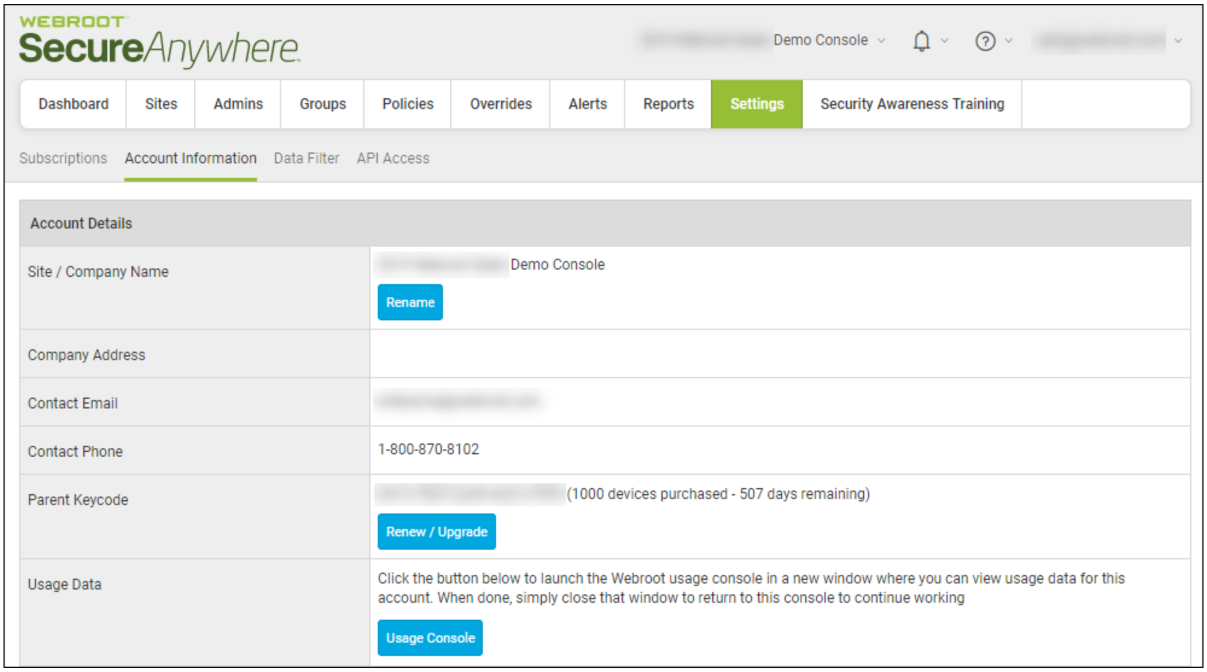
Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Subscription Active

(551 days remaining)

The Account Information tab displays the following information:

- Site/Company name
- Company address
- Contact email
- Contact phone
- Parent keycode, which you can renew or upgrade. Click the **Renew/Upgrade** button to display information about your Channel Partner or Webroot account Manager, either of whom can assist you with renewing or upgrading.
- Usage Data. For more information, see *Accessing Usage Data on page 507* and *Downloading Usage Data Reports on page 515*.



| Account Details | |
|---|---|
| Site / Company Name | [redacted] Demo Console |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | 1-800-870-8102 |
| Parent Keycode | [redacted] (1000 devices purchased - 507 days remaining) |
| Usage Data | Click the button below to launch the Webroot usage console in a new window where you can view usage data for this account. When done, simply close that window to return to this console to continue working |

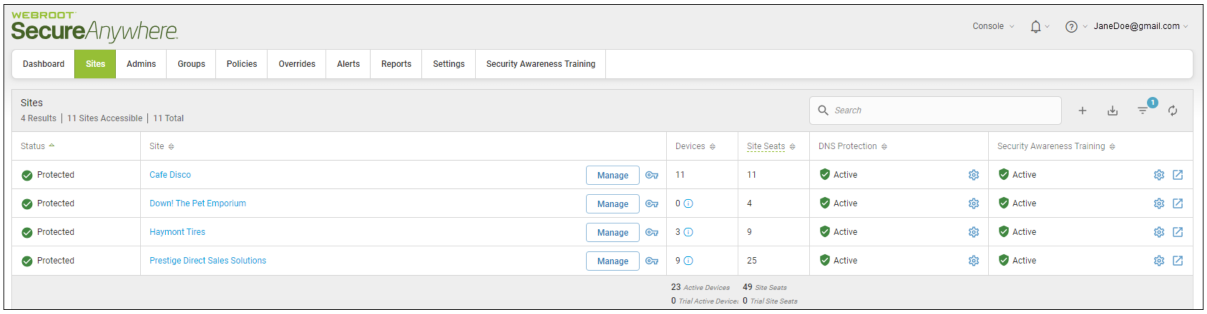
# Accessing Usage Data

With the usage console that includes detailed breakdowns of your Webroot products and services, you can now access your usage data for Endpoint Protection, DNS Protection, and Security Awareness Training.

**To access usage data:**

1. Log in to the management console.

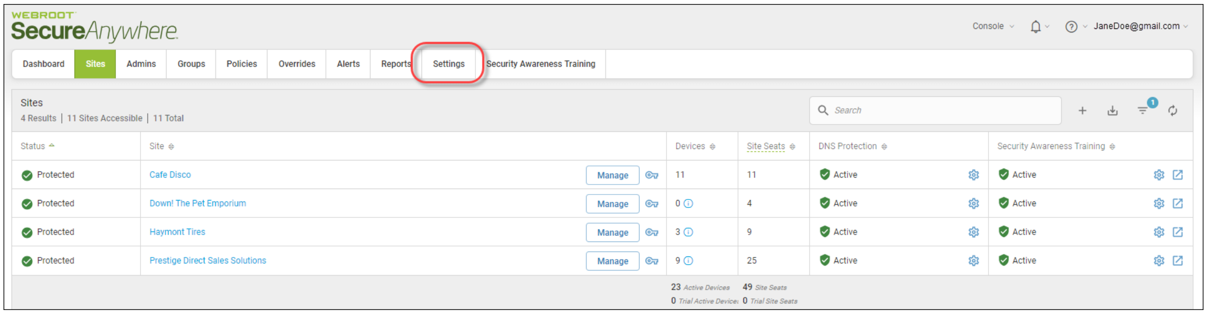
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

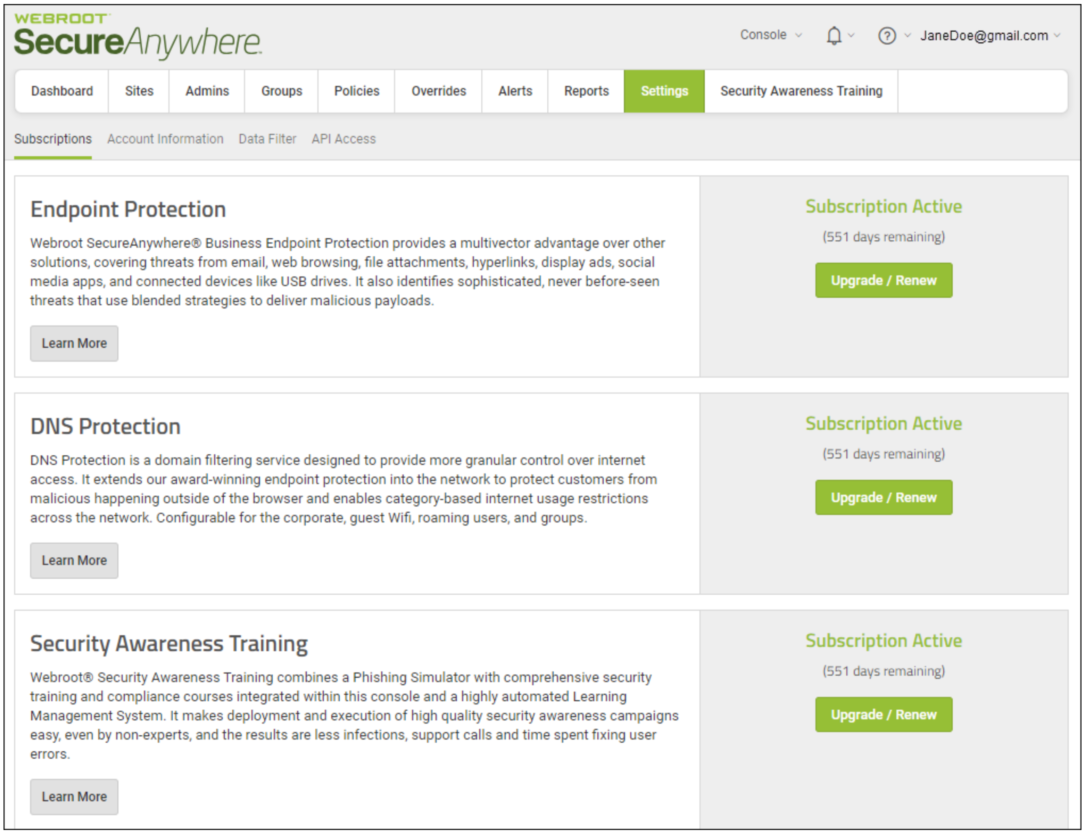
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| ✓ Protected | Cafe Disco | Manage | 11 | 11 | ✓ Active | ✓ Active |
| ✓ Protected | Down! The Pet Emporium | Manage | 0 ⓘ | 4 | ✓ Active | ✓ Active |
| ✓ Protected | Haymont Tires | Manage | 3 ⓘ | 9 | ✓ Active | ✓ Active |
| ✓ Protected | Prestige Direct Sales Solutions | Manage | 9 ⓘ | 25 | ✓ Active | ✓ Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

2. Click the **Settings** tab.


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| ✓ Protected | Cafe Disco | Manage | 11 | 11 | ✓ Active | ✓ Active |
| ✓ Protected | Down! The Pet Emporium | Manage | 0 ⓘ | 4 | ✓ Active | ✓ Active |
| ✓ Protected | Haymont Tires | Manage | 3 ⓘ | 9 | ✓ Active | ✓ Active |
| ✓ Protected | Prestige Direct Sales Solutions | Manage | 9 ⓘ | 25 | ✓ Active | ✓ Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Settings tab displays with the Subscriptions tab active.



## Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

## DNS Protection

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.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

## Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

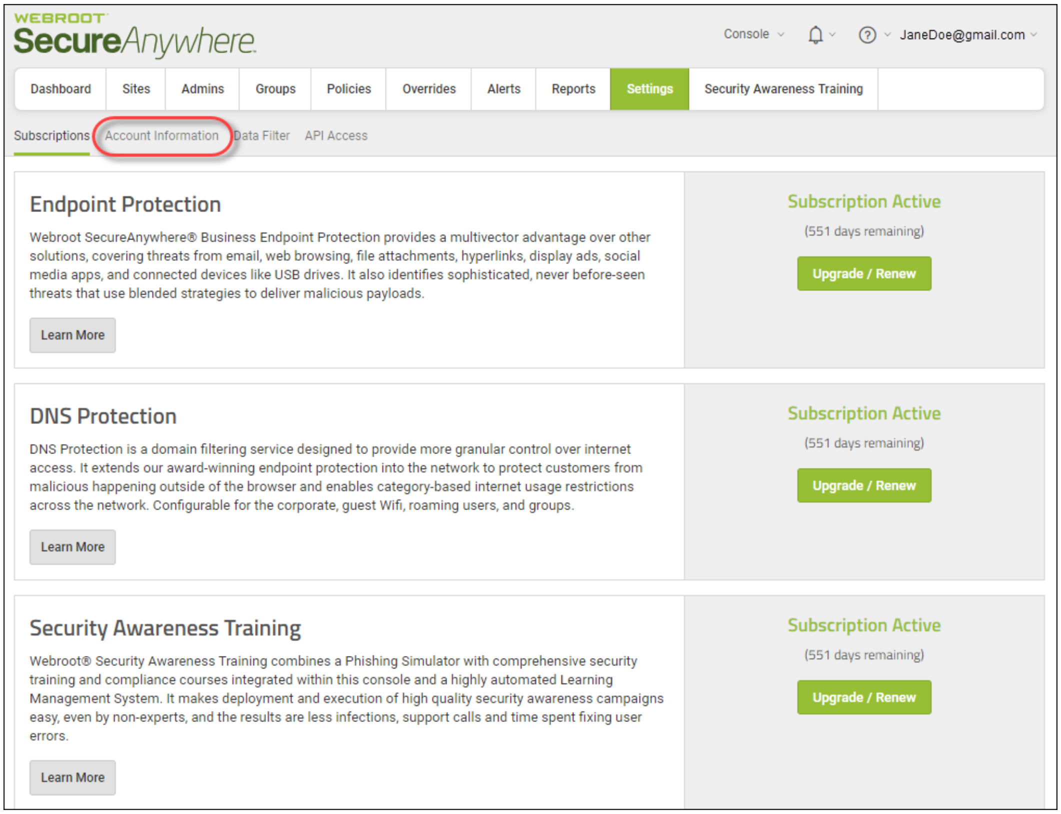
Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

3. Click the **Account Information** tab.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Subscription Active

(551 days remaining)

DNS Protection

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.

Subscription Active

(551 days remaining)

Security Awareness Training

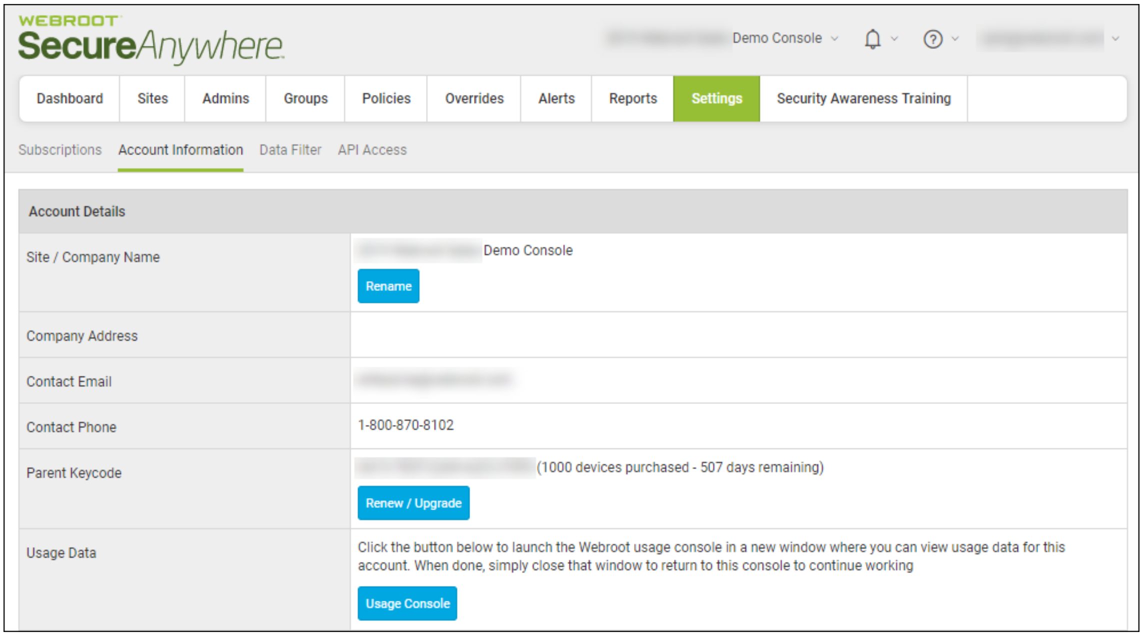
Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Subscription Active

(551 days remaining)

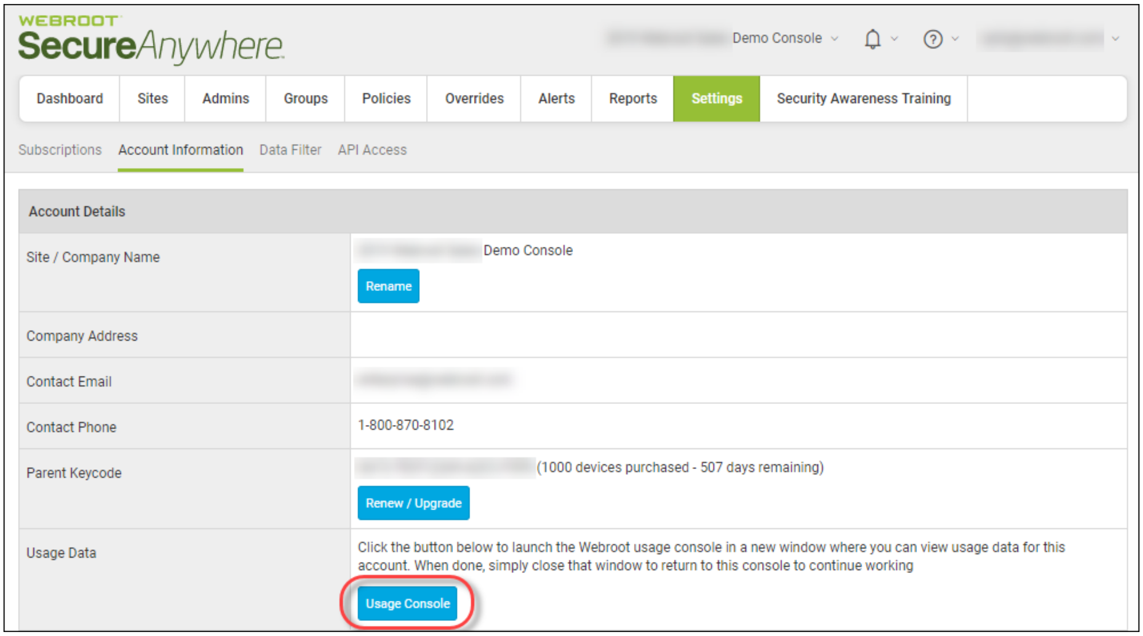
The Account Information tab displays the following information:

- Site/Company name
- Company address
- Contact email
- Contact phone
- Parent keycode, which you can renew or upgrade. Click the **Renew/Upgrade** button to display information about your Channel Partner or Webroot account Manager, either of whom can assist you with renewing or upgrading.



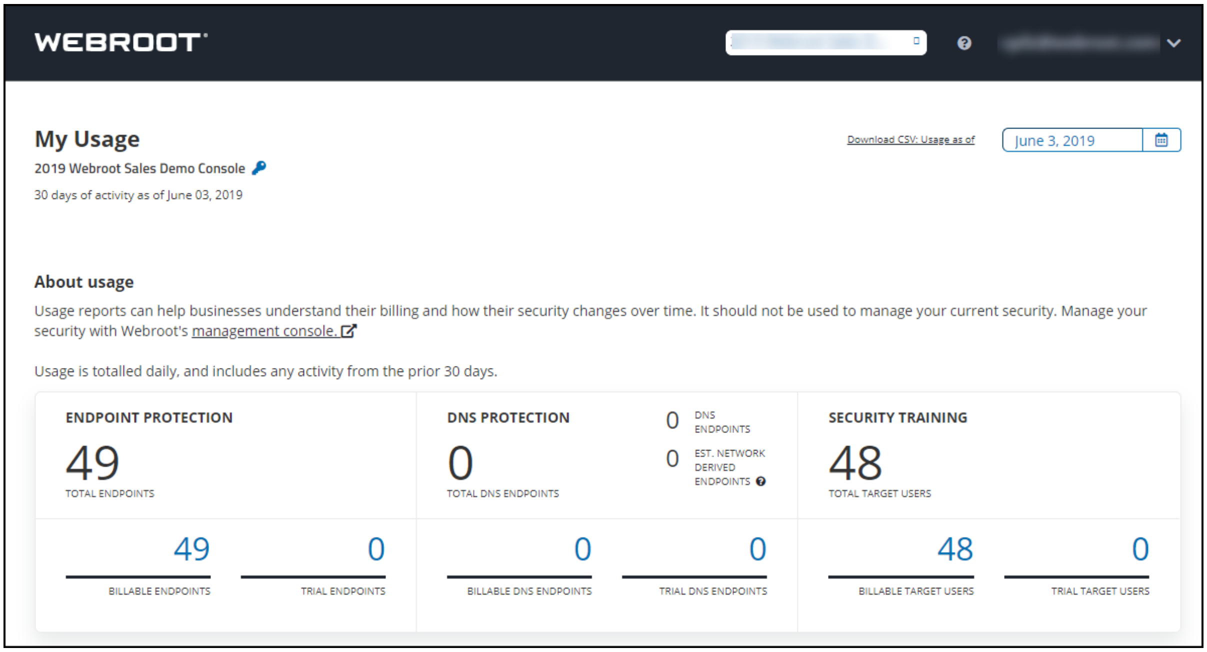
| Account Details | |
|---|---|
| Site / Company Name | [redacted] Demo Console |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | 1-800-870-8102 |
| Parent Keycode | [redacted] (1000 devices purchased - 507 days remaining) |
| Usage Data | Click the button below to launch the Webroot usage console in a new window where you can view usage data for this account. When done, simply close that window to return to this console to continue working |

4. Click the **Usage Console** button.



| Account Details | |
|---|---|
| Site / Company Name | [redacted] Demo Console |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | 1-800-870-8102 |
| Parent Keycode | [redacted] (1000 devices purchased - 507 days remaining) |
| Usage Data | Click the button below to launch the Webroot usage console in a new window where you can view usage data for this account. When done, simply close that window to return to this console to continue working |

The My Usage console displays.



WEBROOT [redacted] [redacted]

My Usage

2019 Webroot Sales Demo Console

30 days of activity as of June 03, 2019

Download CSV: Usage as of June 3, 2019

About usage

Usage reports can help businesses understand their billing and how their security changes over time. It should not be used to manage your current security. Manage your security with Webroot's management console.

Usage is totalled daily, and includes any activity from the prior 30 days.

| ENDPOINT PROTECTION | | DNS PROTECTION | | SECURITY TRAINING | |
|---|---|---|---|---|---|
| 49 TOTAL ENDPOINTS | | 0 TOTAL DNS ENDPOINTS | 0 DNS ENDPOINTS<br>0 EST. NETWORK DERIVED ENDPOINTS | 48 TOTAL TARGET USERS | |
| 49 BILLABLE ENDPOINTS | 0 TRIAL ENDPOINTS | 0 BILLABLE DNS ENDPOINTS | 0 TRIAL DNS ENDPOINTS | 48 BILLABLE TARGET USERS | 0 TRIAL TARGET USERS |

The top portion of the My Usage console displays the following information:

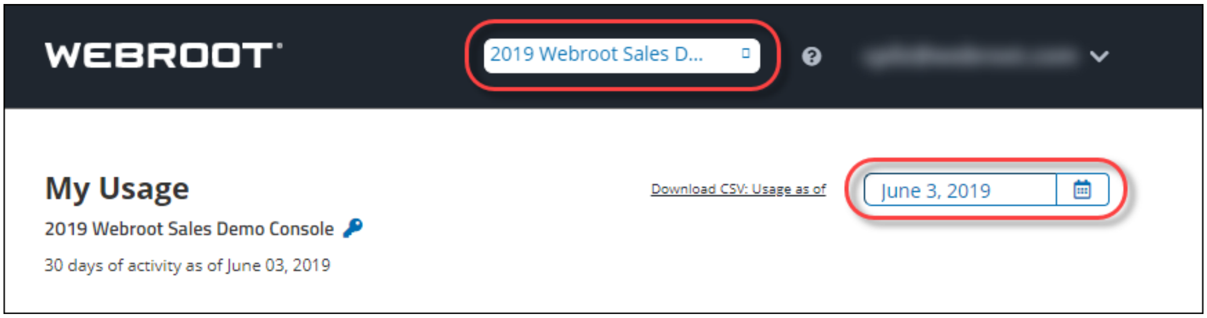
- Number of billable endpoints for Endpoint Protection, DNS Protection, and Security Awareness Training.
- Number of trial endpoints for Endpoint Protection, DNS Protection, and Security Awareness Training.

**Note:** Usage is totaled daily and includes any activity from the prior 30 days for the date in the Date Picker field.

5. As needed, you can do both of the following:

- From the Selection drop-down menu, you can select an alternate management console to view usage about.

- Use the Date Picker to select an alternate date range to view usage for.



My Usage

2019 Webroot Sales Demo Console

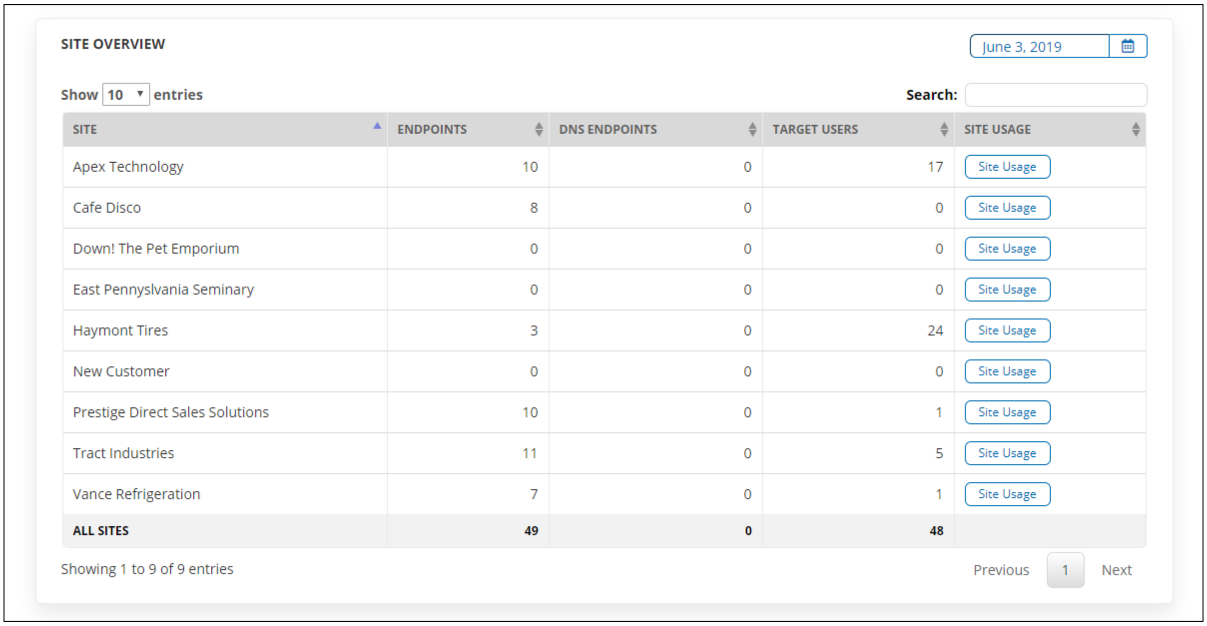
30 days of activity as of June 03, 2019

Download CSV: Usage as of

June 3, 2019

> **Note:** For information about downloading reports, see *Downloading Usage Data Reports on page 515*.

The bottom portion of the My Usage console displays the Site Overview spreadsheet.



SITE OVERVIEW

June 3, 2019

Show 10 entries

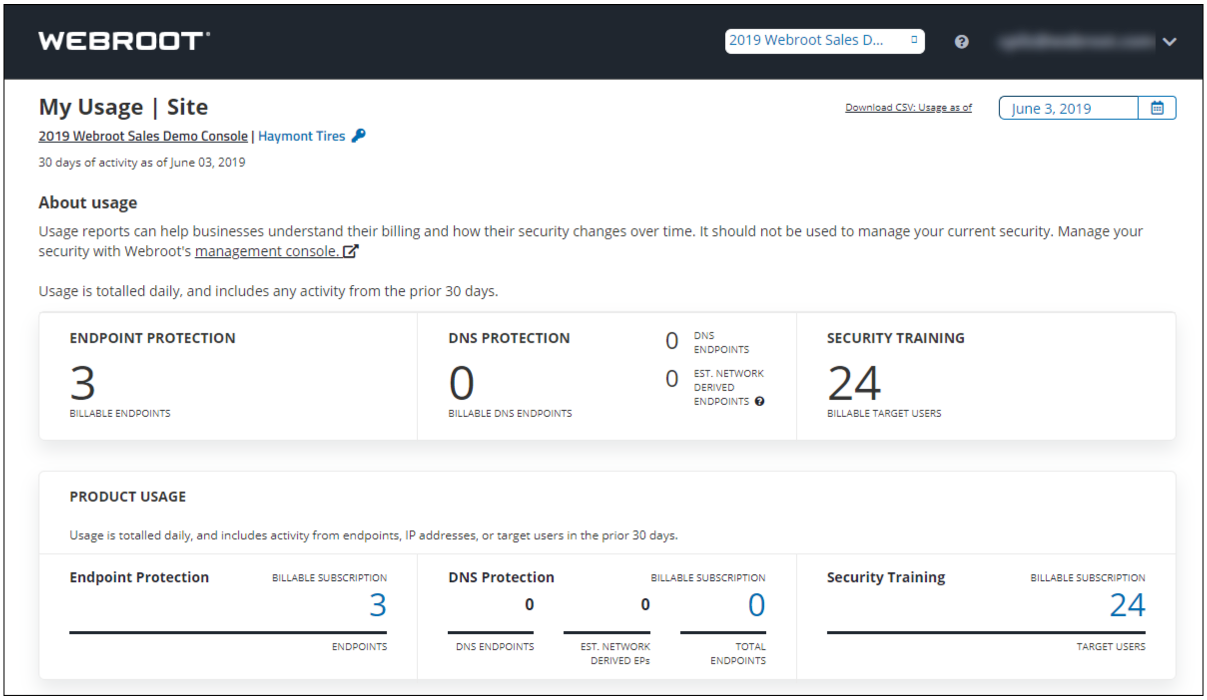
Search:

| SITE | ENDPOINTS | DNS ENDPOINTS | TARGET USERS | SITE USAGE |
|---|---|---|---|---|
| Apex Technology | 10 | 0 | 17 | Site Usage |
| Cafe Disco | 8 | 0 | 0 | Site Usage |
| Down! The Pet Emporium | 0 | 0 | 0 | Site Usage |
| East Pennyslvania Seminary | 0 | 0 | 0 | Site Usage |
| Haymont Tires | 3 | 0 | 24 | Site Usage |
| New Customer | 0 | 0 | 0 | Site Usage |
| Prestige Direct Sales Solutions | 10 | 0 | 1 | Site Usage |
| Tract Industries | 11 | 0 | 5 | Site Usage |
| Vance Refrigeration | 7 | 0 | 1 | Site Usage |
| **ALL SITES** | **49** | **0** | **48** | |

Showing 1 to 9 of 9 entries

The spreadsheet has the following columns:

- **Site** — Displays the name of the site.
- **Endpoints** — Displays the number of billable endpoints. This number reflects the number indicated in the Endpoint Protection area in the top portion of the page.
- **DNS Endpoints** — Displays the number of billable DNS Protection endpoints. This number reflects the number indicated in the DNS Protection area in the top portion of the page.
- **Target Users** — Displays the number of billable target users for Security Awareness Training. This number reflects the number indicated in the Security Training area in the top portion of the page.
- **Site Usage** —Click the **Site Usage** button to display usage data specific to that site.



My Usage | Site

Download CSV: Usage as of June 3, 2019

2019 Webroot Sales Demo Console | Haymont Tires

30 days of activity as of June 03, 2019

About usage

Usage reports can help businesses understand their billing and how their security changes over time. It should not be used to manage your current security. Manage your security with Webroot's management console.

Usage is totalled daily, and includes any activity from the prior 30 days.

ENDPOINT PROTECTION
3
BILLABLE ENDPOINTS

DNS PROTECTION
0
BILLABLE DNS ENDPOINTS
0 DNS ENDPOINTS
0 EST. NETWORK DERIVED ENDPOINTS

SECURITY TRAINING
24
BILLABLE TARGET USERS

PRODUCT USAGE

Usage is totalled daily, and includes activity from endpoints, IP addresses, or target users in the prior 30 days.

Endpoint Protection — BILLABLE SUBSCRIPTION 3 — ENDPOINTS

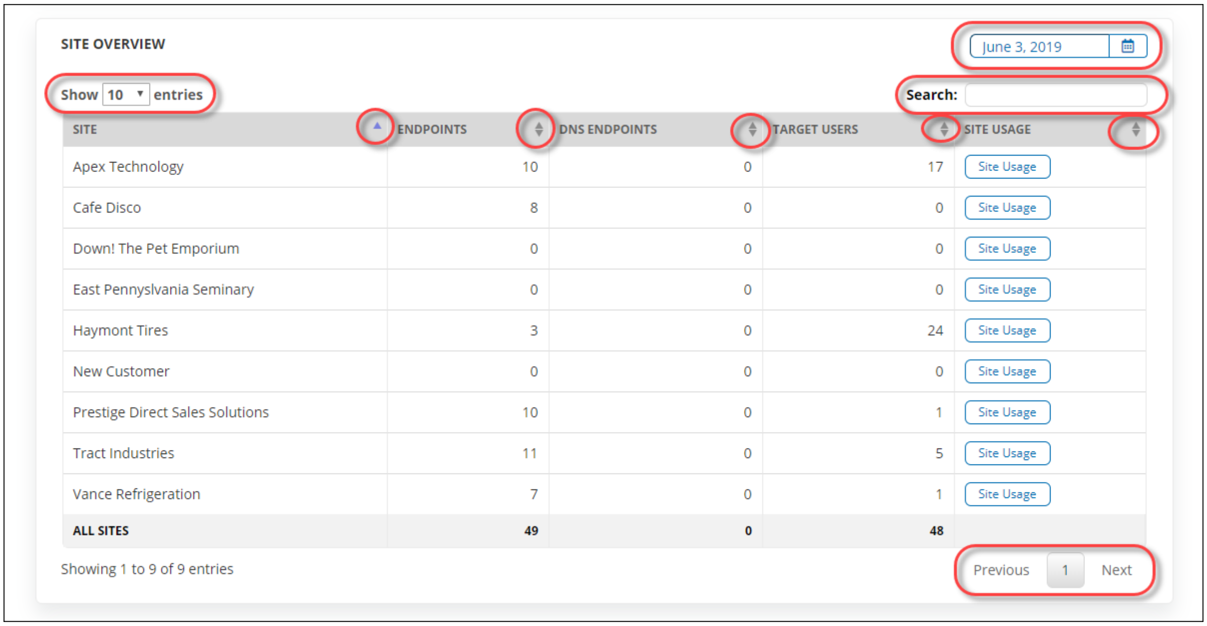
DNS Protection — BILLABLE SUBSCRIPTION — 0 DNS ENDPOINTS — 0 EST. NETWORK DERIVED EPs — 0 TOTAL ENDPOINTS

Security Training — BILLABLE SUBSCRIPTION 24 — TARGET USERS

As needed, you can do any of the following:

- Use the Date Picker to select an alternate date range to view usage for.
- Click the **Up** and **Down** arrows in each of the columns to sort information.
- Enter a site name in the Search field to help you locate a specific site.
- Adjust the number in the Show entries drop-down menu to display additional entries.

- If there are additional entries, you can click the **Previous** and **Next** arrows to display additional pages.



SITE OVERVIEW

June 3, 2019

Show 10 entries

Search:

| SITE | ENDPOINTS | DNS ENDPOINTS | TARGET USERS | SITE USAGE |
|---|---|---|---|---|
| Apex Technology | 10 | 0 | 17 | Site Usage |
| Cafe Disco | 8 | 0 | 0 | Site Usage |
| Down! The Pet Emporium | 0 | 0 | 0 | Site Usage |
| East Pennyslvania Seminary | 0 | 0 | 0 | Site Usage |
| Haymont Tires | 3 | 0 | 24 | Site Usage |
| New Customer | 0 | 0 | 0 | Site Usage |
| Prestige Direct Sales Solutions | 10 | 0 | 1 | Site Usage |
| Tract Industries | 11 | 0 | 5 | Site Usage |
| Vance Refrigeration | 7 | 0 | 1 | Site Usage |
| ALL SITES | 49 | 0 | 48 | |

Showing 1 to 9 of 9 entries

# Downloading Usage Data Reports

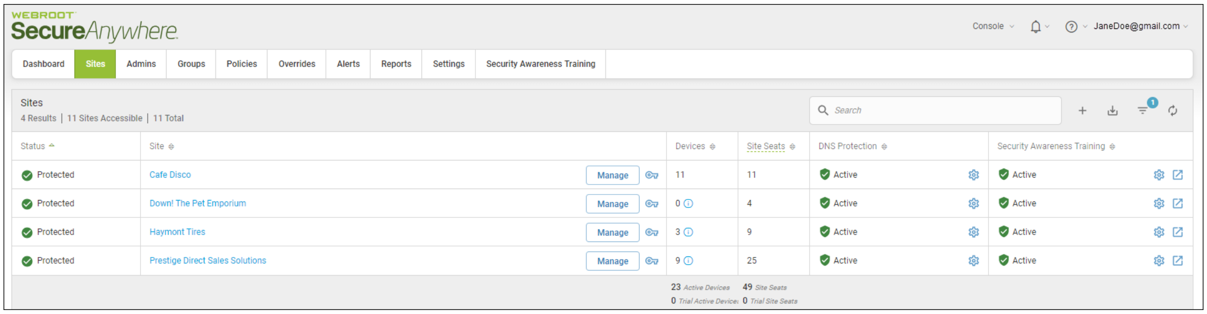
After you have viewed your usage data, follow this procedure to download a CSV file.

**Note:** For information about usage data, see *Accessing Usage Data on page 507*.

**To access usage data:**

1. Log in to the management console.

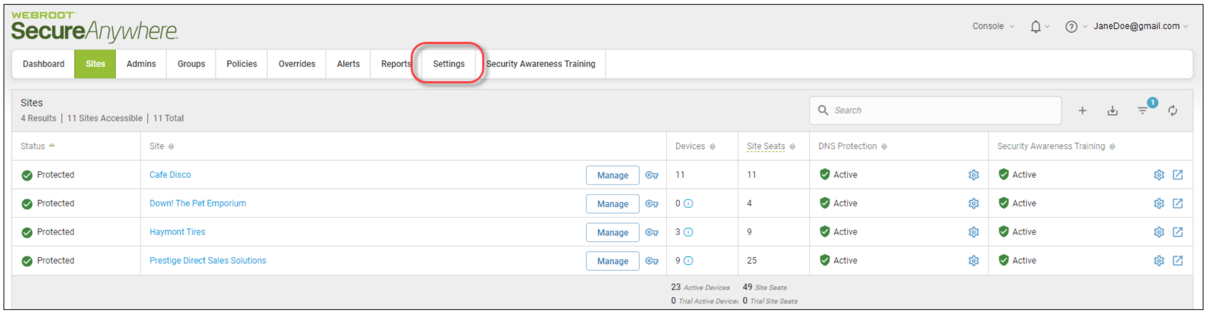
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

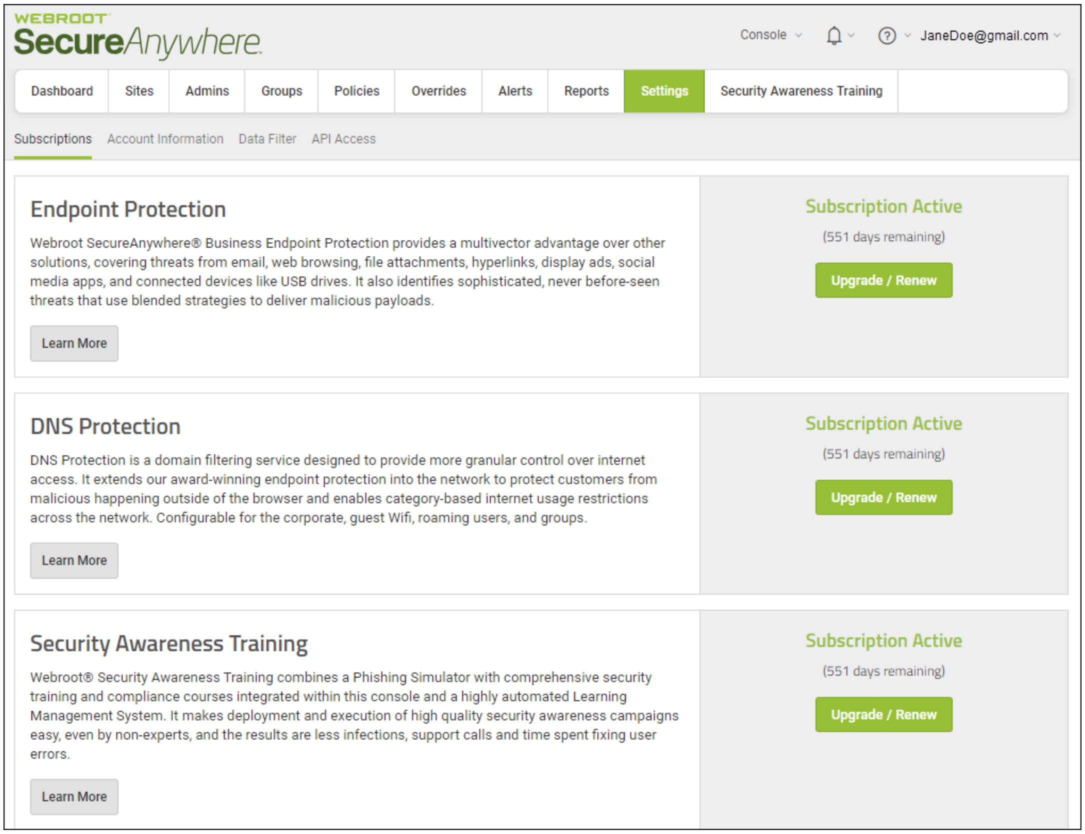
2. Click the **Settings** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Settings tab displays with the Subscriptions tab active.



## Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

## DNS Protection

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.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

## Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

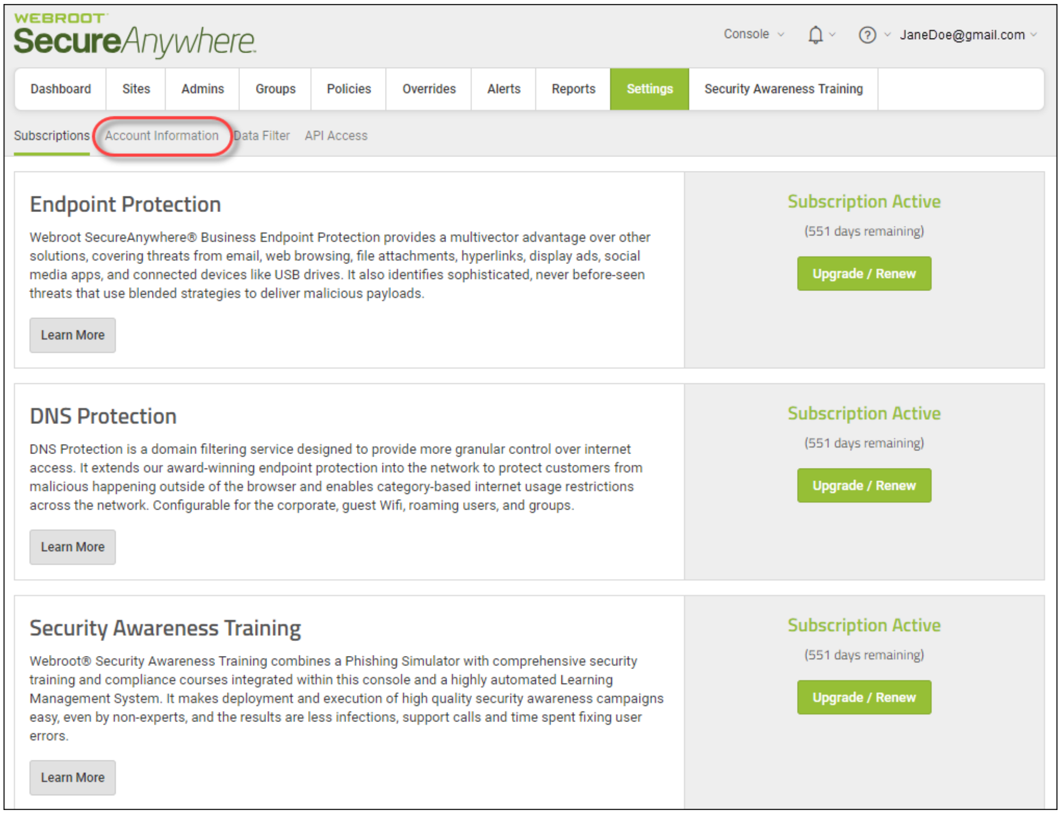
Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

3. Click the **Account Information** tab.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

DNS Protection

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.

Learn More

Subscription Active

(551 days remaining)

Upgrade / Renew

Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Learn More

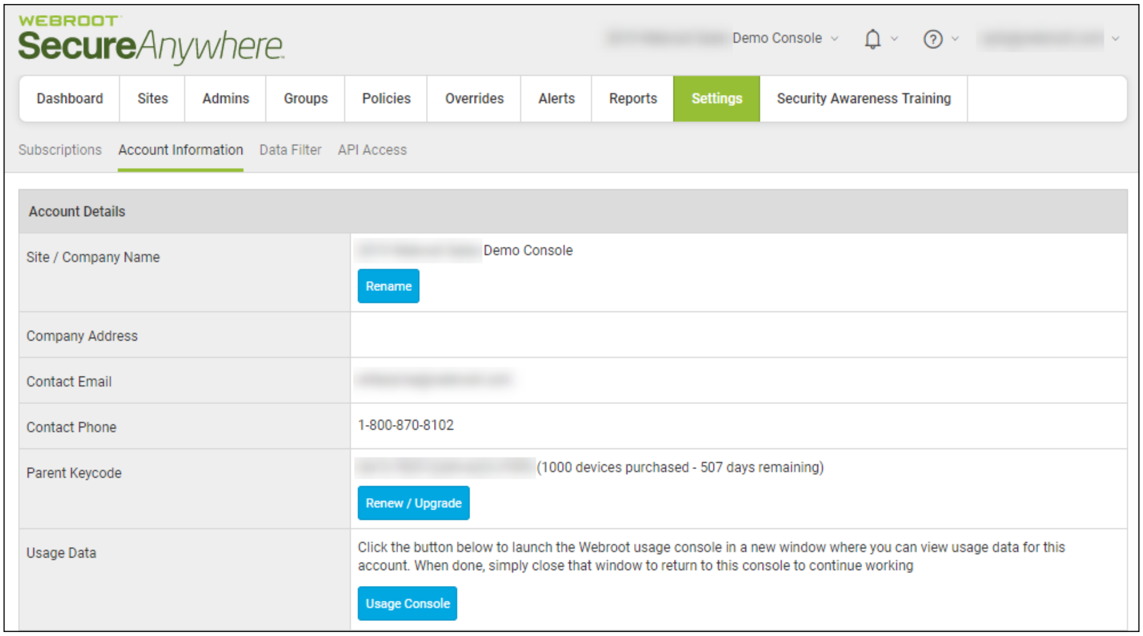
Subscription Active

(551 days remaining)

Upgrade / Renew

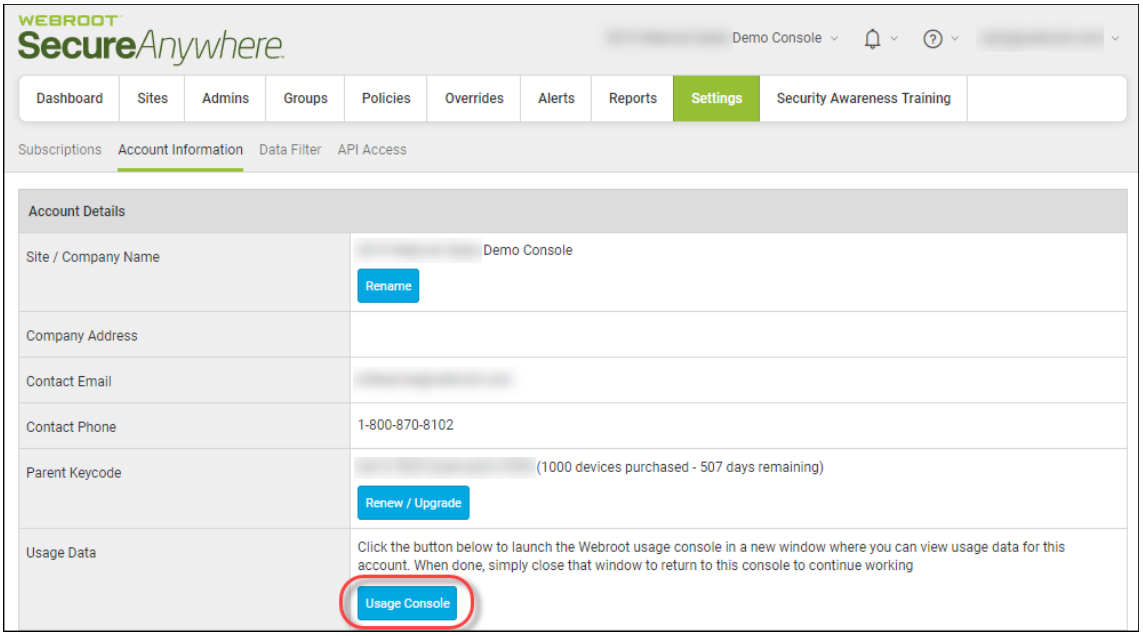
The Account Information tab displays the following information:

- Site/Company name
- Company address
- Contact email
- Contact phone
- Parent keycode, which you can renew or upgrade. Click the **Renew/Upgrade** button to display information about your Channel Partner or Webroot account Manager, either of whom can assist you with renewing or upgrading.



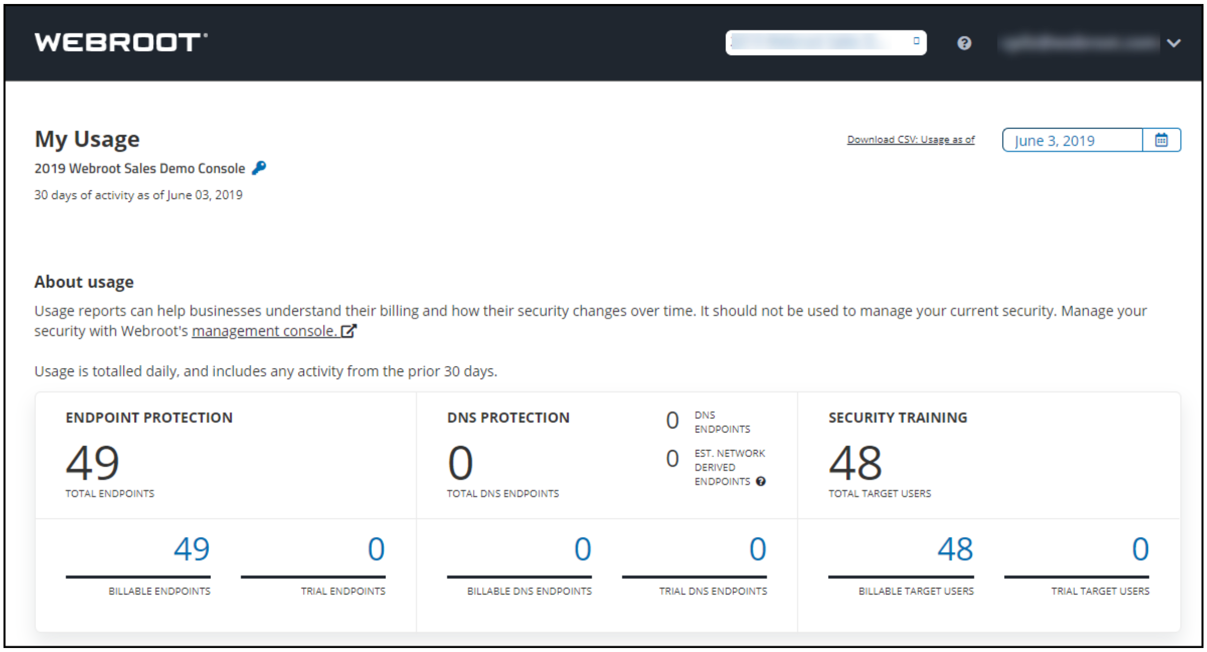
| Account Details | |
|---|---|
| Site / Company Name | [redacted] Demo Console |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | 1-800-870-8102 |
| Parent Keycode | [redacted] (1000 devices purchased - 507 days remaining) |
| Usage Data | Click the button below to launch the Webroot usage console in a new window where you can view usage data for this account. When done, simply close that window to return to this console to continue working |

4. Click the **Usage Console** button.



| Account Details | |
|---|---|
| Site / Company Name | [redacted] Demo Console |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | 1-800-870-8102 |
| Parent Keycode | [redacted] (1000 devices purchased - 507 days remaining) |
| Usage Data | Click the button below to launch the Webroot usage console in a new window where you can view usage data for this account. When done, simply close that window to return to this console to continue working |

The My Usage console displays.



## My Usage

2019 Webroot Sales Demo Console

30 days of activity as of June 03, 2019

Download CSV: Usage as of June 3, 2019

### About usage

Usage reports can help businesses understand their billing and how their security changes over time. It should not be used to manage your current security. Manage your security with Webroot's management console.

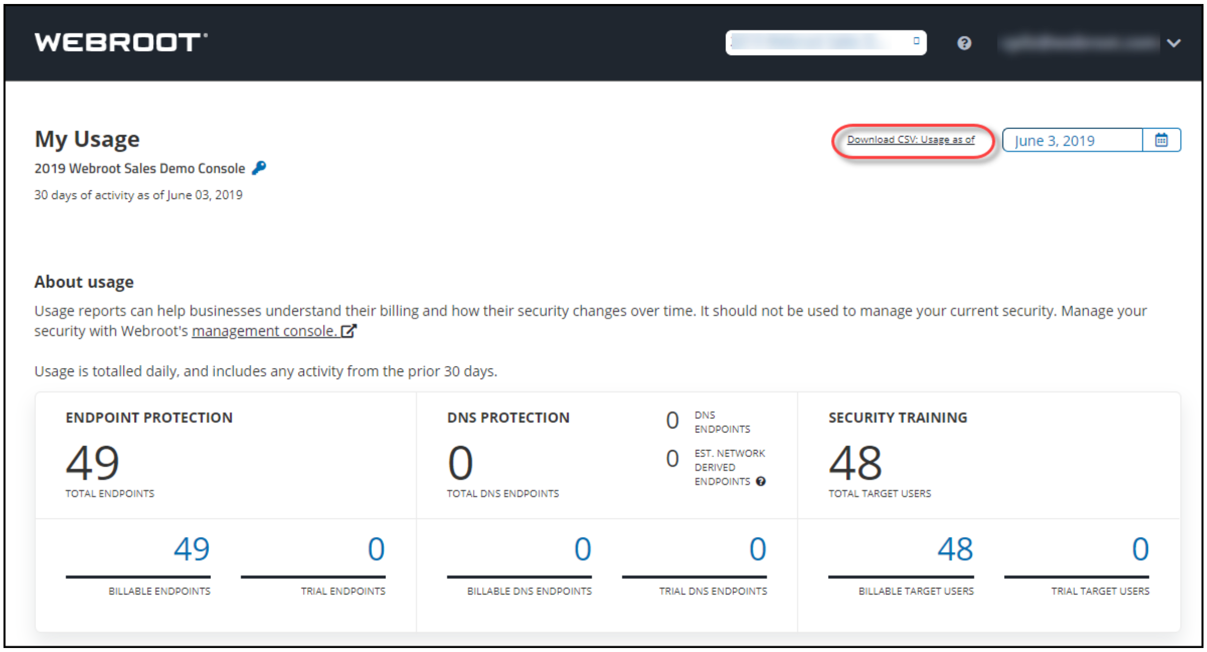
Usage is totalled daily, and includes any activity from the prior 30 days.

ENDPOINT PROTECTION
49 TOTAL ENDPOINTS
49 BILLABLE ENDPOINTS
0 TRIAL ENDPOINTS

DNS PROTECTION
0 TOTAL DNS ENDPOINTS
0 DNS ENDPOINTS
0 EST. NETWORK DERIVED ENDPOINTS
0 BILLABLE DNS ENDPOINTS
0 TRIAL DNS ENDPOINTS

SECURITY TRAINING
48 TOTAL TARGET USERS
48 BILLABLE TARGET USERS
0 TRIAL TARGET USERS

5. After you have used the Date Picker to select the date range, click the **Download CSV Usage as of** link.


WEBROOT
[redacted]
[redacted]

My Usage

2019 Webroot Sales Demo Console

30 days of activity as of June 03, 2019

Download CSV: Usage as of June 3, 2019

About usage

Usage reports can help businesses understand their billing and how their security changes over time. It should not be used to manage your current security. Manage your security with Webroot's management console.

Usage is totalled daily, and includes any activity from the prior 30 days.

ENDPOINT PROTECTION
49 TOTAL ENDPOINTS
49 BILLABLE ENDPOINTS
0 TRIAL ENDPOINTS

DNS PROTECTION
0 TOTAL DNS ENDPOINTS
0 DNS ENDPOINTS
0 EST. NETWORK DERIVED ENDPOINTS
0 BILLABLE DNS ENDPOINTS
0 TRIAL DNS ENDPOINTS

SECURITY TRAINING
48 TOTAL TARGET USERS
48 BILLABLE TARGET USERS
0 TRIAL TARGET USERS

Webroot downloads a CSV file to your computer.

6. Click on the download to open the file and view the information. The spreadsheet contains the following information:
   - GSM Key
   - Usage Date
   - Site Key
   - Site Name
   - Site State
   - SAEP Total Endpoints
   - DNSP Enabled
   - DNSP License Type
   - Total DNSP Devices Actual
   - DNSP EST Network Derived Endpoints
   - Total DNSP Agents
   - WSAT Enabled
   - WSAT License Type
   - Total WSAT Users

# Setting GSM-Level Data Filters

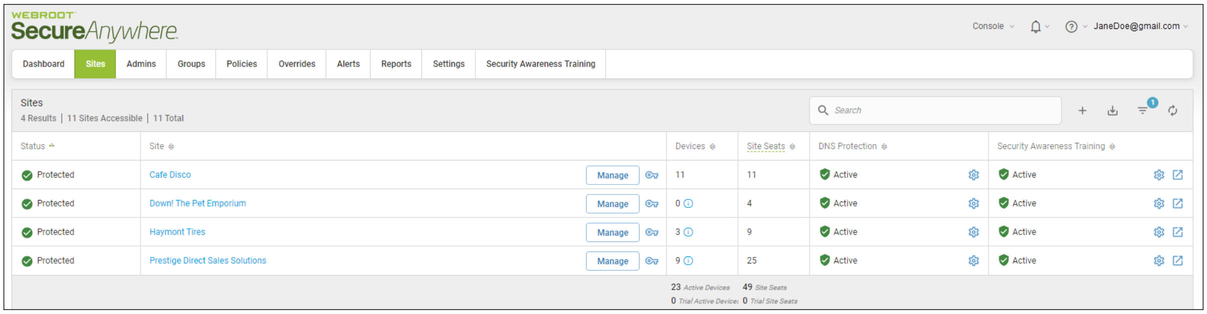
Within the management console, you can remove endpoints from your data that have not been seen for a set period of time, giving you the most accurate data for the current state-of-play of your deployment.

You can set a master setting in your management console to be inherited by all sites under that management console, or set sites individually. Your Dashboard and Scheduled Reports will only display endpoints which have been seen in the time period you select.

**To set a management console-level data filter:**

1. Log in to the management console.

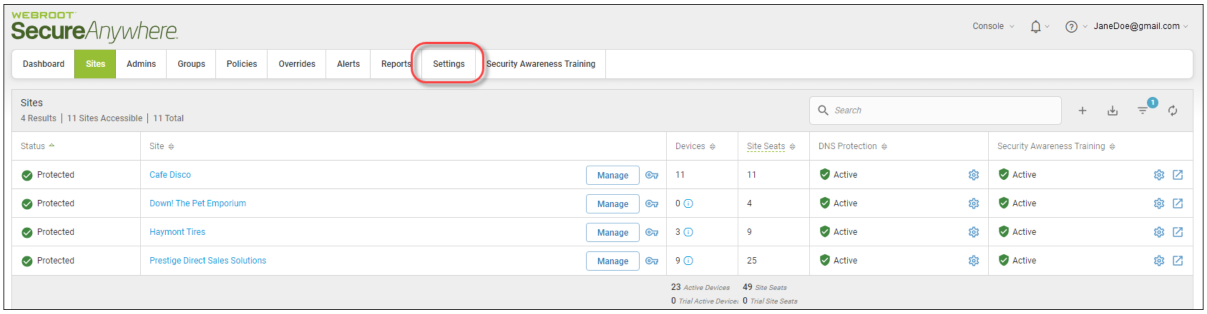
   The management console displays with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

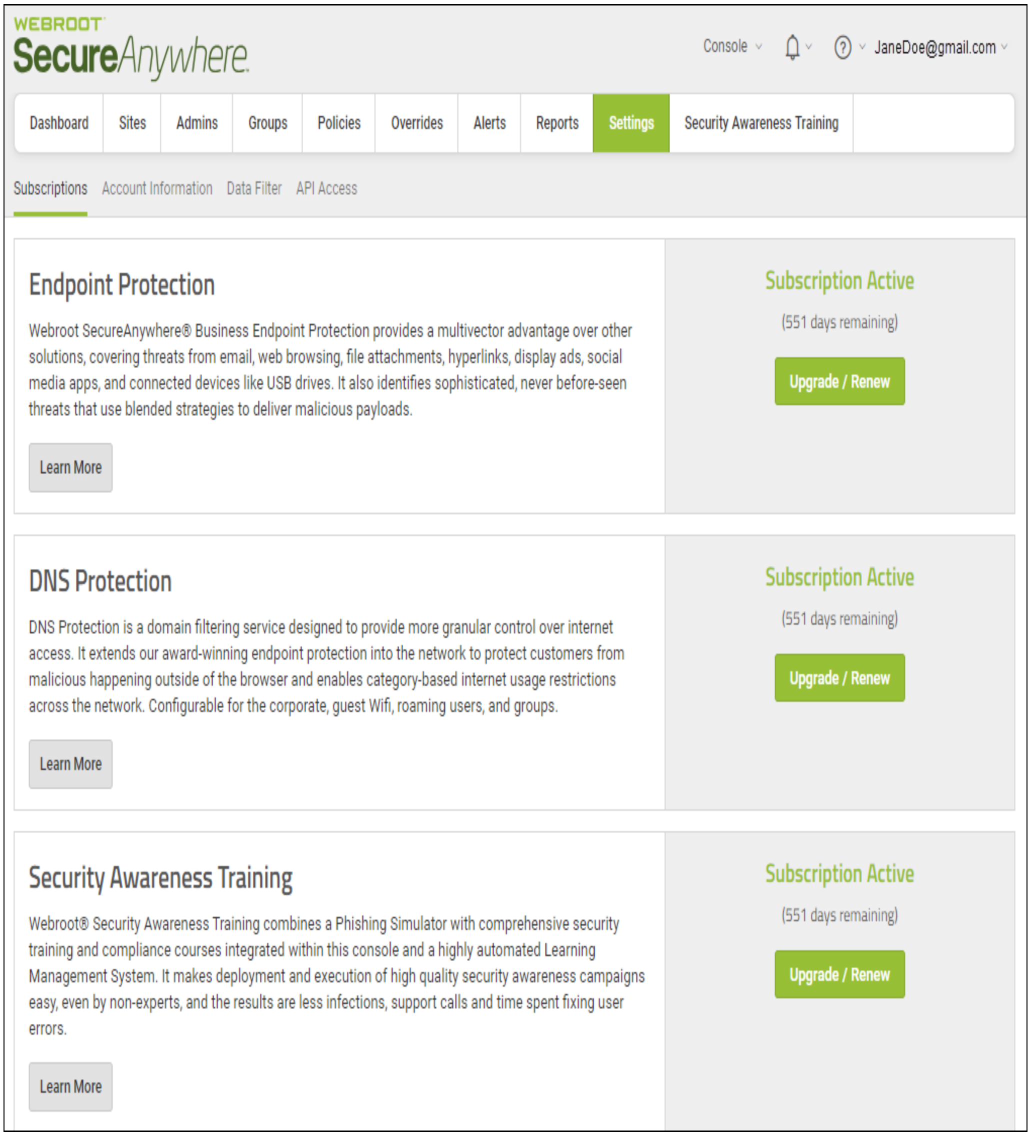
| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

2. Click the **Settings** tab.


Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Settings tab displays, with the Subscription tab active.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Subscription Active

(551 days remaining)

DNS Protection

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.

Subscription Active

(551 days remaining)

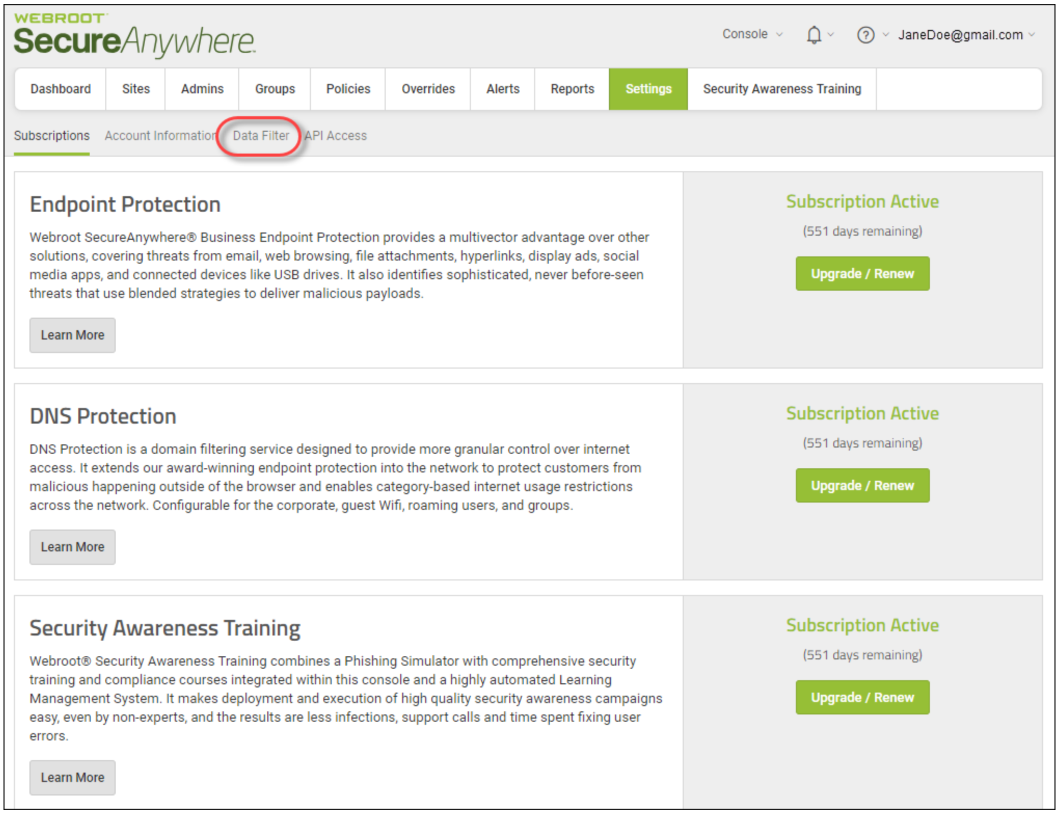
Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Subscription Active

(551 days remaining)

3. Click the **Data Filter** tab.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Subscription Active

(551 days remaining)

DNS Protection

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.

Subscription Active

(551 days remaining)

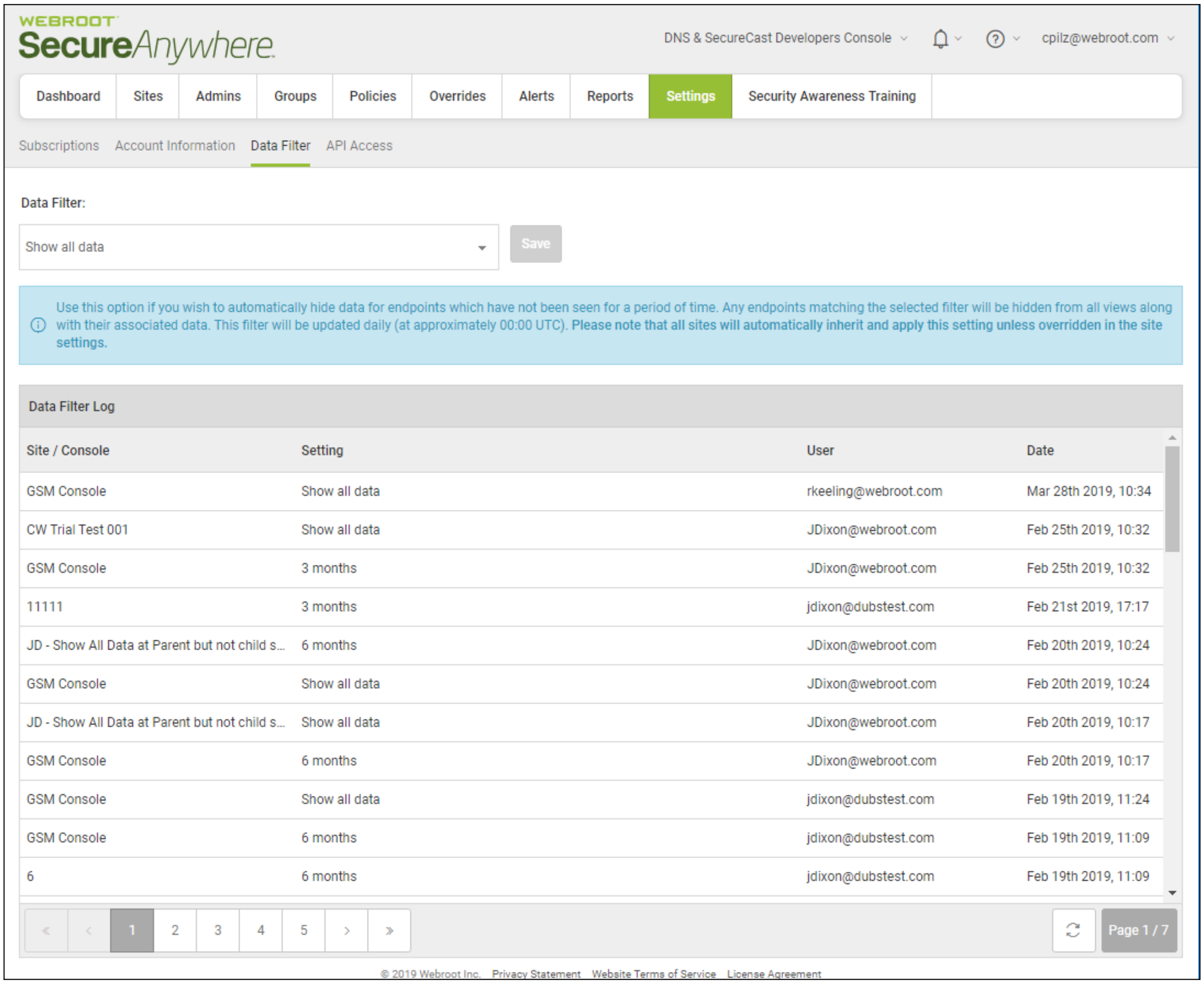
Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Subscription Active

(551 days remaining)

The system displays the Data Filter tab.



Data Filter:

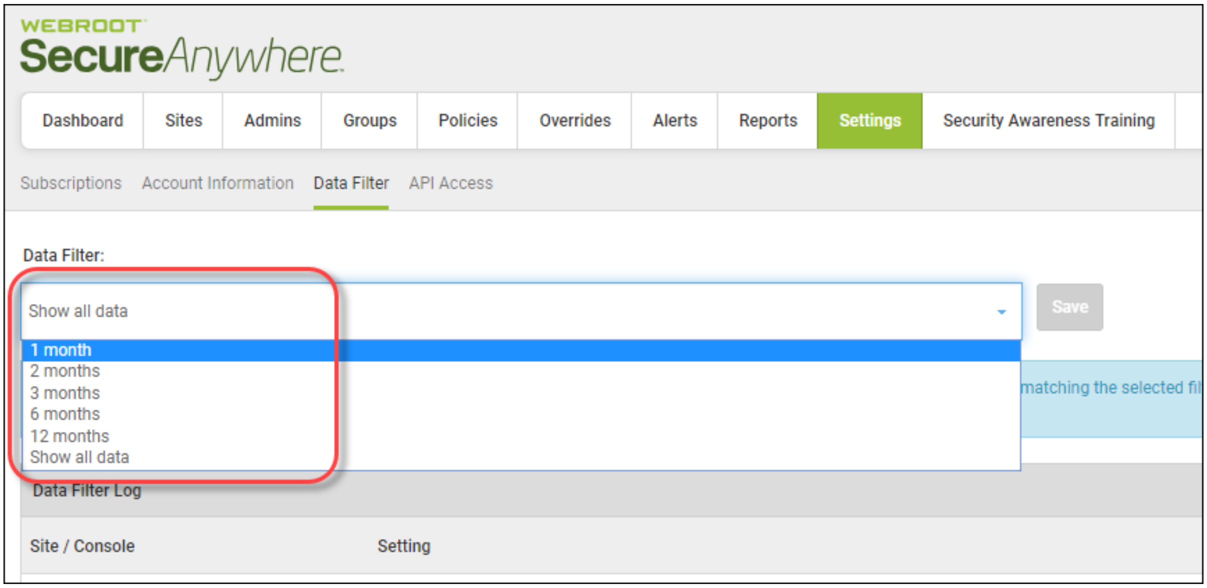
Show all data

Use this option if you wish to automatically hide data for endpoints which have not been seen for a period of time. Any endpoints matching the selected filter will be hidden from all views along with their associated data. This filter will be updated daily (at approximately 00:00 UTC). **Please note that all sites will automatically inherit and apply this setting unless overridden in the site settings.**

Data Filter Log

| Site / Console | Setting | User | Date |
|---|---|---|---|
| GSM Console | Show all data | rkeeling@webroot.com | Mar 28th 2019, 10:34 |
| CW Trial Test 001 | Show all data | JDixon@webroot.com | Feb 25th 2019, 10:32 |
| GSM Console | 3 months | JDixon@webroot.com | Feb 25th 2019, 10:32 |
| 11111 | 3 months | jdixon@dubstest.com | Feb 21st 2019, 17:17 |
| JD - Show All Data at Parent but not child s... | 6 months | JDixon@webroot.com | Feb 20th 2019, 10:24 |
| GSM Console | Show all data | JDixon@webroot.com | Feb 20th 2019, 10:24 |
| JD - Show All Data at Parent but not child s... | Show all data | JDixon@webroot.com | Feb 20th 2019, 10:17 |
| GSM Console | 6 months | JDixon@webroot.com | Feb 20th 2019, 10:17 |
| GSM Console | Show all data | jdixon@dubstest.com | Feb 19th 2019, 11:24 |
| GSM Console | 6 months | jdixon@dubstest.com | Feb 19th 2019, 11:09 |
| 6 | 6 months | jdixon@dubstest.com | Feb 19th 2019, 11:09 |

4. From the Data Filter drop-down menu, select one of the following:
   - **Show all data; this is the default setting**
   - **1 month**
   - **2 months**
   - **3 months**
   - **6 months**
   - **12 months**

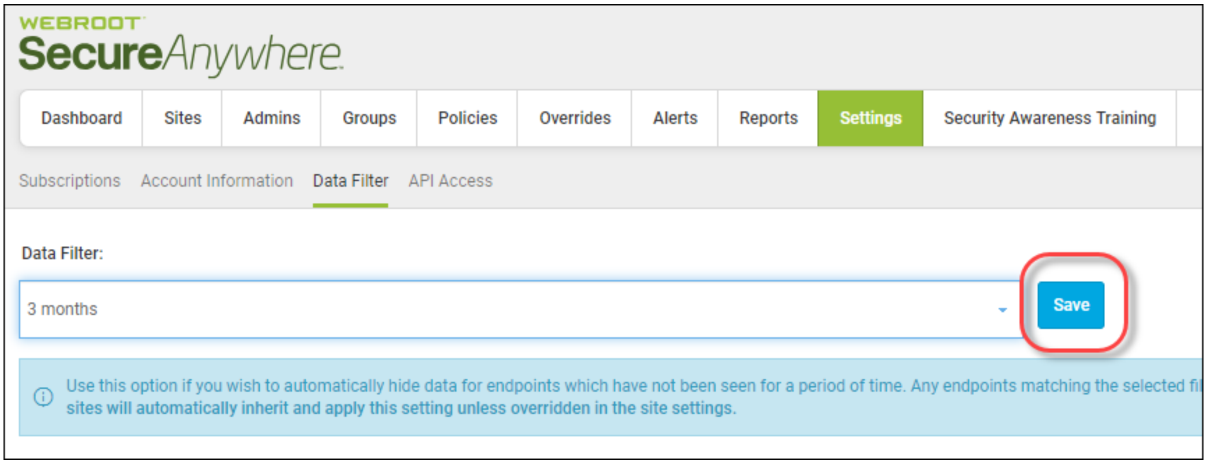


Data Filter: Show all data

matching the selected fi

**Note:** When using the data filter settings, data is not deleted, but simply hidden from the dataset you are viewing based on your options. Selecting a different time period or selecting to display all data will always display all endpoint information relevant to your selection

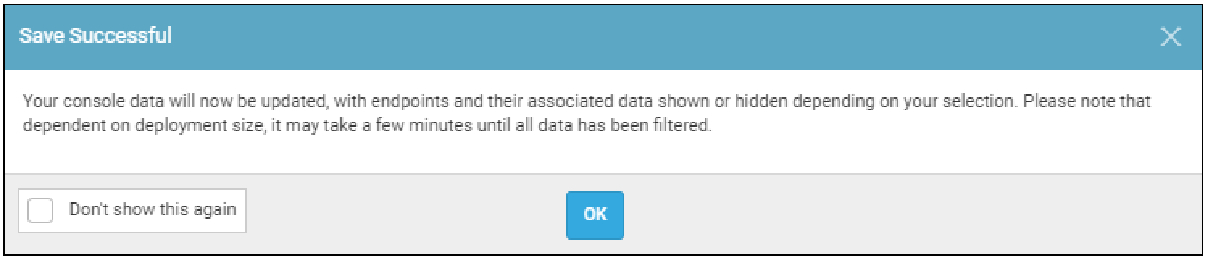
5. When you're done, click the**Save** button.



Data Filter: 3 months

ⓘ Use this option if you wish to automatically hide data for endpoints which have not been seen for a period of time. Any endpoints matching the selected fi
sites will automatically inherit and apply this setting unless overridden in the site settings.

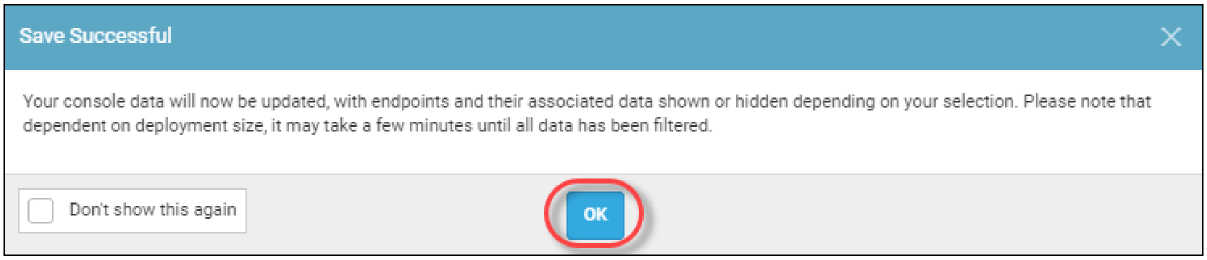
The system displays a note indicating that your changes have been saved.



Your console data will now be updated, with endpoints and their associated data shown or hidden depending on your selection. Please note that dependent on deployment size, it may take a few minutes until all data has been filtered.

□ Don't show this again

6. Click the **OK** button.



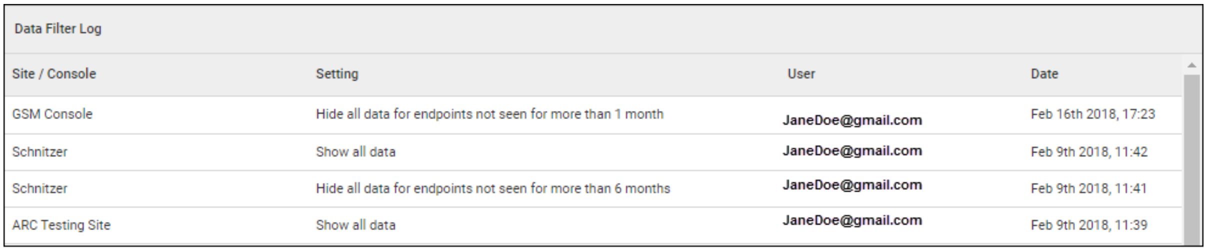
Your console data will now be updated, with endpoints and their associated data shown or hidden depending on your selection. Please note that dependent on deployment size, it may take a few minutes until all data has been filtered.

□ Don't show this again

**Note:** If needed, select the **Don't show this again** checkbox to have the system not display the Save Successful message in future.

The lower half of the Settings panel displays a Data Filter log, which audits and logs all changes made to data filter settings. The log includes the following information:

- **Site/Console** — The site the change was applied to or the management console parent setting that was changed.
- **Setting** — The option that was selected.
- **User** — The name of the user who made the change.
- **Date** — The date and time the change was made.



Data Filter Log

| Site / Console | Setting | User | Date |
|---|---|---|---|
| GSM Console | Hide all data for endpoints not seen for more than 1 month | JaneDoe@gmail.com | Feb 16th 2018, 17:23 |
| Schnitzer | Show all data | JaneDoe@gmail.com | Feb 9th 2018, 11:42 |
| Schnitzer | Hide all data for endpoints not seen for more than 6 months | JaneDoe@gmail.com | Feb 9th 2018, 11:41 |
| ARC Testing Site | Show all data | JaneDoe@gmail.com | Feb 9th 2018, 11:39 |

# Creating API Client Credentials

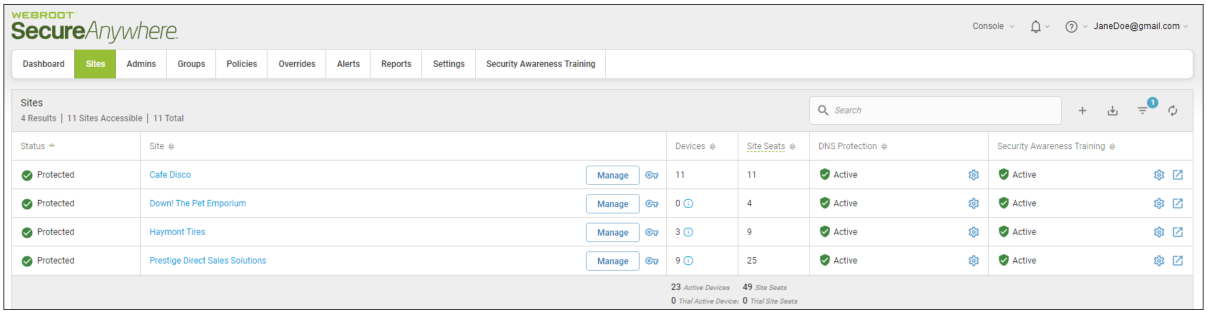
Creating API client credentials allows you to connect with the Unity API system using a secure, authenticated connection between SecureAnywhere and your managed systems. This, in turn, allows you to automate billing, reporting, deployment, and other processes.

For more information on API, see Webroot Unity API.

**To create an API client credential:**

1. Log in to the management console.

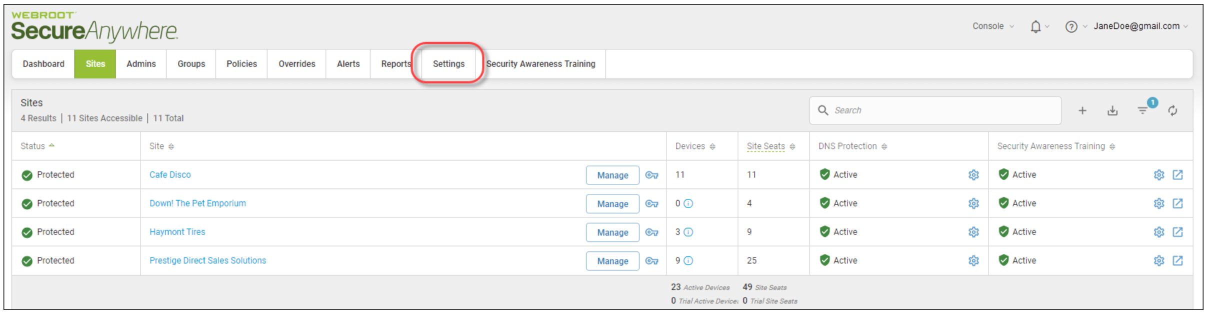
   The management console displays, with the Sites tab active.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

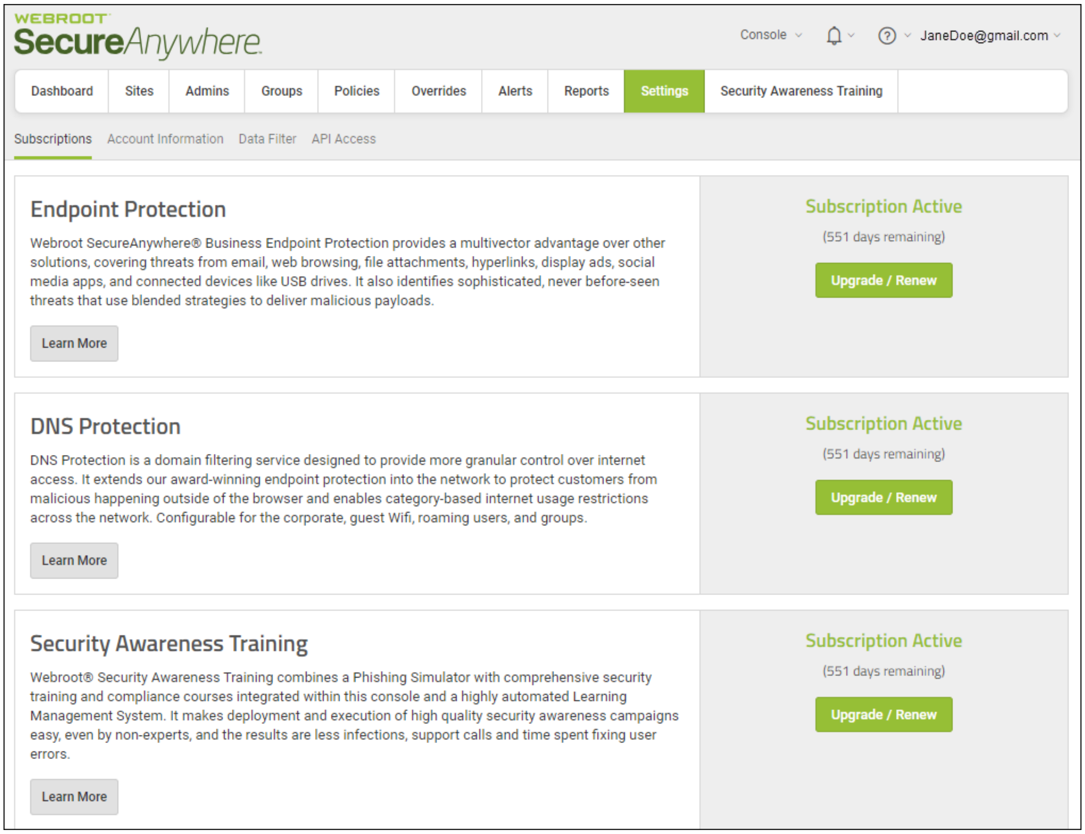
2. Click the **Settings** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

| Status | Site | | Devices | Site Seats | DNS Protection | Security Awareness Training |
|---|---|---|---|---|---|---|
| Protected | Cafe Disco | Manage | 11 | 11 | Active | Active |
| Protected | Down! The Pet Emporium | Manage | 0 | 4 | Active | Active |
| Protected | Haymont Tires | Manage | 3 | 9 | Active | Active |
| Protected | Prestige Direct Sales Solutions | Manage | 9 | 25 | Active | Active |
| | | | 23 Active Devices<br>0 Trial Active Device: | 49 Site Seats<br>0 Trial Site Seats | | |

   The Settings tab displays with the Subscriptions tab active.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Subscription Active

(551 days remaining)

DNS Protection

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.

Subscription Active

(551 days remaining)

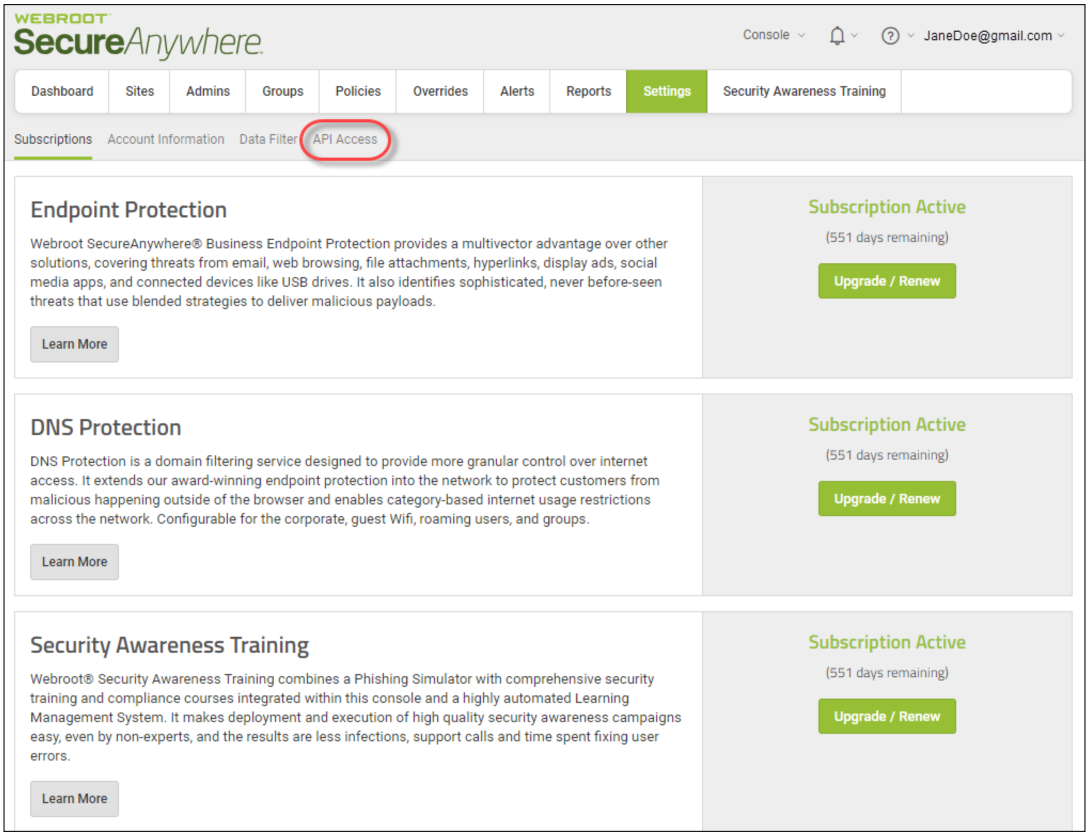
Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Subscription Active

(551 days remaining)

3. Click the **API Access** tab.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

Subscription Active

(551 days remaining)

DNS Protection

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.

Subscription Active

(551 days remaining)

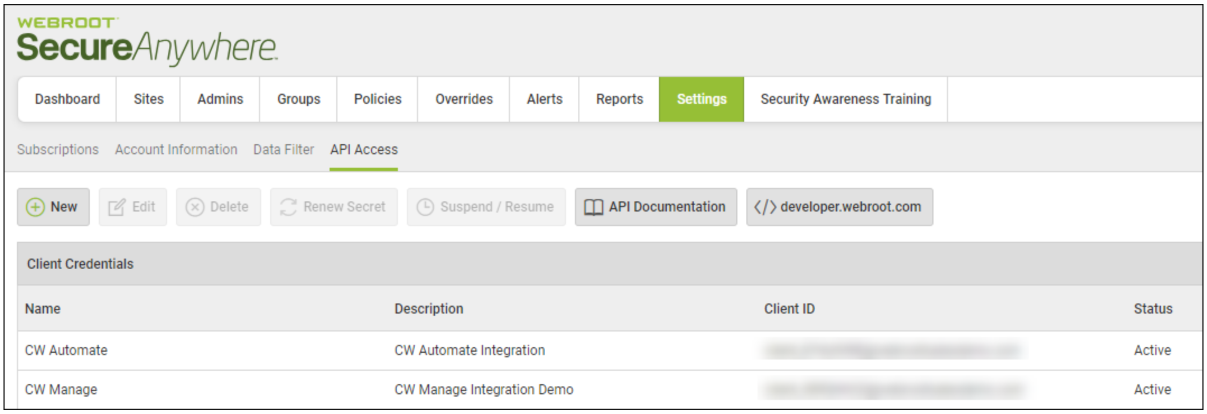
Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

Subscription Active

(551 days remaining)

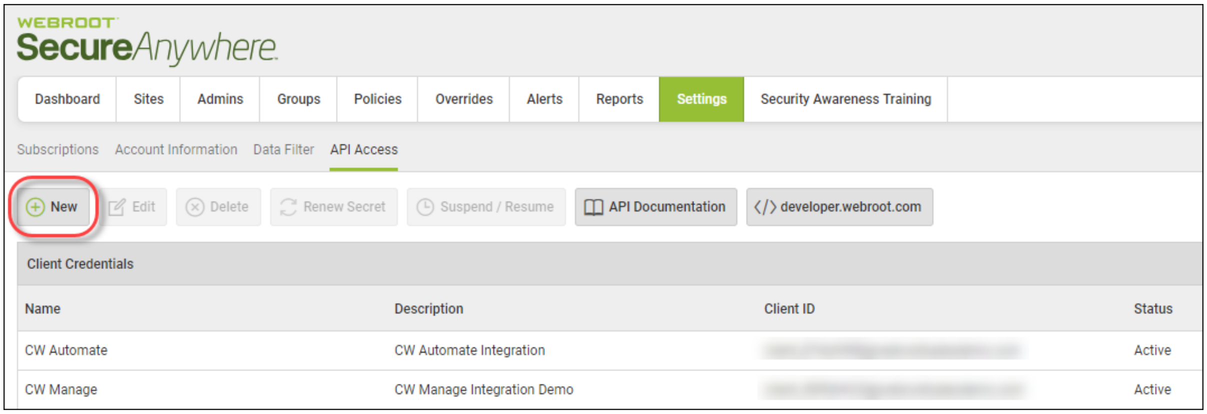
The API access tab displays.



Client Credentials

| Name | Description | Client ID | Status |
|---|---|---|---|
| CW Automate | CW Automate Integration | [redacted] | Active |
| CW Manage | CW Manage Integration Demo | [redacted] | Active |

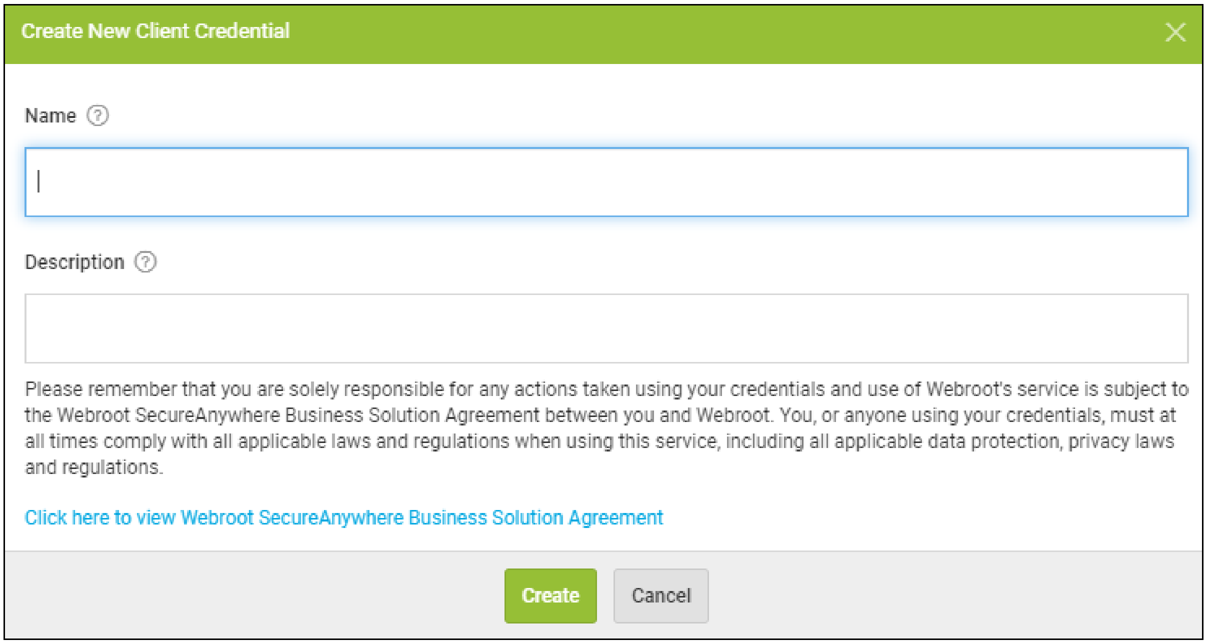
4. Click the **New** button.



Client Credentials

| Name | Description | Client ID | Status |
|---|---|---|---|
| CW Automate | CW Automate Integration | [redacted] | Active |
| CW Manage | CW Manage Integration Demo | [redacted] | Active |

The Create New Client Credential window displays.

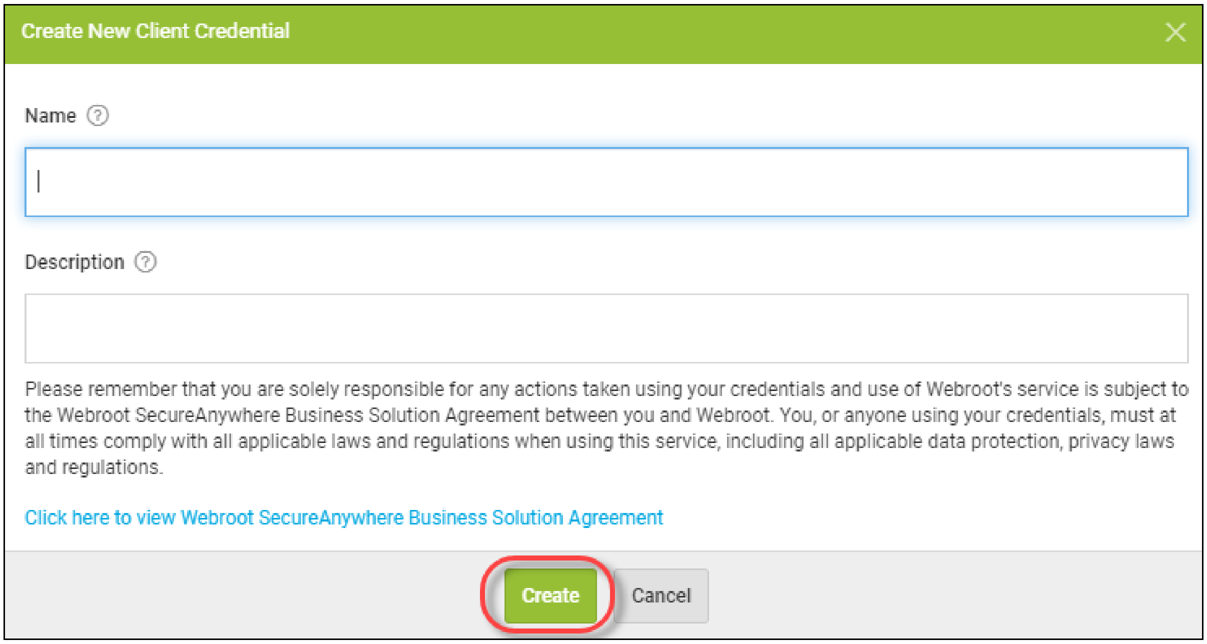


Please remember that you are solely responsible for any actions taken using your credentials and use of Webroot's service is subject to the Webroot SecureAnywhere Business Solution Agreement between you and Webroot. You, or anyone using your credentials, must at all times comply with all applicable laws and regulations when using this service, including all applicable data protection, privacy laws and regulations.

Click here to view Webroot SecureAnywhere Business Solution Agreement

5. In the Name field, enter the name of the credential.
6. In the Description field, enter a short description of the credential.
7. Click the **Click here to view Webroot SecureAnywhere Business Solution** link, and review the service terms and conditions for [Webroot Unity SDK and Unity API Agreement](#).

8. When you're done, click the **Create** button.



Create New Client Credential

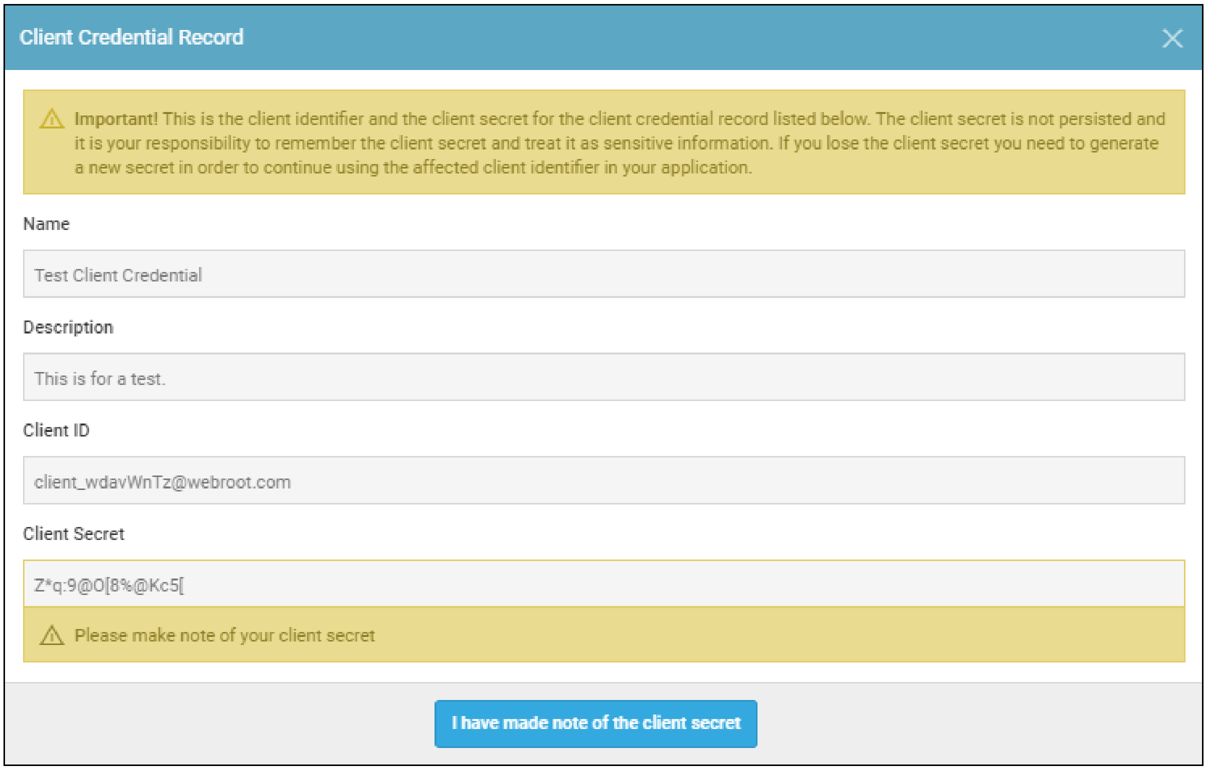
Name

Description

Please remember that you are solely responsible for any actions taken using your credentials and use of Webroot's service is subject to the Webroot SecureAnywhere Business Solution Agreement between you and Webroot. You, or anyone using your credentials, must at all times comply with all applicable laws and regulations when using this service, including all applicable data protection, privacy laws and regulations.

Click here to view Webroot SecureAnywhere Business Solution Agreement

The system displays the Client Credential Record window. This window displays the name and description of the credential, reflecting what you entered, but also the Client ID, which displays in the Client ID column.



⚠ Important! This is the client identifier and the client secret for the client credential record listed below. The client secret is not persisted and it is your responsibility to remember the client secret and treat it as sensitive information. If you lose the client secret you need to generate a new secret in order to continue using the affected client identifier in your application.

Name

Test Client Credential

Description

This is for a test.

Client ID

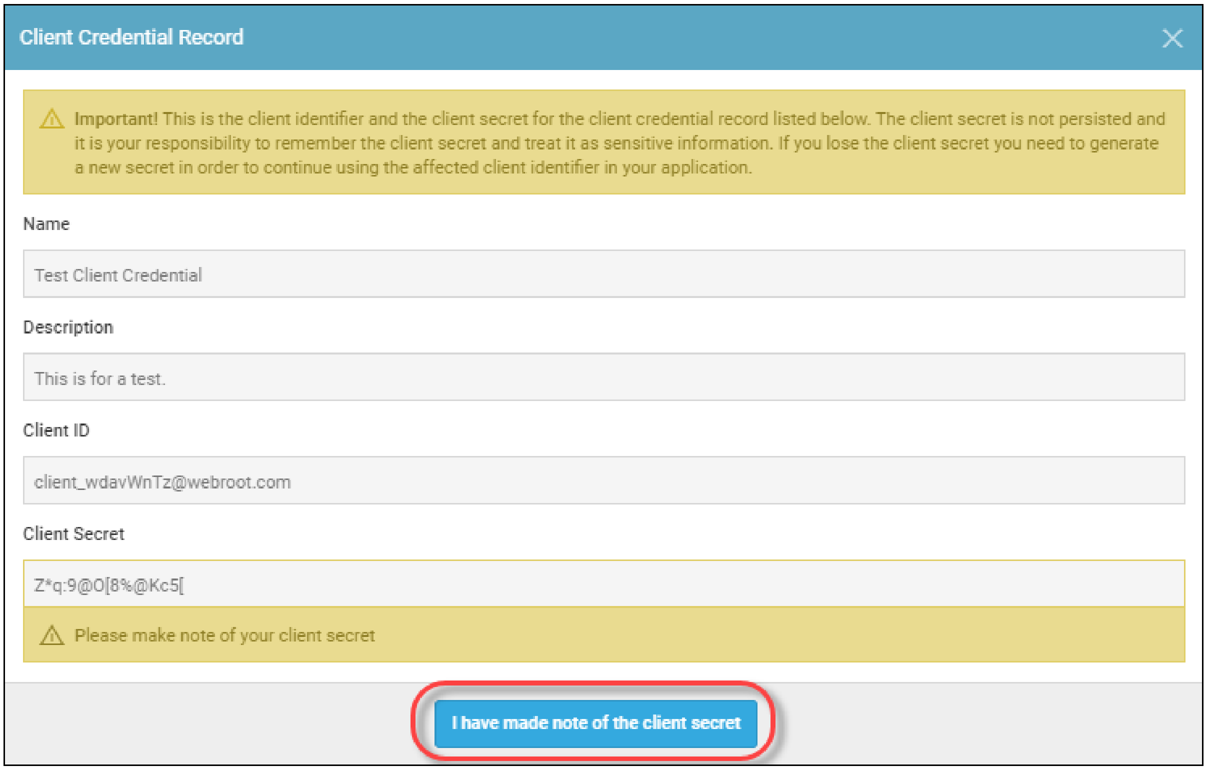
client_wdavWnTz@webroot.com

Client Secret

Z*q:9@O[8%@Kc5[

⚠ Please make note of your client secret

More importantly, the window displays the client secret, which is not displayed in the console. You must make note of the client secret, after which, click the **I have made note of the client secret** button.



⚠ Important! This is the client identifier and the client secret for the client credential record listed below. The client secret is not persisted and it is your responsibility to remember the client secret and treat it as sensitive information. If you lose the client secret you need to generate a new secret in order to continue using the affected client identifier in your application.

Name: Test Client Credential

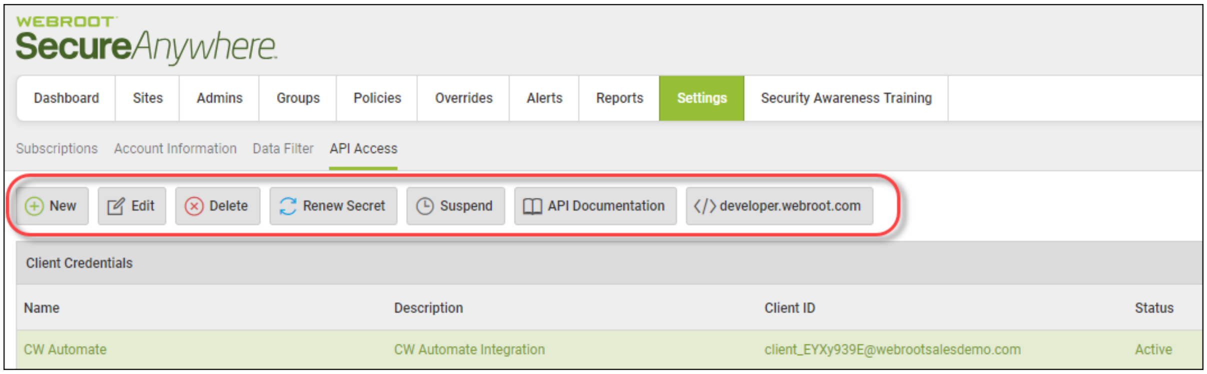
Description: This is for a test.

Client ID: client_wdavWnTz@webroot.com

Client Secret: Z*q:9@O[8%@Kc5[

⚠ Please make note of your client secret

9. As needed, you can highlight the client line item and perform any of the following functions:
   - To edit a client credential, click the **Edit** button, and update the fields. When you're done, click the **Save Changes** button.
   - To delete a client credential, click the **Delete** button. Confirm the deletion by clicking the **Delete** button.
   - To create a new client secret, click the **Renew Secret** button, and take note of the new client secret before clicking the **I have made note of the client secret** button.
   - To suspend a client, click the **Suspend** button. Confirm the suspension by clicking the **Suspend** button.
   - To access relevant documentation, click the **Unity API** button.
   - To access relevant documentation, click the **Developer** button.



Client Credentials

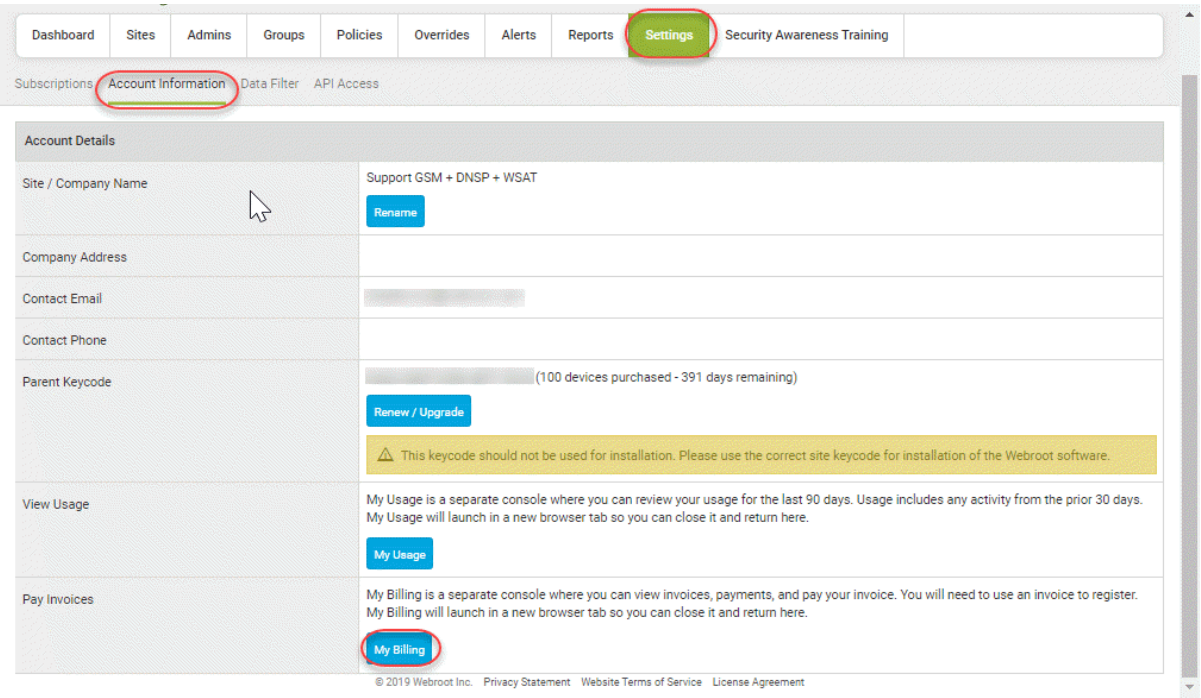
| Name | Description | Client ID | Status |
|---|---|---|---|
| CW Automate | CW Automate Integration | client_EYXy939E@webrootsalesdemo.com | Active |

# Accessing the My Billing portal

The My Billing portal is accessible for those that pay Webroot directly. If you are an MSP that pays your Webroot bill through an RMM integration or are a company that purchases Webroot services from an MSP or third party, all billing activities will happen through them. The My Billing portal will not be accessible to you. To access the My Billing portal, go to the Webroot management console, and follow the steps below:

**To access My Billing through the Webroot management console:**

1. Log into the Webroot management console.
2. In the top navigation bar, select **Settings**, then click **Account Information**, and **My Billing**.



| Account Details | |
|---|---|
| Site / Company Name | Support GSM + DNSP + WSAT<br>Rename |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | |
| Parent Keycode | [redacted] (100 devices purchased - 391 days remaining)<br>Renew / Upgrade<br>⚠ This keycode should not be used for installation. Please use the correct site keycode for installation of the Webroot software. |
| View Usage | My Usage is a separate console where you can review your usage for the last 90 days. Usage includes any activity from the prior 30 days. My Usage will launch in a new browser tab so you can close it and return here.<br>My Usage |
| Pay Invoices | My Billing is a separate console where you can view invoices, payments, and pay your invoice. You will need to use an invoice to register. My Billing will launch in a new browser tab so you can close it and return here.<br>My Billing |

© 2019 Webroot Inc. Privacy Statement Website Terms of Service License Agreement

3. The My Usage portal will display, click **My Billing** to see the billing information.

> **Note:** If this is the first time the My Billing portal is being accessed, you will have to add an account before you can see billing information. Click here for help adding an account.

**To access the My Billing portal through the My Usage portal:**

1. Go to the Webroot usage portal: https://usage.webroot.com/
2. Enter the email address and password you use to log into the Webroot management console, select the My Billing radio button and click Log In to log into the My Billing portal.

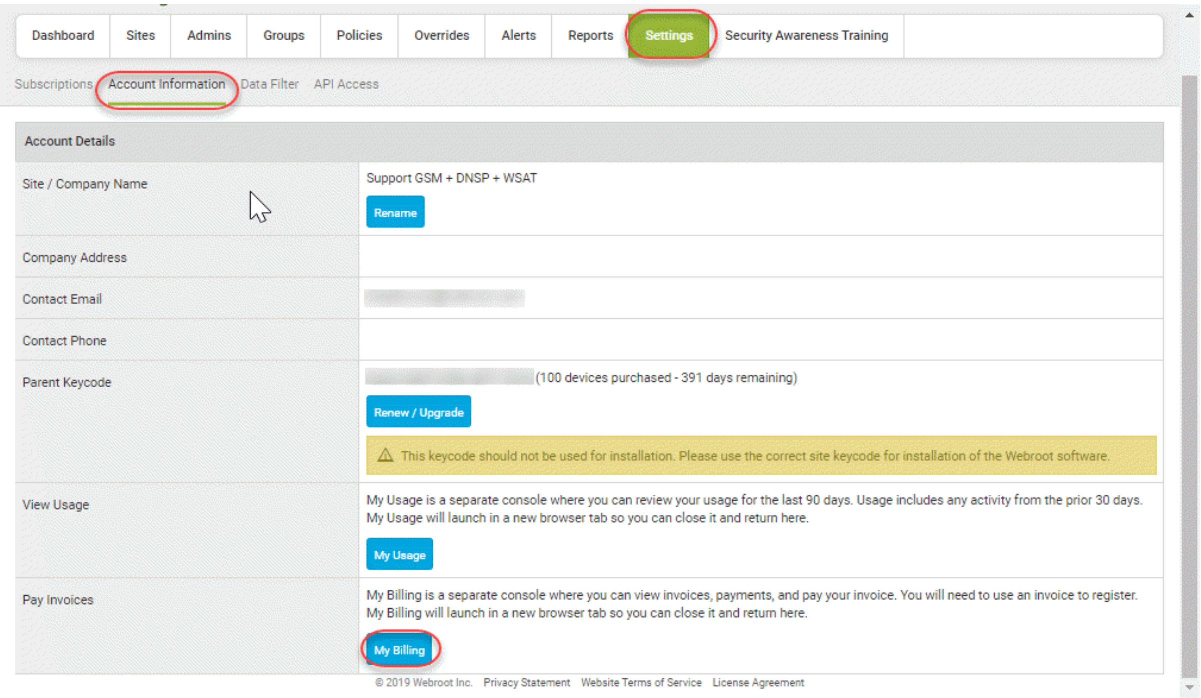
**Note:** If this is the first time accessing the My Billing portal and no accounts have been setup, you will be taken to the My Usage portal. For help adding an account, click here.

# Adding an account on the My Billing portal

Before billing information will be displayed in the My Billing portal, account information must be added.

**To add account information to the My Billing portal:**

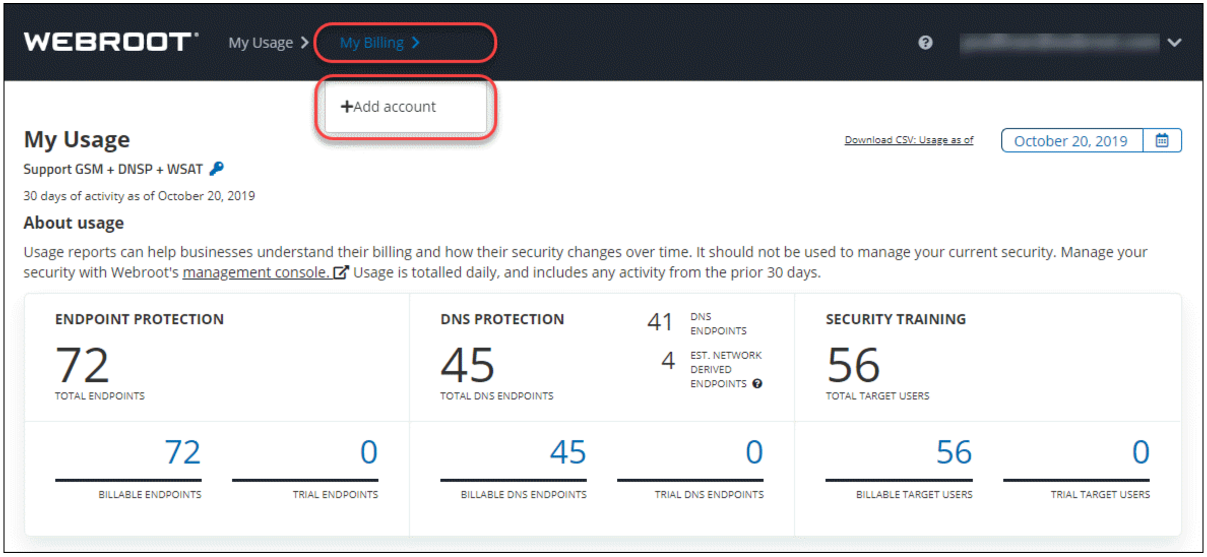
1. Log into the management console.
2. In the top navigation bar, select **Settings**, then click **Account Information** and click the **My Billing** button.



| Account Details | |
|---|---|
| Site / Company Name | Support GSM + DNSP + WSAT |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | |
| Parent Keycode | [redacted] (100 devices purchased - 391 days remaining)<br>⚠ This keycode should not be used for installation. Please use the correct site keycode for installation of the Webroot software. |
| View Usage | My Usage is a separate console where you can review your usage for the last 90 days. Usage includes any activity from the prior 30 days. My Usage will launch in a new browser tab so you can close it and return here. |
| Pay Invoices | My Billing is a separate console where you can view invoices, payments, and pay your invoice. You will need to use an invoice to register. My Billing will launch in a new browser tab so you can close it and return here. |

© 2019 Webroot Inc. Privacy Statement Website Terms of Service License Agreement

3. In the top bar, click **My Billing** and in the dropdown, click + **Add account**.



My Usage

Support GSM + DNSP + WSAT

30 days of activity as of October 20, 2019

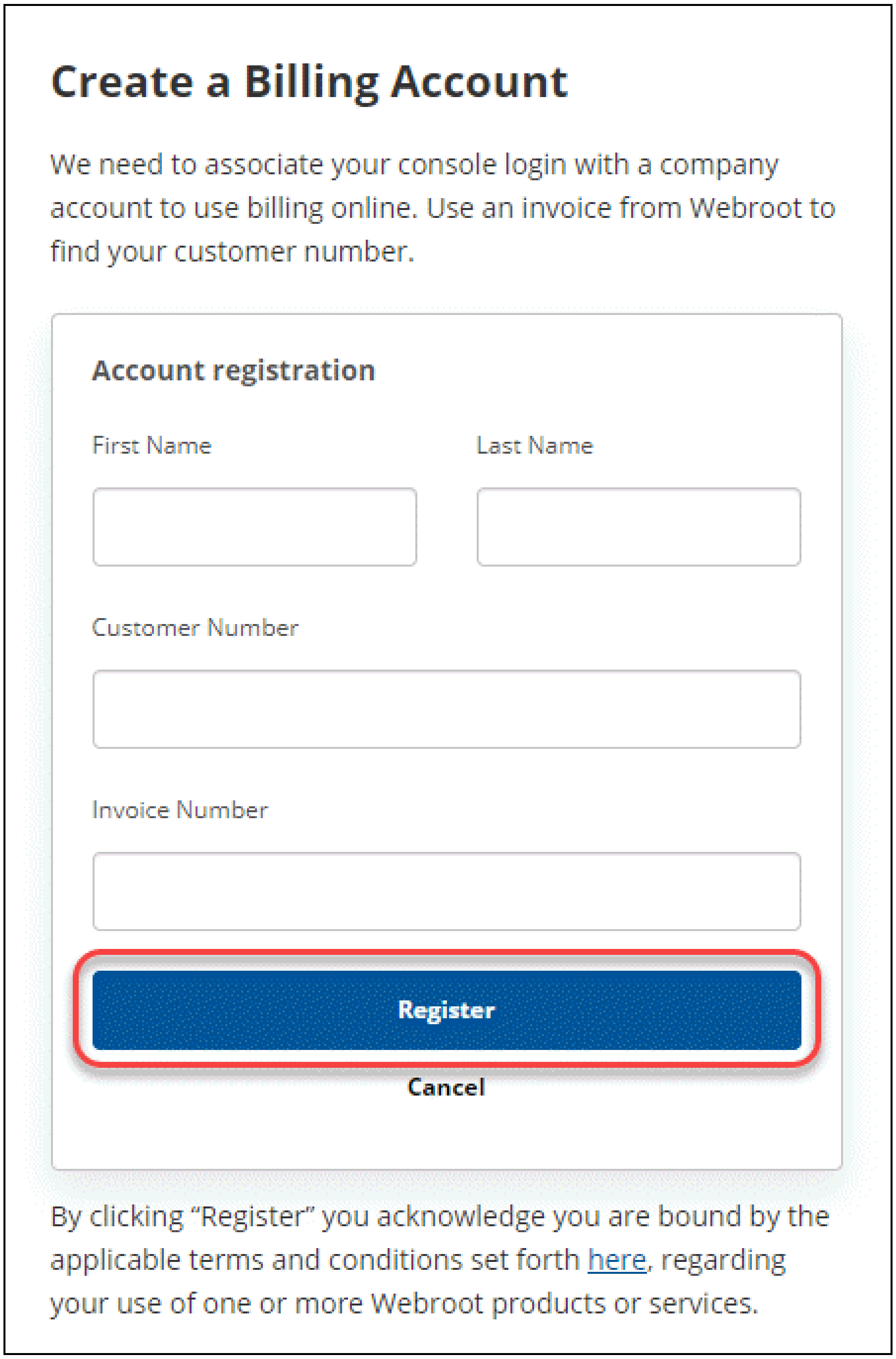
About usage

Usage reports can help businesses understand their billing and how their security changes over time. It should not be used to manage your current security. Manage your security with Webroot's management console. Usage is totalled daily, and includes any activity from the prior 30 days.

| ENDPOINT PROTECTION | | DNS PROTECTION | | SECURITY TRAINING | |
|---|---|---|---|---|---|
| 72 TOTAL ENDPOINTS | | 45 TOTAL DNS ENDPOINTS | 41 DNS ENDPOINTS<br>4 EST. NETWORK DERIVED ENDPOINTS | 56 TOTAL TARGET USERS | |
| 72 BILLABLE ENDPOINTS | 0 TRIAL ENDPOINTS | 45 BILLABLE DNS ENDPOINTS | 0 TRIAL DNS ENDPOINTS | 56 BILLABLE TARGET USERS | 0 TRIAL TARGET USERS |

4. The Create a Billing Account screen appears. Provide the requested information:

- **First Name**
- **Last Name**
- **Customer Number** – available from an invoice
- **Invoice Number** – any invoice number can be used, available from an invoice



Create a Billing Account

We need to associate your console login with a company account to use billing online. Use an invoice from Webroot to find your customer number.

Account registration

First Name

Last Name

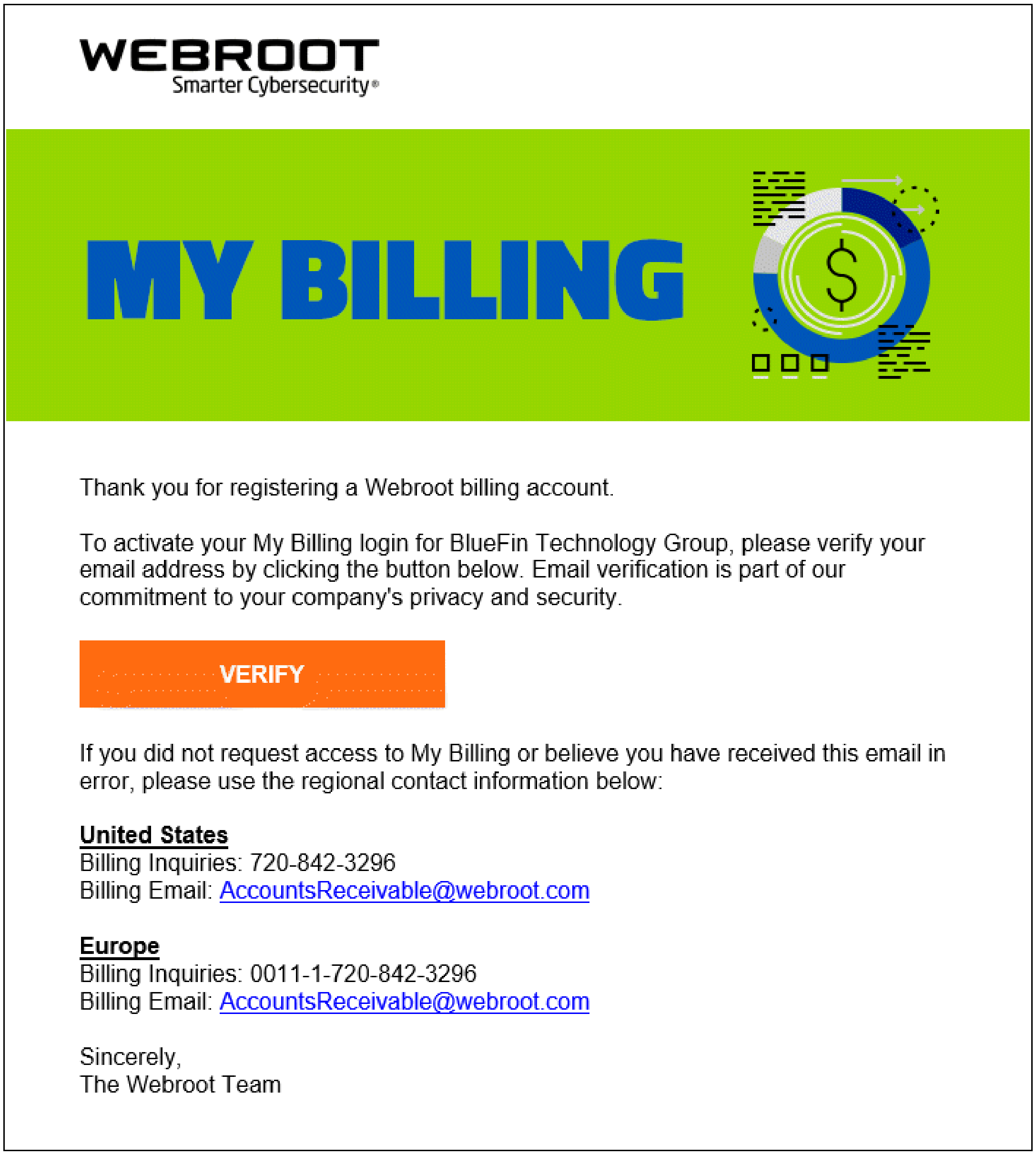
Customer Number

Invoice Number

By clicking "Register" you acknowledge you are bound by the applicable terms and conditions set forth here, regarding your use of one or more Webroot products or services.

Click **Register** to continue.

4. The My Billing portal will send an activation email message to you. Click the **Verify** button in the email message to complete the activation process.



Thank you for registering a Webroot billing account.

To activate your My Billing login for BlueFin Technology Group, please verify your email address by clicking the button below. Email verification is part of our commitment to your company's privacy and security.

If you did not request access to My Billing or believe you have received this email in error, please use the regional contact information below:

**United States**
Billing Inquiries: 720-842-3296
Billing Email: AccountsReceivable@webroot.com

**Europe**
Billing Inquiries: 0011-1-720-842-3296
Billing Email: AccountsReceivable@webroot.com

Sincerely,
The Webroot Team

**Note:** This step must be completed before billing information will be displayed.

5. Once the confirmation message has been verified, the My Billing portal will display billing information for the account. An additional email message will be sent to you informing you that the My Billing account has been activated.

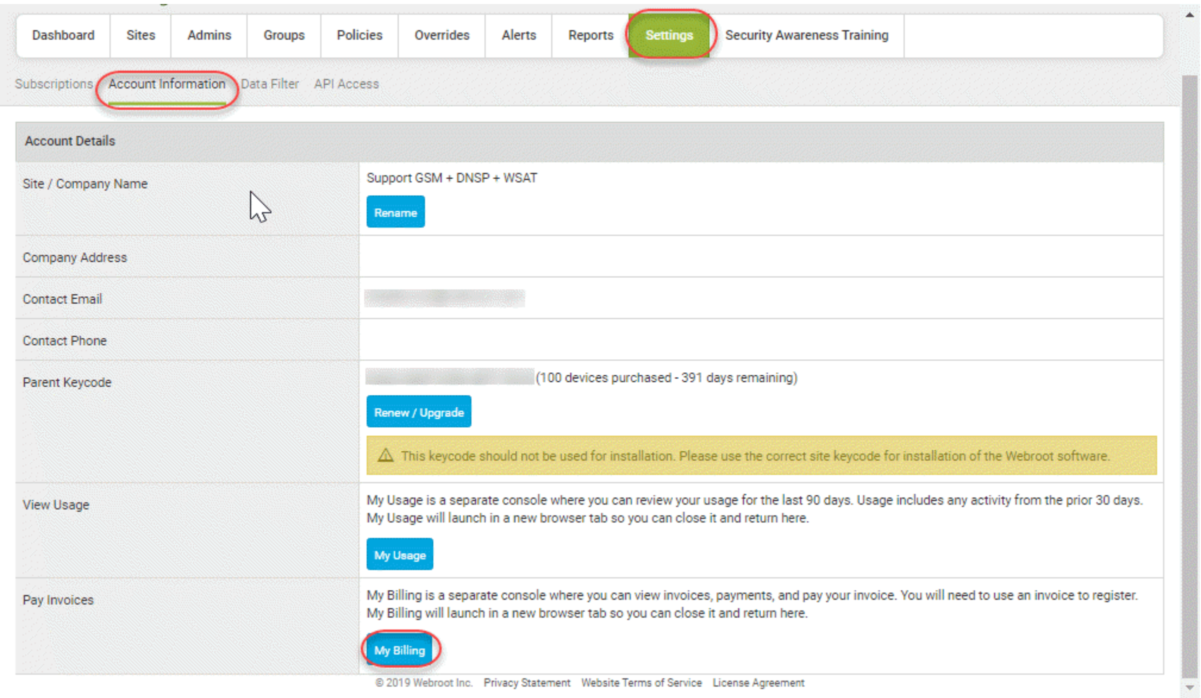
6. You can add as many accounts as you have access to—there are no limits. If multiple accounts have been added, you can switch between them by clicking My Billing in the top navigation bar and selecting the account you want to view.

# Using the My Billing Portal to Pay a Bill

You can use the My Billing portal to pay either the entire bill or an individual invoice.

**To use My Billing to pay the entire bill:**

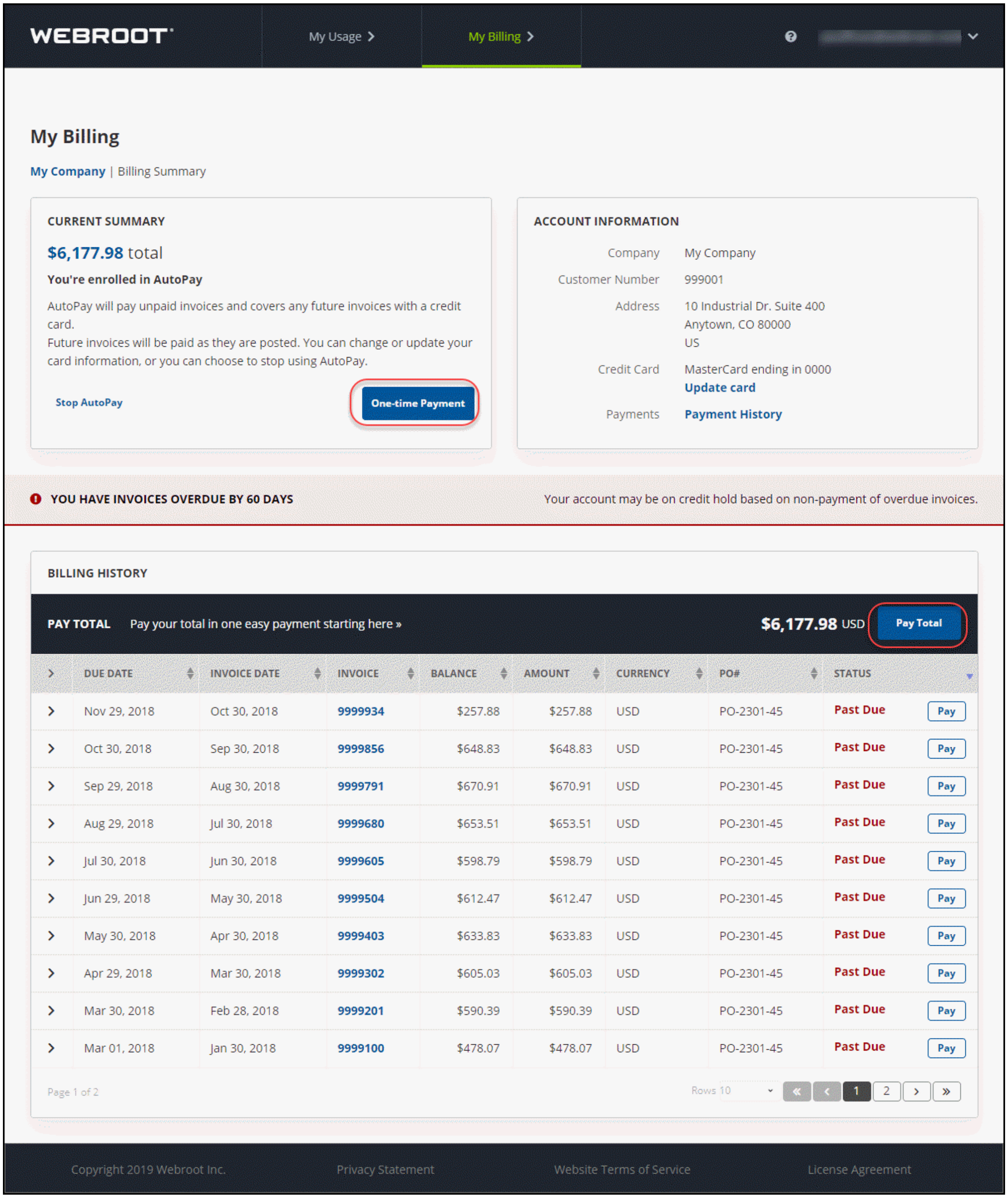
1. Log into the management console.
2. In the top navigation bar, select **Settings**, then click **Account Information** and click the **My Billing** button.



| Account Details | |
|---|---|
| Site / Company Name | Support GSM + DNSP + WSAT<br>Rename |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | |
| Parent Keycode | [redacted] (100 devices purchased - 391 days remaining)<br>Renew / Upgrade<br>⚠ This keycode should not be used for installation. Please use the correct site keycode for installation of the Webroot software. |
| View Usage | My Usage is a separate console where you can review your usage for the last 90 days. Usage includes any activity from the prior 30 days. My Usage will launch in a new browser tab so you can close it and return here.<br>My Usage |
| Pay Invoices | My Billing is a separate console where you can view invoices, payments, and pay your invoice. You will need to use an invoice to register. My Billing will launch in a new browser tab so you can close it and return here.<br>My Billing |

© 2019 Webroot Inc. Privacy Statement Website Terms of Service License Agreement

3. The My Billing portal will display billing information if an account has been added. Select either the **One-time Payment** option under Current Summary, or **Pay Total** under Billing History.



## My Billing

**My Company** | Billing Summary

**CURRENT SUMMARY**

**$6,177.98** total

**You're enrolled in AutoPay**

AutoPay will pay unpaid invoices and covers any future invoices with a credit card.
Future invoices will be paid as they are posted. You can change or update your card information, or you can choose to stop using AutoPay.

**Stop AutoPay** — **One-time Payment**

**ACCOUNT INFORMATION**

| | |
|---|---|
| Company | My Company |
| Customer Number | 999001 |
| Address | 10 Industrial Dr. Suite 400<br>Anytown, CO 80000<br>US |
| Credit Card | MasterCard ending in 0000<br>**Update card** |
| Payments | **Payment History** |

**YOU HAVE INVOICES OVERDUE BY 60 DAYS** — Your account may be on credit hold based on non-payment of overdue invoices.

**BILLING HISTORY**

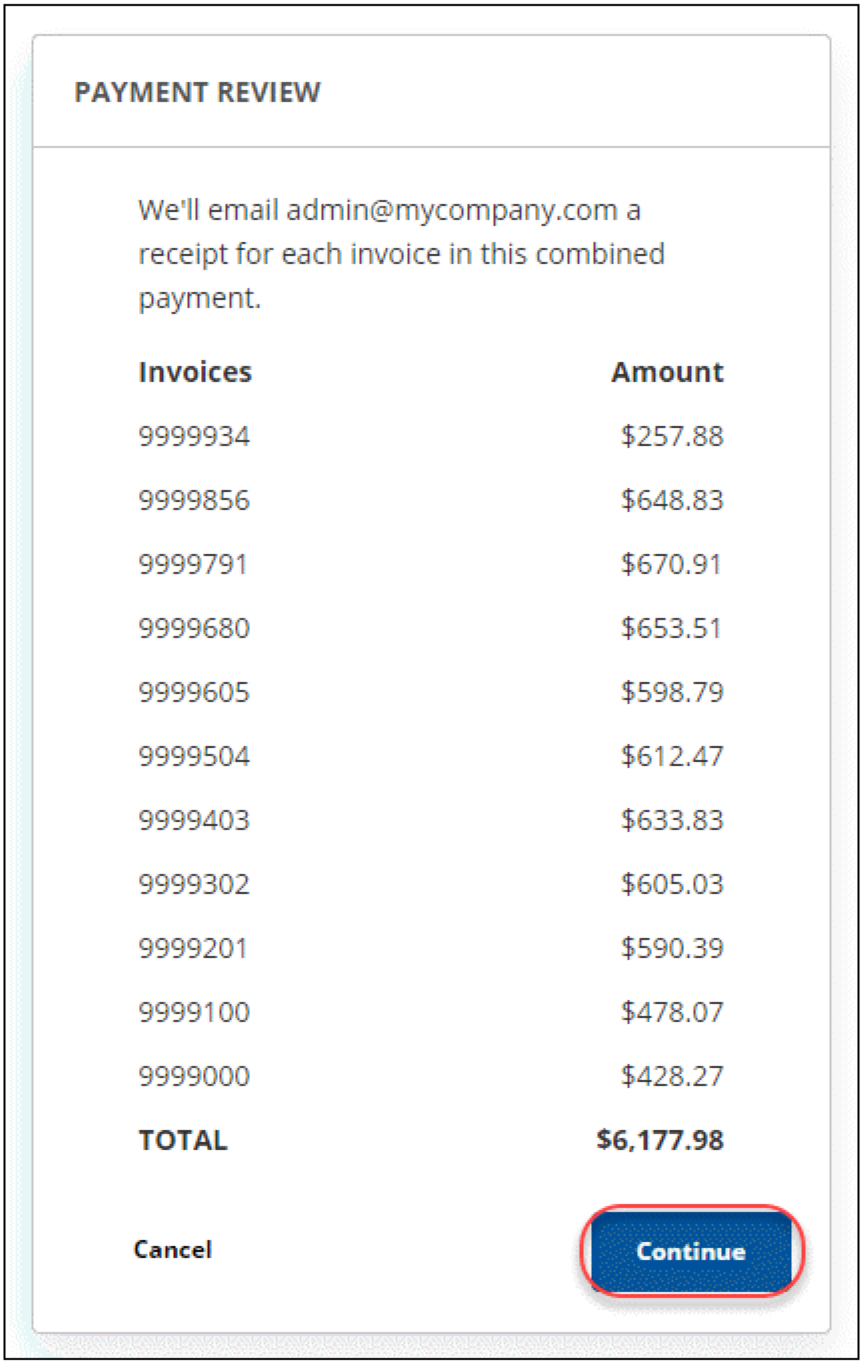
**PAY TOTAL** Pay your total in one easy payment starting here » **$6,177.98** USD **Pay Total**

| > | DUE DATE | INVOICE DATE | INVOICE | BALANCE | AMOUNT | CURRENCY | PO# | STATUS | |
|---|---|---|---|---|---|---|---|---|---|
| > | Nov 29, 2018 | Oct 30, 2018 | 9999934 | $257.88 | $257.88 | USD | PO-2301-45 | Past Due | Pay |
| > | Oct 30, 2018 | Sep 30, 2018 | 9999856 | $648.83 | $648.83 | USD | PO-2301-45 | Past Due | Pay |
| > | Sep 29, 2018 | Aug 30, 2018 | 9999791 | $670.91 | $670.91 | USD | PO-2301-45 | Past Due | Pay |
| > | Aug 29, 2018 | Jul 30, 2018 | 9999680 | $653.51 | $653.51 | USD | PO-2301-45 | Past Due | Pay |
| > | Jul 30, 2018 | Jun 30, 2018 | 9999605 | $598.79 | $598.79 | USD | PO-2301-45 | Past Due | Pay |
| > | Jun 29, 2018 | May 30, 2018 | 9999504 | $612.47 | $612.47 | USD | PO-2301-45 | Past Due | Pay |
| > | May 30, 2018 | Apr 30, 2018 | 9999403 | $633.83 | $633.83 | USD | PO-2301-45 | Past Due | Pay |
| > | Apr 29, 2018 | Mar 30, 2018 | 9999302 | $605.03 | $605.03 | USD | PO-2301-45 | Past Due | Pay |
| > | Mar 30, 2018 | Feb 28, 2018 | 9999201 | $590.39 | $590.39 | USD | PO-2301-45 | Past Due | Pay |
| > | Mar 01, 2018 | Jan 30, 2018 | 9999100 | $478.07 | $478.07 | USD | PO-2301-45 | Past Due | Pay |

Page 1 of 2 — Rows 10

Copyright 2019 Webroot Inc. Privacy Statement Website Terms of Service License Agreement

4. Review the information presented and click **Continue** to proceed.



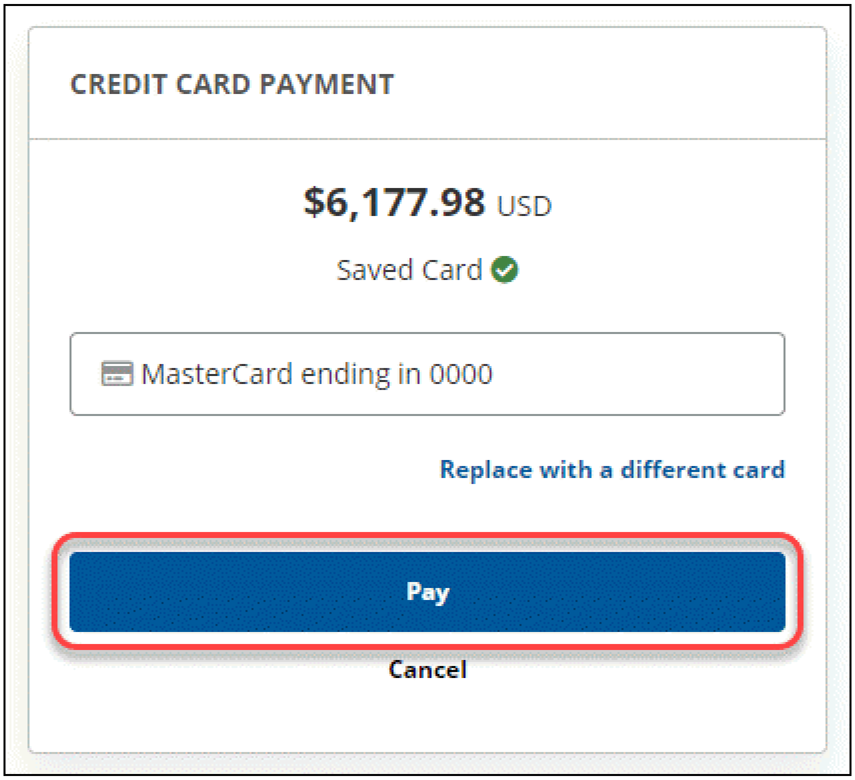
PAYMENT REVIEW

We'll email admin@mycompany.com a receipt for each invoice in this combined payment.

| Invoices | Amount |
|---|---|
| 9999934 | $257.88 |
| 9999856 | $648.83 |
| 9999791 | $670.91 |
| 9999680 | $653.51 |
| 9999605 | $598.79 |
| 9999504 | $612.47 |
| 9999403 | $633.83 |
| 9999302 | $605.03 |
| 9999201 | $590.39 |
| 9999100 | $478.07 |
| 9999000 | $428.27 |
| **TOTAL** | **$6,177.98** |

5. The Credit Card Payment screen will appear and display information about the saved credit card which includes the type of card and the last 4 digits of the card. If the credit card information is accurate, click **Pay**.

> **Note:** If the credit card information needs to be updated, click the **Replace with a different card** link and follow the prompts to update the card info.



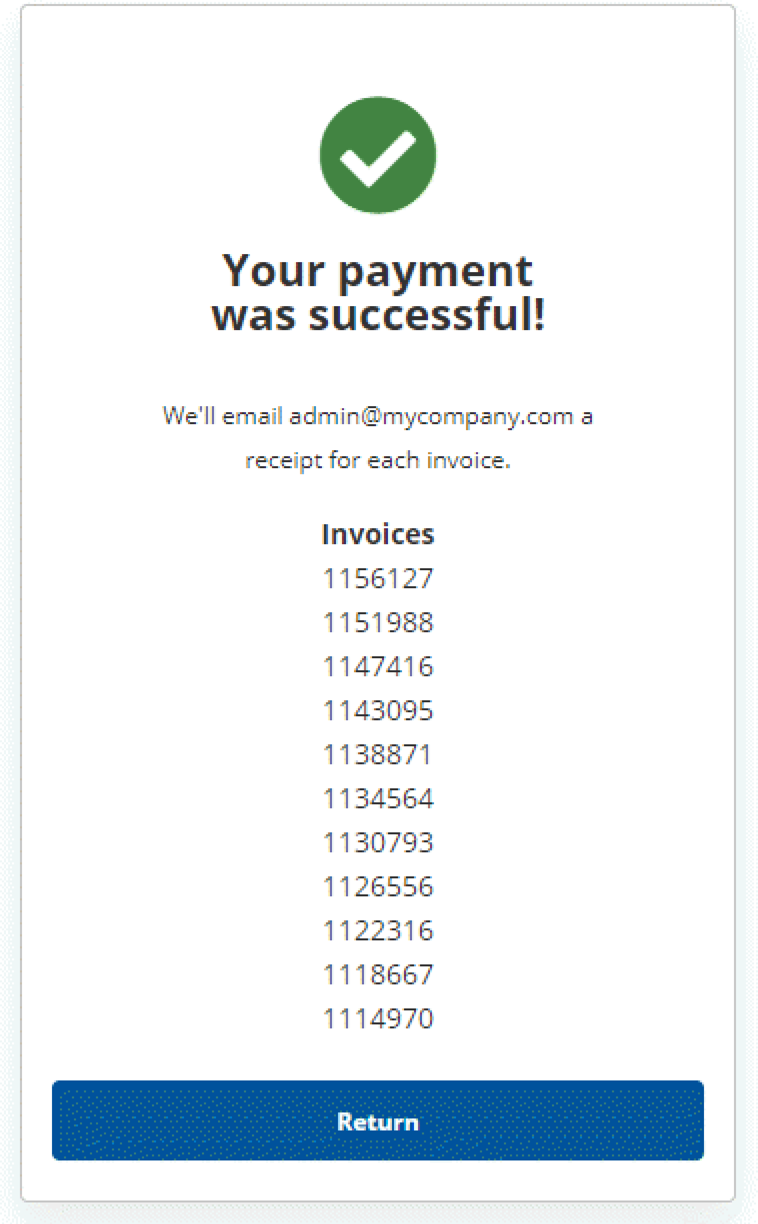
CREDIT CARD PAYMENT

$6,177.98 USD

Saved Card ✓

MasterCard ending in 0000

6. Once the payment has been processed successfully, the system will display the payment successful screen:



Your payment was successful!

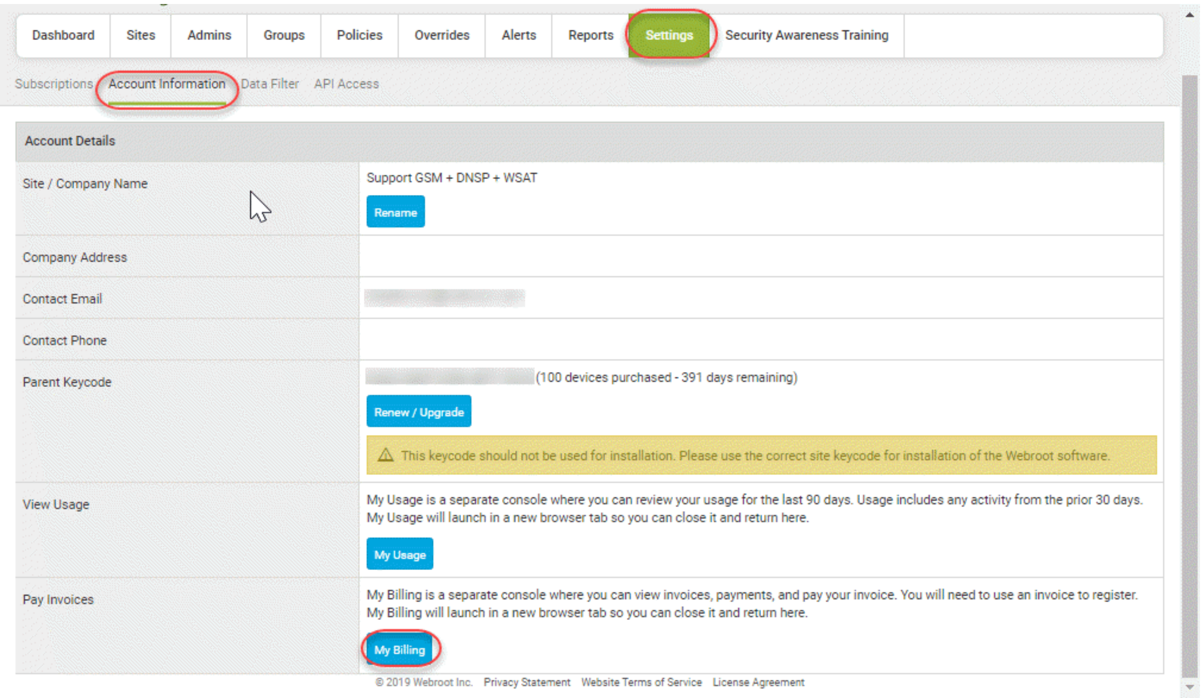
We'll email admin@mycompany.com a receipt for each invoice.

Invoices
1156127
1151988
1147416
1143095
1138871
1134564
1130793
1126556
1122316
1118667
1114970

**To pay an individual invoice**

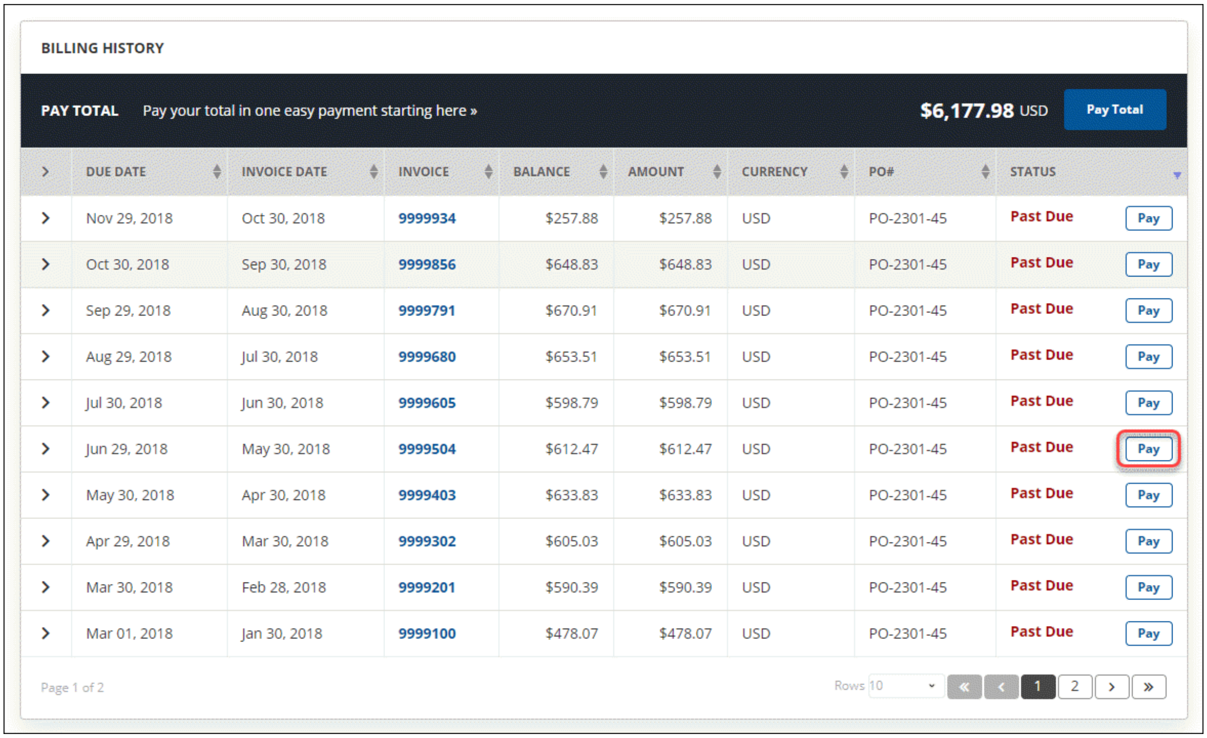
1. Log into the management console.

2. In the top navigation bar, select **Settings**, then click **Account Information** and click the **My Billing** button.



| Account Details | |
|---|---|
| Site / Company Name | Support GSM + DNSP + WSAT<br>Rename |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | |
| Parent Keycode | [redacted] (100 devices purchased - 391 days remaining)<br>Renew / Upgrade<br>⚠ This keycode should not be used for installation. Please use the correct site keycode for installation of the Webroot software. |
| View Usage | My Usage is a separate console where you can review your usage for the last 90 days. Usage includes any activity from the prior 30 days. My Usage will launch in a new browser tab so you can close it and return here.<br>My Usage |
| Pay Invoices | My Billing is a separate console where you can view invoices, payments, and pay your invoice. You will need to use an invoice to register. My Billing will launch in a new browser tab so you can close it and return here.<br>My Billing |

3. Click **Pay** In the bottom section of the My Billing portal next to an individual invoice.



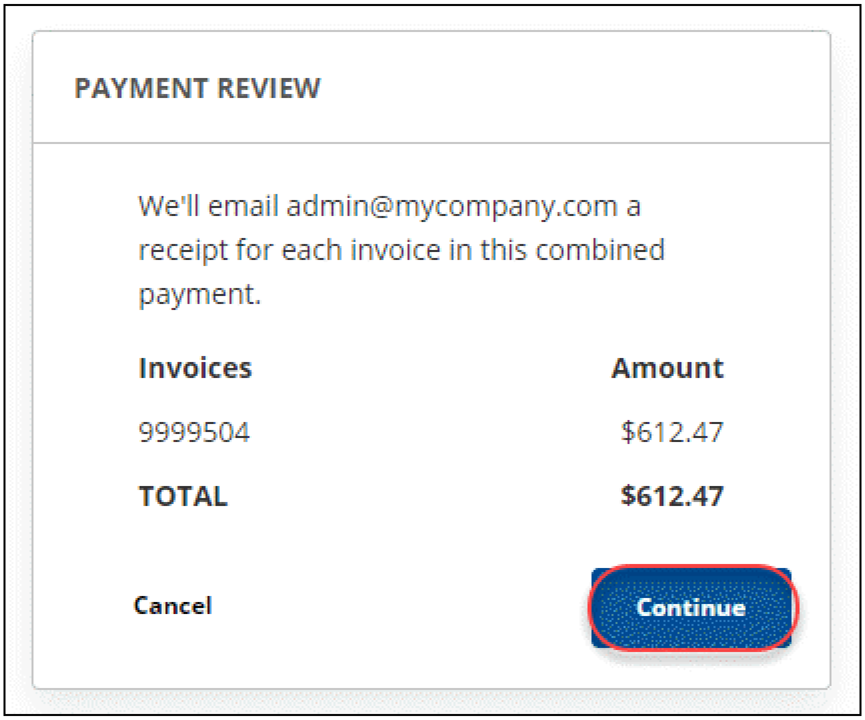
BILLING HISTORY

**PAY TOTAL** Pay your total in one easy payment starting here » **$6,177.98** USD

| > | DUE DATE | INVOICE DATE | INVOICE | BALANCE | AMOUNT | CURRENCY | PO# | STATUS | |
|---|---|---|---|---|---|---|---|---|---|
| > | Nov 29, 2018 | Oct 30, 2018 | 9999934 | $257.88 | $257.88 | USD | PO-2301-45 | Past Due | Pay |
| > | Oct 30, 2018 | Sep 30, 2018 | 9999856 | $648.83 | $648.83 | USD | PO-2301-45 | Past Due | Pay |
| > | Sep 29, 2018 | Aug 30, 2018 | 9999791 | $670.91 | $670.91 | USD | PO-2301-45 | Past Due | Pay |
| > | Aug 29, 2018 | Jul 30, 2018 | 9999680 | $653.51 | $653.51 | USD | PO-2301-45 | Past Due | Pay |
| > | Jul 30, 2018 | Jun 30, 2018 | 9999605 | $598.79 | $598.79 | USD | PO-2301-45 | Past Due | Pay |
| > | Jun 29, 2018 | May 30, 2018 | 9999504 | $612.47 | $612.47 | USD | PO-2301-45 | Past Due | Pay |
| > | May 30, 2018 | Apr 30, 2018 | 9999403 | $633.83 | $633.83 | USD | PO-2301-45 | Past Due | Pay |
| > | Apr 29, 2018 | Mar 30, 2018 | 9999302 | $605.03 | $605.03 | USD | PO-2301-45 | Past Due | Pay |
| > | Mar 30, 2018 | Feb 28, 2018 | 9999201 | $590.39 | $590.39 | USD | PO-2301-45 | Past Due | Pay |
| > | Mar 01, 2018 | Jan 30, 2018 | 9999100 | $478.07 | $478.07 | USD | PO-2301-45 | Past Due | Pay |

Page 1 of 2

4. Click **Continue** on the Payment Review screen.



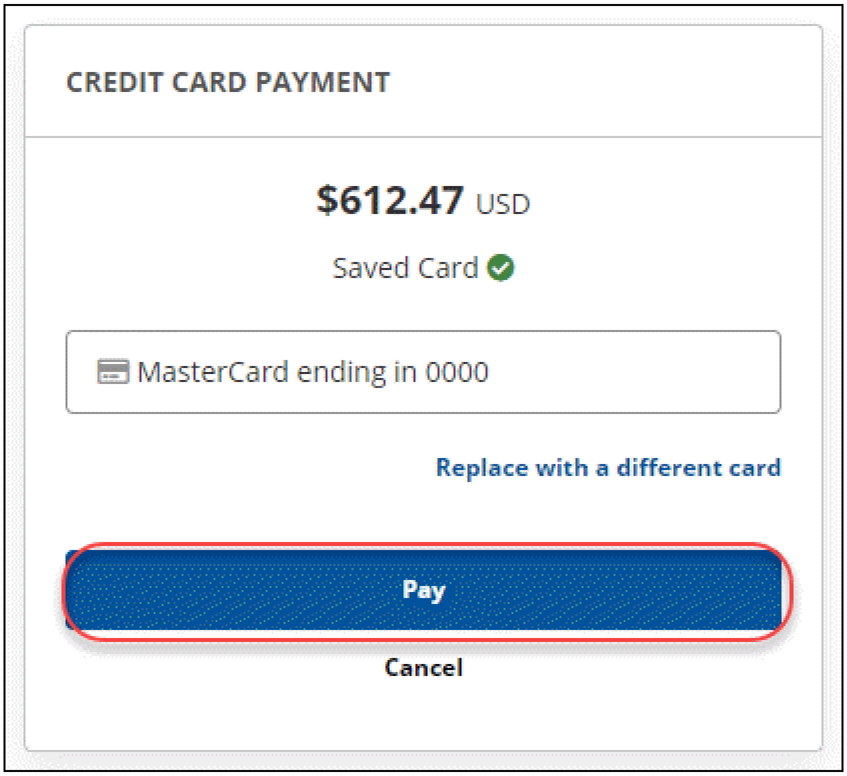
PAYMENT REVIEW

We'll email admin@mycompany.com a receipt for each invoice in this combined payment.

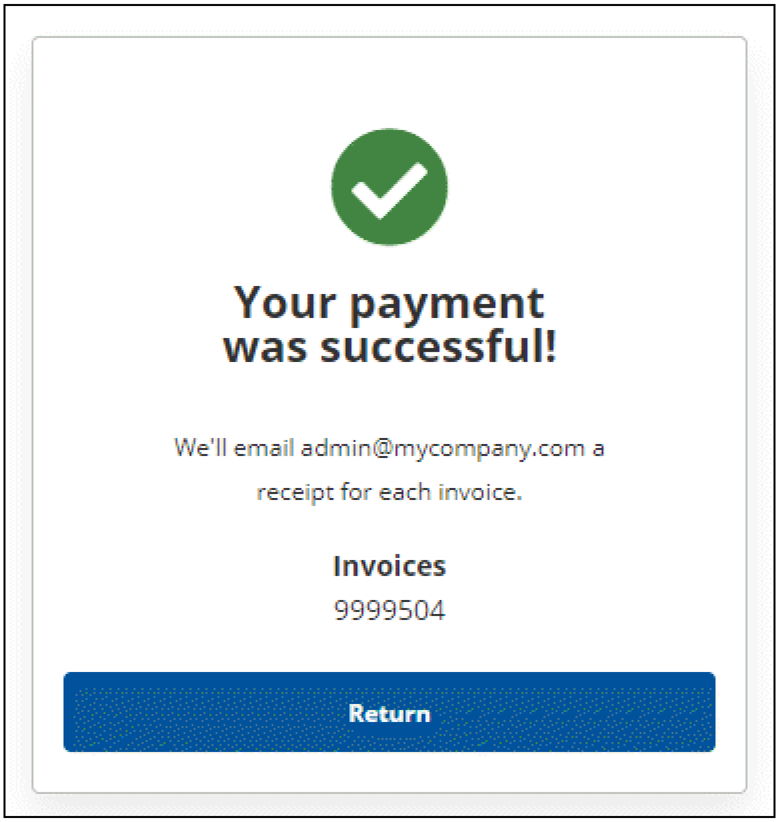
| Invoices | Amount |
|---|---|
| 9999504 | $612.47 |
| **TOTAL** | **$612.47** |

5. The Credit Card Payment screen will appear and display information about the saved credit card which includes the type of card and the last 4 digits of the card. If the credit card information is accurate, click **Pay**.

> **Note: I**f the credit card information needs to be updated, click the **Replace with a different card** link and follow the prompts to update the card info.



6. Once the payment has been processed successfully, the system will display the payment successful screen:



Your payment was successful!

We'll email admin@mycompany.com a receipt for each invoice.

Invoices

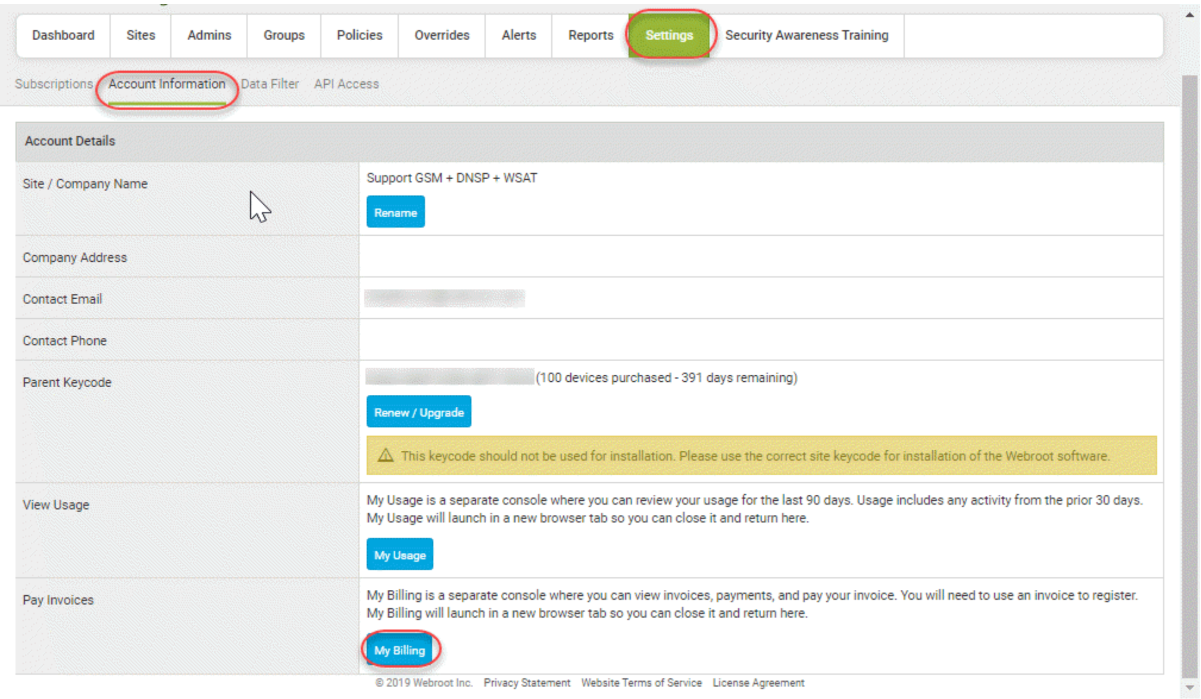
9999504

# Setting Up Auto Pay

You can use the My Billing portal to setup AutoPay, which will use the saved credit card to pay your bill automatically.

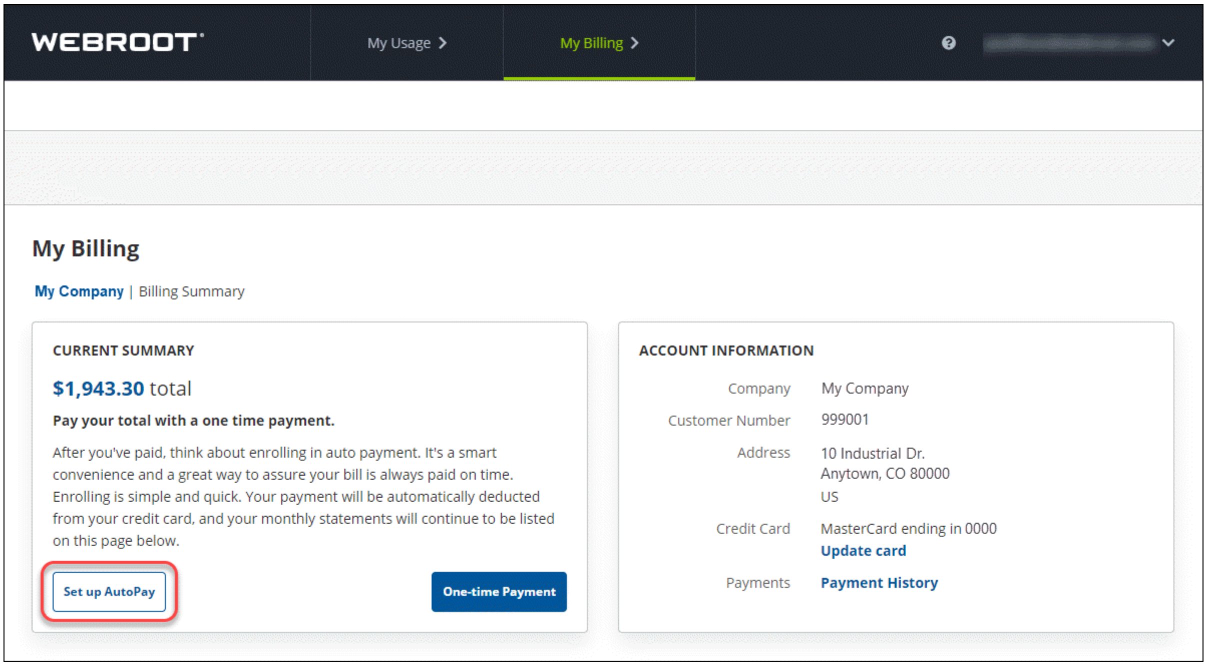
**To set up AutoPay:**

1. Log into the management console.
2. In the top navigation bar, select **Settings**, then click **Account Information** and click the **My Billing** button.



| Account Details | |
|---|---|
| Site / Company Name | Support GSM + DNSP + WSAT |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | |
| Parent Keycode | [redacted] (100 devices purchased - 391 days remaining)<br>⚠ This keycode should not be used for installation. Please use the correct site keycode for installation of the Webroot software. |
| View Usage | My Usage is a separate console where you can review your usage for the last 90 days. Usage includes any activity from the prior 30 days. My Usage will launch in a new browser tab so you can close it and return here. |
| Pay Invoices | My Billing is a separate console where you can view invoices, payments, and pay your invoice. You will need to use an invoice to register. My Billing will launch in a new browser tab so you can close it and return here. |

3. Click **Set up AutoPay** under Current Summary to display more information about how AutoPay works. If you wish you enroll your account in AutoPay, click **Begin**.



My Billing

My Company | Billing Summary

CURRENT SUMMARY

$1,943.30 total

Pay your total with a one time payment.

After you've paid, think about enrolling in auto payment. It's a smart convenience and a great way to assure your bill is always paid on time. Enrolling is simple and quick. Your payment will be automatically deducted from your credit card, and your monthly statements will continue to be listed on this page below.

ACCOUNT INFORMATION

| | |
|---|---|
| Company | My Company |
| Customer Number | 999001 |
| Address | 10 Industrial Dr.<br>Anytown, CO 80000<br>US |
| Credit Card | MasterCard ending in 0000<br>Update card |
| Payments | Payment History |

4. Terms and conditions are presented, including contact information for additional questions or inquiries, and Click **Agree** to continue.
5. The Credit Card Selection screen appears and displays the type and last 4 digits of the saved credit card. Here, you can:

- Use the saved credit card.
- Add a credit card if one is not saved.
- Update the saved credit card information and add a new credit card.

6. Once the credit card information is correct, click **Complete AutoPay**.
7. You will get a confirmation message that your company has been enrolled in AutoPay.

**Note:** If you have used the My Billing portal to setup AutoPay, you will need to contact Webroot either by phone, email, or by contacting your personal sales representative, and request that we remove your company from AutoPay.

Here are the contact methods available:

- Email AccountsReceivable@webroot.com
- Call us in the United States at +1 (720) 842-3296.

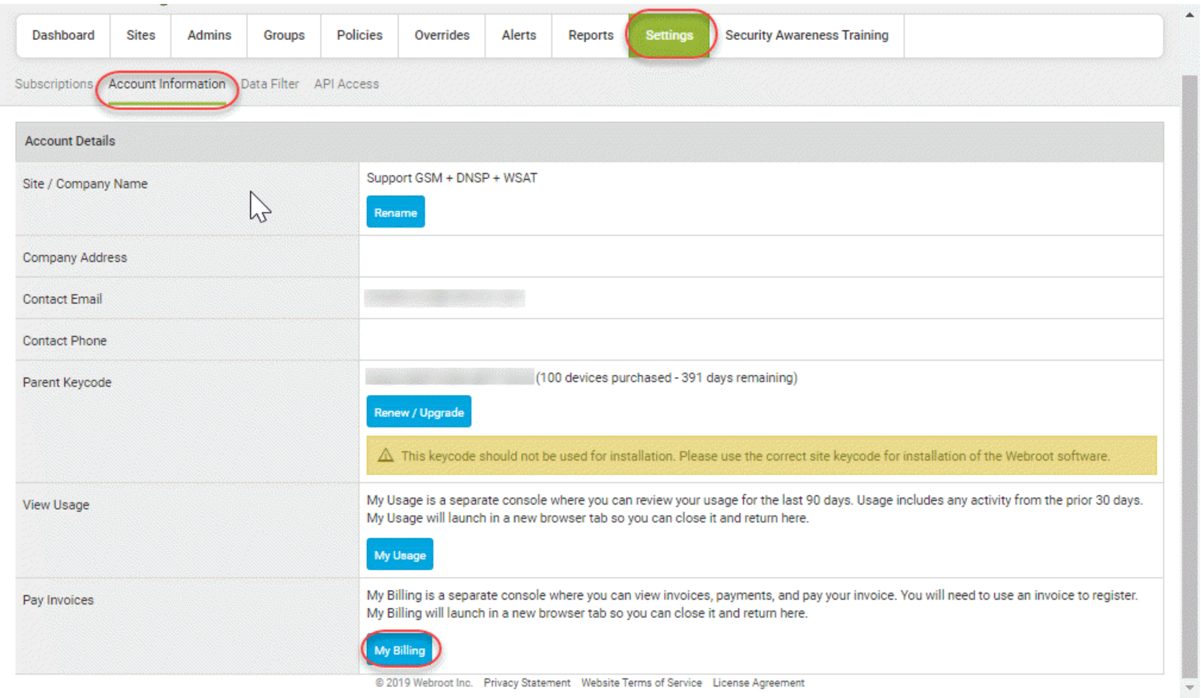
- Contact your Sales Rep for assistance.

# Updating Saved Credit Card Information in the My Billing Portal

You can use the My Billing portal to update the saved credit card information in the Management console.

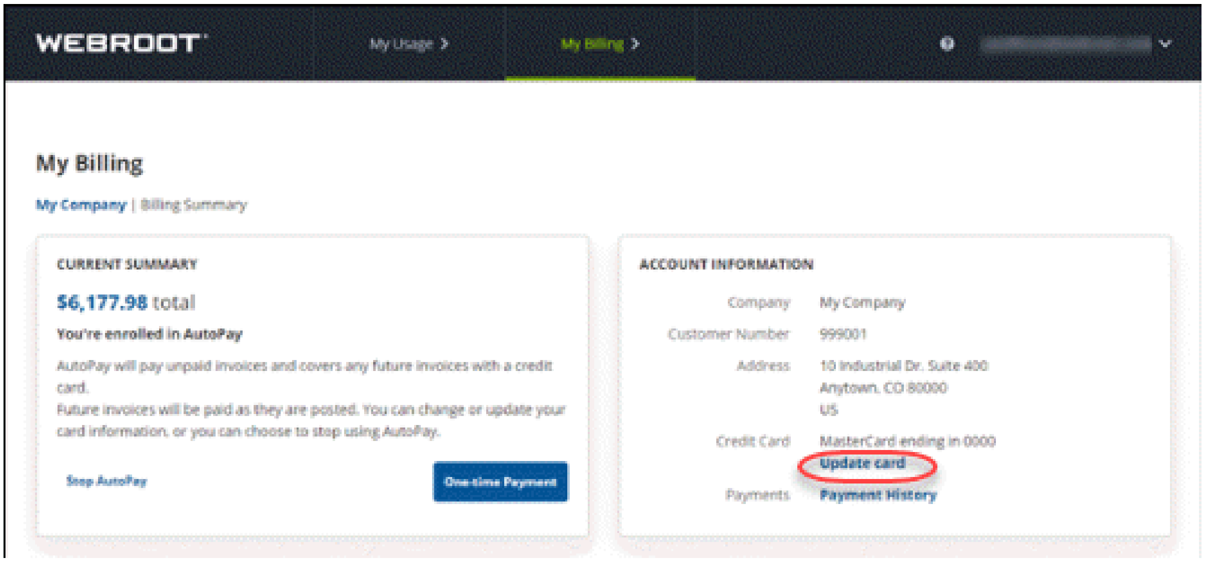
**To update the saved credit card information:**

1. Log into the management console.
2. In the top navigation bar, select **Settings**, then click **Account Information** and click the **My Billing** button.



| Account Details | |
|---|---|
| Site / Company Name | Support GSM + DNSP + WSAT<br>Rename |
| Company Address | |
| Contact Email | [redacted] |
| Contact Phone | |
| Parent Keycode | [redacted] (100 devices purchased - 391 days remaining)<br>Renew / Upgrade<br>⚠ This keycode should not be used for installation. Please use the correct site keycode for installation of the Webroot software. |
| View Usage | My Usage is a separate console where you can review your usage for the last 90 days. Usage includes any activity from the prior 30 days. My Usage will launch in a new browser tab so you can close it and return here.<br>My Usage |
| Pay Invoices | My Billing is a separate console where you can view invoices, payments, and pay your invoice. You will need to use an invoice to register. My Billing will launch in a new browser tab so you can close it and return here.<br>My Billing |

3. The My Billing portal will display billing information, assuming an account has been added. Under Account Information, click **Update card**.



My Billing

My Company | Billing Summary

CURRENT SUMMARY

$6,177.98 total

You're enrolled in AutoPay

AutoPay will pay unpaid invoices and covers any future invoices with a credit card.
Future invoices will be paid as they are posted. You can change or update your card information, or you can choose to stop using AutoPay.

ACCOUNT INFORMATION

| | |
|---|---|
| Company | My Company |
| Customer Number | 999001 |
| Address | 10 Industrial Dr. Suite 400<br>Anytown, CO 80000<br>US |
| Credit Card | MasterCard ending in 0000<br>Update card |
| Payments | Payment History |

**Note:** You can also change the card on file by clicking the **Replace with a different card link** during the payment process or while setting up AutoPay.

4. The My Billing screen will display and you will need to provide the new credit card info and click **Save & Next**.
5. The **My Billing** screen will appear and you need to provide the credit card Billing Address information and then click **Register**.
6. Once completed, you will get a message saying that your credit card was successfully updated.

# Chapter 12: About DNS Protection

To learn more about DNS Protection, see the following topic:

# DNS Protection Overview

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.

- To activate a subscription for DNS Protection, log in to a console and click the **Settings** tab.
- To review online guides for DNS Protection, click here.

# Starting DNS Protection Trials

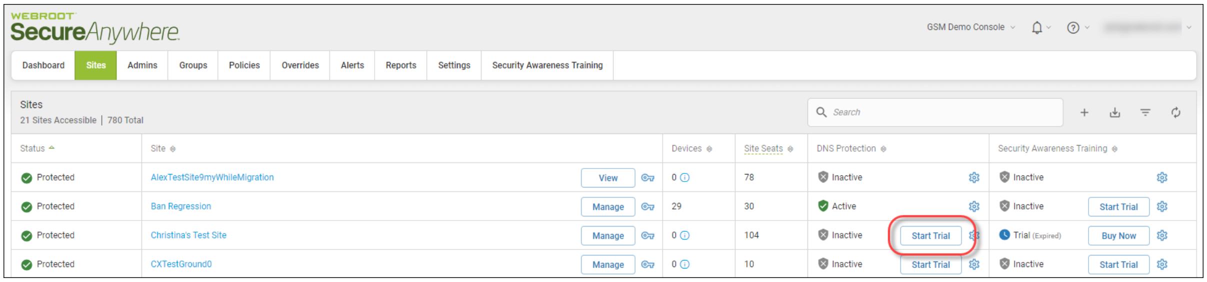
To trial DNS Protection for a site with a few selected devices, there is now a Guided Setup available to help you set up the DNS agent quickly and easily. This topic describes the process flow of the setup.

- Step 1 — Activate the DNS Protection Trial.
- Step 2 — Follow along with the Setup Wizard to configure DNS Protection for your sites.

**Note:** To start a DNS Protection trial, you must have at least one Endpoint configured with the Webroot SecureAnywhere software deployed. If you don't have an endpoint configured yet, the guided setup will detect this and give you the following options.

## Step 1 — Activate a Trial

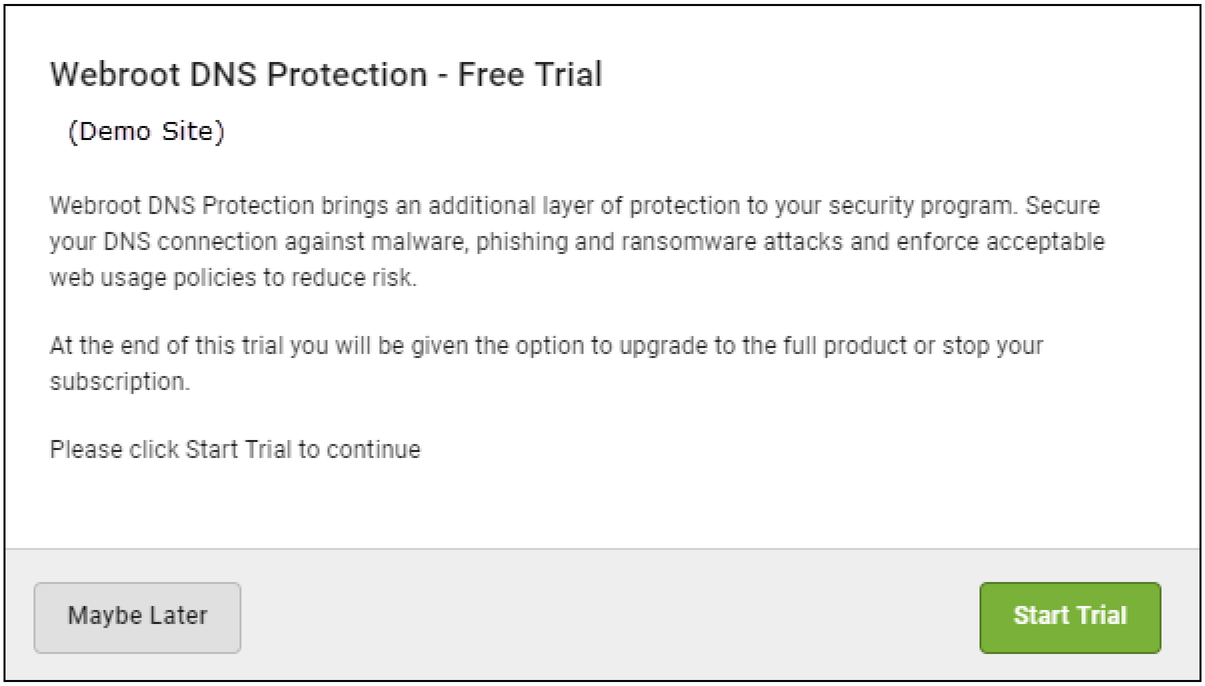
To access the Guided Setup, from the Sites page, click the **Start Trial** button for the site that you want to trial DNS Protection on.



Sites
21 Sites Accessible | 780 Total

| Status | Site | | Devices | Site Seats | DNS Protection | | Security Awareness Training | |
|---|---|---|---|---|---|---|---|---|
| ✓ Protected | AlexTestSite9myWhileMigration | View | 0 ⓘ | 78 | Inactive | | Inactive | |
| ✓ Protected | Ban Regression | Manage | 29 | 30 | ✓ Active | | Inactive | Start Trial |
| ✓ Protected | Christina's Test Site | Manage | 0 ⓘ | 104 | Inactive | Start Trial | Trial (Expired) | Buy Now |
| ✓ Protected | CXTestGround0 | Manage | 0 ⓘ | 10 | Inactive | Start Trial | Inactive | Start Trial |

The DNS Protection - Free Trial window displays.



Webroot DNS Protection - Free Trial

(Demo Site)

Webroot DNS Protection brings an additional layer of protection to your security program. Secure your DNS connection against malware, phishing and ransomware attacks and enforce acceptable web usage policies to reduce risk.

At the end of this trial you will be given the option to upgrade to the full product or stop your subscription.

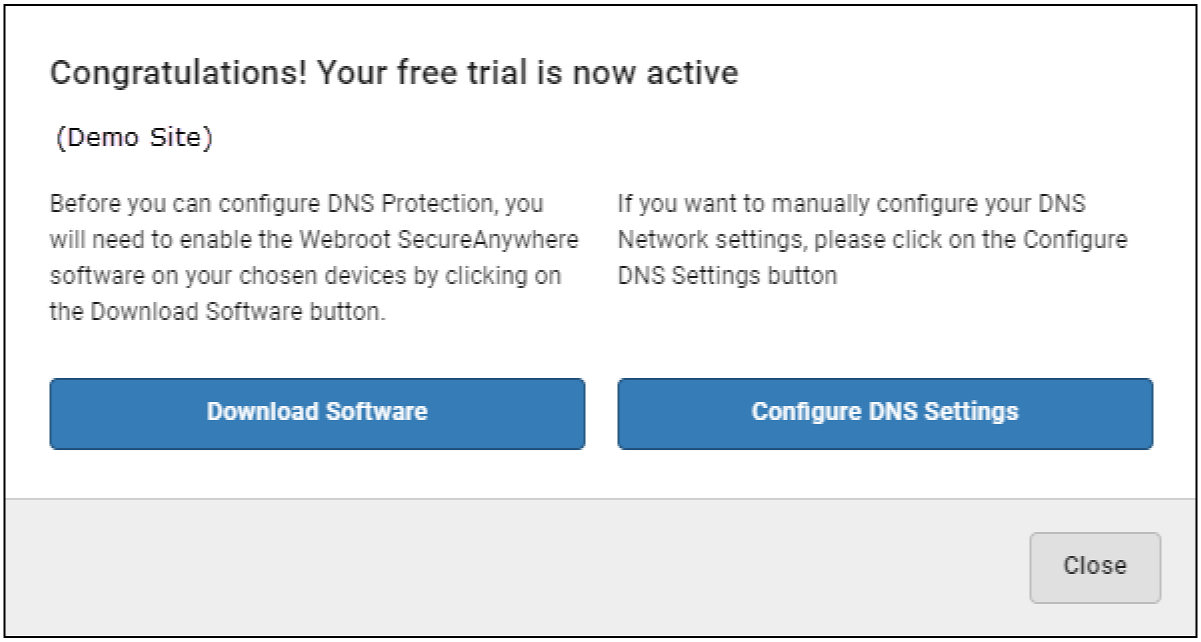
Please click Start Trial to continue

Do either of the following:

- Click the **Start Trial** button to begin the trial.
- Click the **Maybe Later** button to begin the trial at a later time.

## Step 2 — Trial Confirmation and Begin Guided Setup

If you click the **Start Trial** button, the confirmation window displays, indicating that your trial for the site is now active.



Congratulations! Your free trial is now active

(Demo Site)

Before you can configure DNS Protection, you will need to enable the Webroot SecureAnywhere software on your chosen devices by clicking on the Download Software button.

If you want to manually configure your DNS Network settings, please click on the Configure DNS Settings button

Do either of the following:

- If you don't already have DNS Protection installed, click the **Download Software** button to display the Downloads page, where you can download a copy of the software. Then continue with configuring your settings.
- Click the **Configure DNS Settings** button to follow along with the guided setup. We recommend you follow along withe the guided setup.

Continue with *About the DNS Protection Guided Setup on page 563*.

# About the DNS Protection Guided Setup

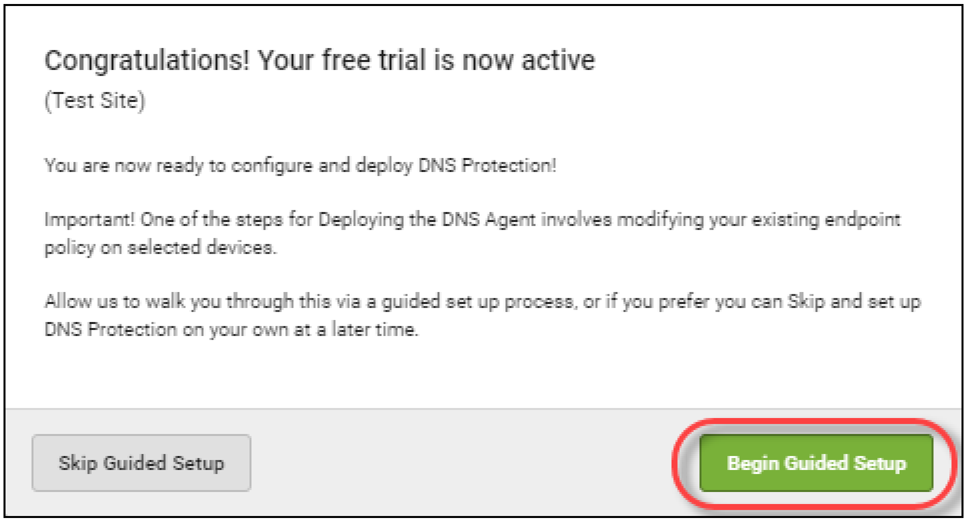
Use the DNS Protection Guided Setup to easily configure DNS Protection using three steps:

- Step 1 — Select DNS Group Policy
- Step 2 — Select Endpoints
- Step 3 — Review and Confirm

**Note:** The Guided Setup is always available for you to use at any time from **Sites** > **DNS Protection Settings**.

## Step 1 — Select DNS Group Policy

Click the **Begin Guided Setup** button.



Congratulations! Your free trial is now active

(Test Site)

You are now ready to configure and deploy DNS Protection!

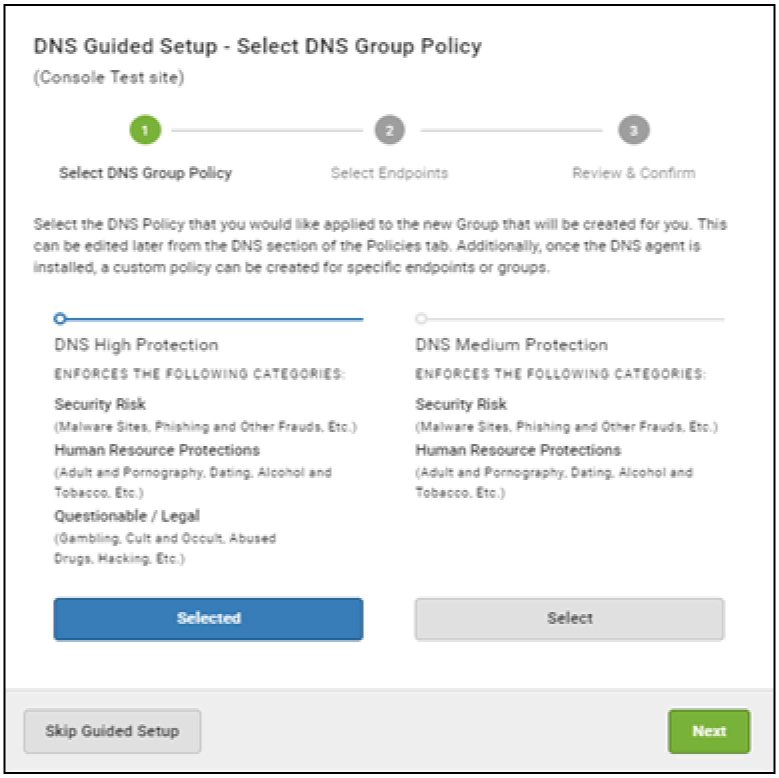
Important! One of the steps for Deploying the DNS Agent involves modifying your existing endpoint policy on selected devices.

Allow us to walk you through this via a guided set up process, or if you prefer you can Skip and set up DNS Protection on your own at a later time.

You will be taken to the first of three steps to configure DNS Protection on your endpoints.

The first step is to choose a Policy for a new group that will be created for you. There are two policies to choose from

- DNS High Protection
- DNS Medium Protection.



DNS Guided Setup - Select DNS Group Policy

(Console Test site)

Select the DNS Policy that you would like applied to the new Group that will be created for you. This can be edited later from the DNS section of the Policies tab. Additionally, once the DNS agent is installed, a custom policy can be created for specific endpoints or groups.

DNS High Protection

ENFORCES THE FOLLOWING CATEGORIES:

Security Risk
(Malware Sites, Phishing and Other Frauds, Etc.)

Human Resource Protections
(Adult and Pornography, Dating, Alcohol and Tobacco, Etc.)

Questionable / Legal
(Gambling, Cult and Occult, Abused Drugs, Hacking, Etc.)

DNS Medium Protection

ENFORCES THE FOLLOWING CATEGORIES:

Security Risk
(Malware Sites, Phishing and Other Frauds, Etc.)

Human Resource Protections
(Adult and Pornography, Dating, Alcohol and Tobacco, Etc.)

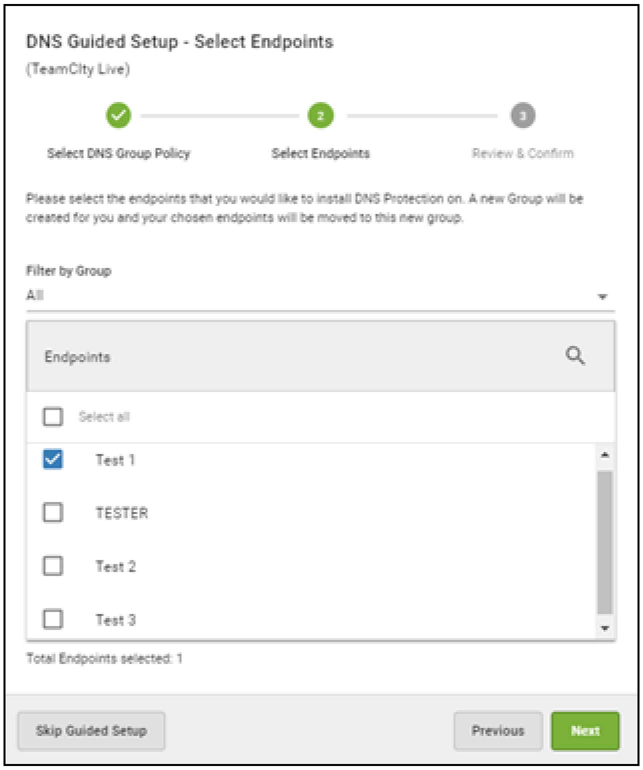
**Note:** You can create your own Policy at a later time from the Policies tab in the console if you wanted to have a custom policy to meet your business requirements.

Once you have selected your policy, click the **Next** button.

## Step 2 — Select Endpoints

The next step is to choose the Endpoints that you would like to install the DNS Agent on.

The Guided Setup will display a drop down list with all of your groups. Select which Endpoints from those groups you want to move to the new DNS Enabled group, which will be created for you automatically.



DNS Guided Setup - Select Endpoints

(TeamCity Live)

Please select the endpoints that you would like to install DNS Protection on. A new Group will be created for you and your chosen endpoints will be moved to this new group.

Filter by Group

All

Endpoints

□ Select all

☑ Test 1

□ TESTER

□ Test 2

□ Test 3

Total Endpoints selected: 1

Once you have selected your endpoints, click the **Next** button.

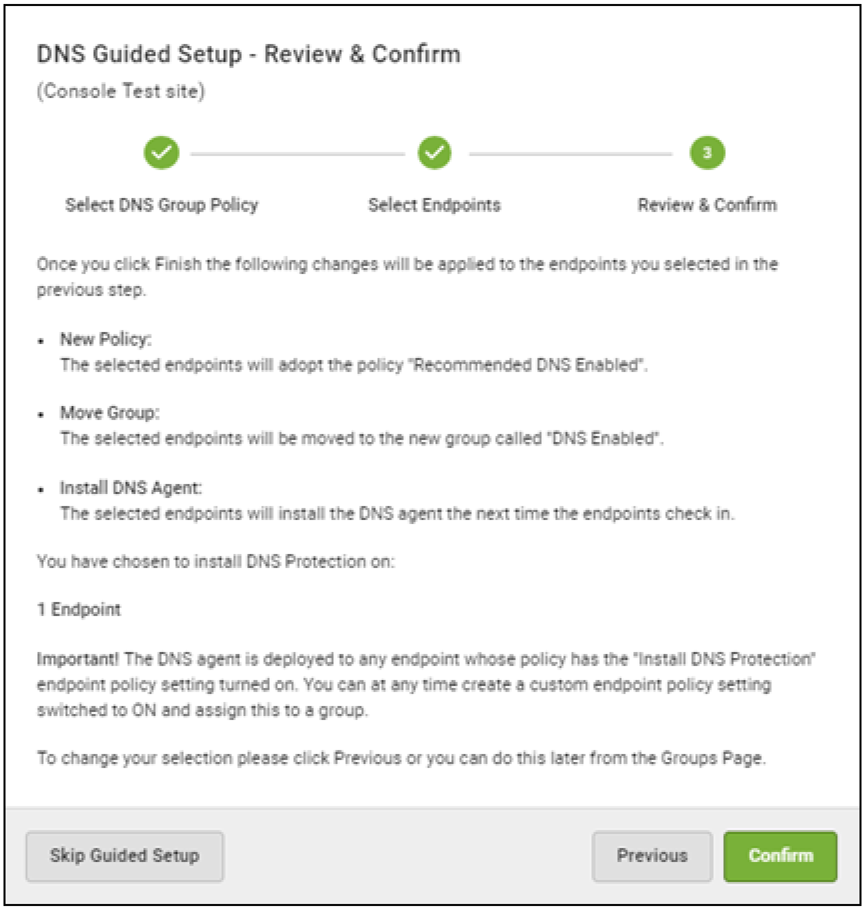
## Step 3 — Review and Confirm

The final step is to review the changes you made.

- To make any changes, click the **Previous** button.
- To confirm your changes, click the **Confirm** button.

If you clicked the Confirm button, the following occurs:

- A new Group called DNS Enabled will be created for you with your selected DNS policy, either DNS High or Medium Protection.
- The group will have the Endpoint Policy Recommended DNS Enabled policy activated. This will automatically install the DNS Agent onto your selected Endpoints the next time they check in.



DNS Guided Setup - Review & Confirm

(Console Test site)

Once you click Finish the following changes will be applied to the endpoints you selected in the previous step.

- New Policy:
  The selected endpoints will adopt the policy "Recommended DNS Enabled".
- Move Group:
  The selected endpoints will be moved to the new group called "DNS Enabled".
- Install DNS Agent:
  The selected endpoints will install the DNS agent the next time the endpoints check in.

You have chosen to install DNS Protection on:

1 Endpoint

Important! The DNS agent is deployed to any endpoint whose policy has the "Install DNS Protection" endpoint policy setting turned on. You can at any time create a custom endpoint policy setting switched to ON and assign this to a group.

To change your selection please click Previous or you can do this later from the Groups Page.

You will then be taken to the Groups page, where the new group you created is displayed.

# Chapter 13: About Security Awareness Training

To learn more about Security Awareness Training, see the following topic:

# Security Awareness Training Overview

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

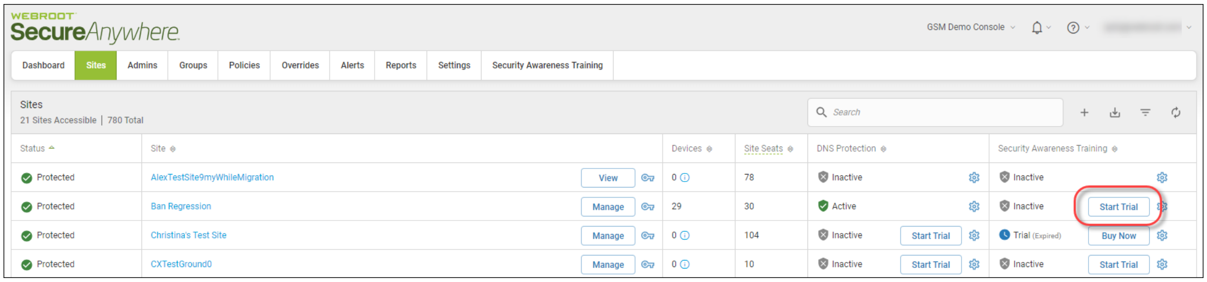
- To activate a subscription for Security Awareness Training, log into a management console and click the **Settings** tab.
- To review online guides for Security Awareness Training, click here.

# Starting Security Awareness Training Trials

If you wanted to trial Security Awareness Training for any of your sites, there is now a Guided Setup available to help you set up Security Awareness Training quickly and easily. This topic describes the process flow of the setup.

## Activate a Trial

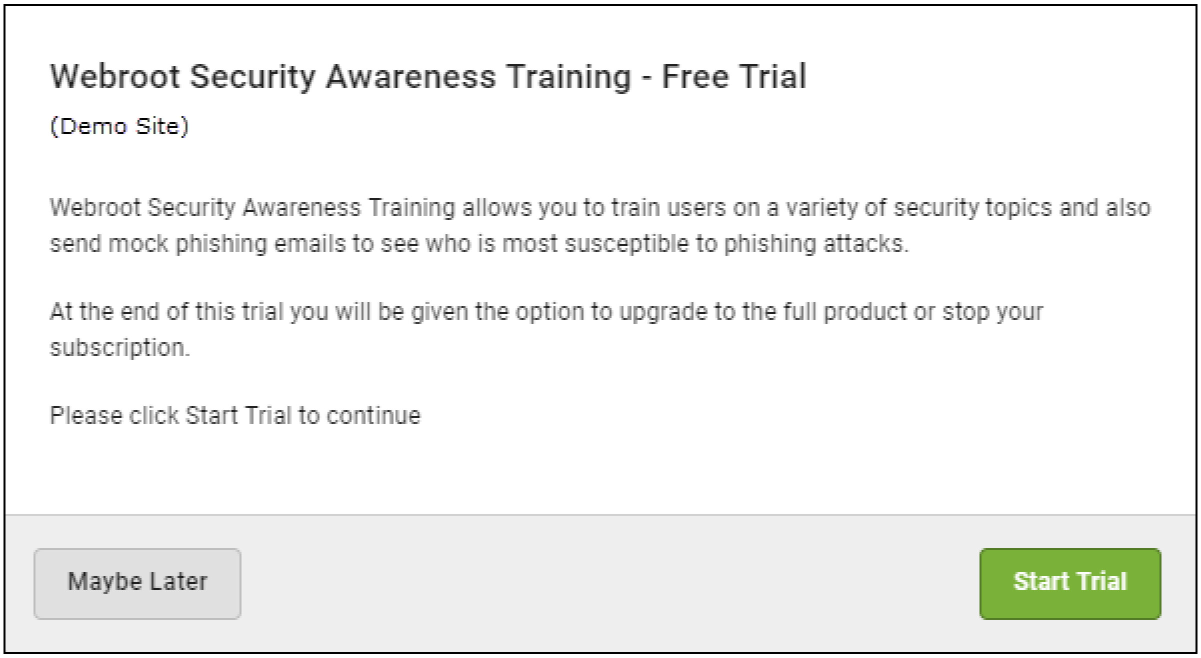
To access the Guided Setup, from the Sites page, click the **Start Trial** button for the site that you want to trial Security Awareness Training on.



Sites
21 Sites Accessible | 780 Total

| Status | Site | | Devices | Site Seats | DNS Protection | | Security Awareness Training | |
|---|---|---|---|---|---|---|---|---|
| Protected | AlexTestSite9myWhileMigration | View | 0 | 78 | Inactive | | Inactive | |
| Protected | Ban Regression | Manage | 29 | 30 | Active | | Inactive | Start Trial |
| Protected | Christina's Test Site | Manage | 0 | 104 | Inactive | Start Trial | Trial (Expired) | Buy Now |
| Protected | CXTestGround0 | Manage | 0 | 10 | Inactive | Start Trial | Inactive | Start Trial |

The Security Awareness Training - Free Trial window displays.



Webroot Security Awareness Training - Free Trial

(Demo Site)

Webroot Security Awareness Training allows you to train users on a variety of security topics and also send mock phishing emails to see who is most susceptible to phishing attacks.

At the end of this trial you will be given the option to upgrade to the full product or stop your subscription.

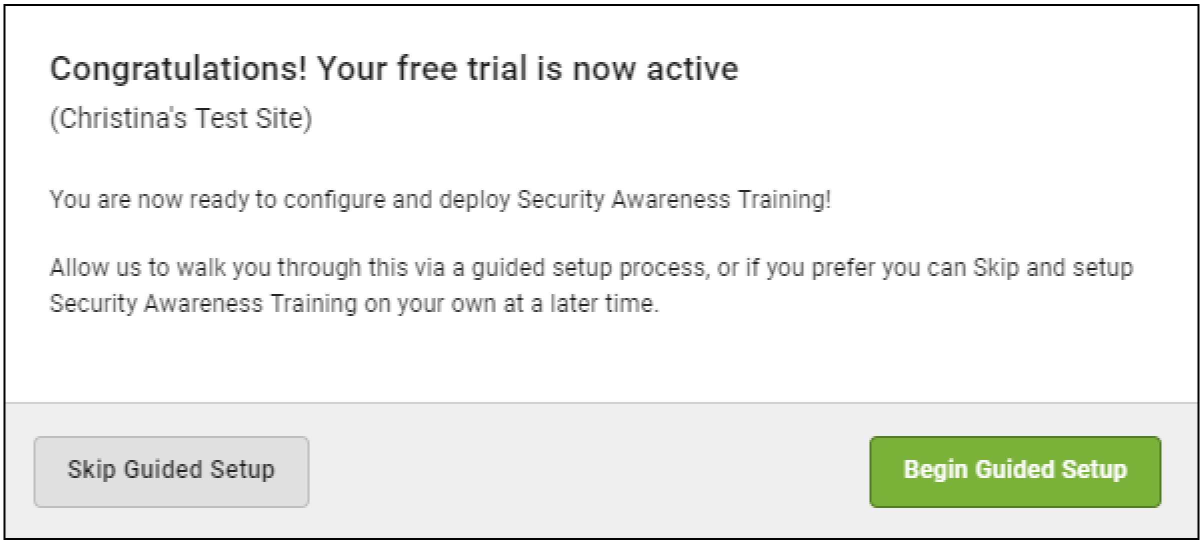
Please click Start Trial to continue

Do either of the following:

- Click the **Start Trial** button to begin the trial.
- Click the **Maybe Later** button to begin the trial at a later time.

## Trial Confirmation and Begin Guided Setup

If you click the **Start Trial** button, the confirmation window displays, indicating that your trial for the site is now active.



Congratulations! Your free trial is now active

(Christina's Test Site)

You are now ready to configure and deploy Security Awareness Training!

Allow us to walk you through this via a guided setup process, or if you prefer you can Skip and setup Security Awareness Training on your own at a later time.

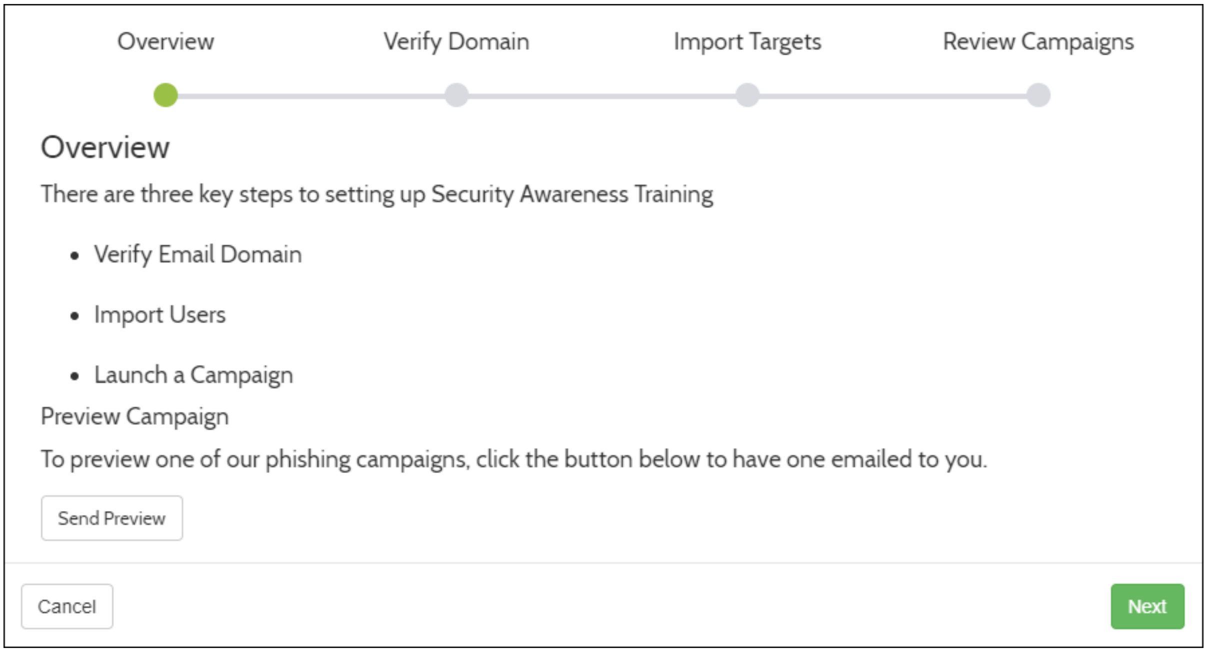
Do either of the following:

- Click the **Skip Guided Setup** button to manually configure your settings.
- Click the **Begin Guided Setup** button to follow along with the guided setup. We recommend you follow along withe the guided setup.

## Guided Setup - Overview

If you click the **Begin Guided Setup** button, you will be taken to the overview screen which describes the three-step process to set up Security Awareness Training. These are the steps:

- Verify Email Domain
- Import Targets
- Review Campaigns



Overview

There are three key steps to setting up Security Awareness Training

- Verify Email Domain
- Import Users
- Launch a Campaign

Preview Campaign

To preview one of our phishing campaigns, click the button below to have one emailed to you.

From this screen you can also click the **Send Preview** button to preview an example phishing campaign and have one emailed to you.

Once you are ready to continue, click the **Next** button and continue with *About the Security Awareness Training Guided Setup on page 572*.

# About the Security Awareness Training Guided Setup

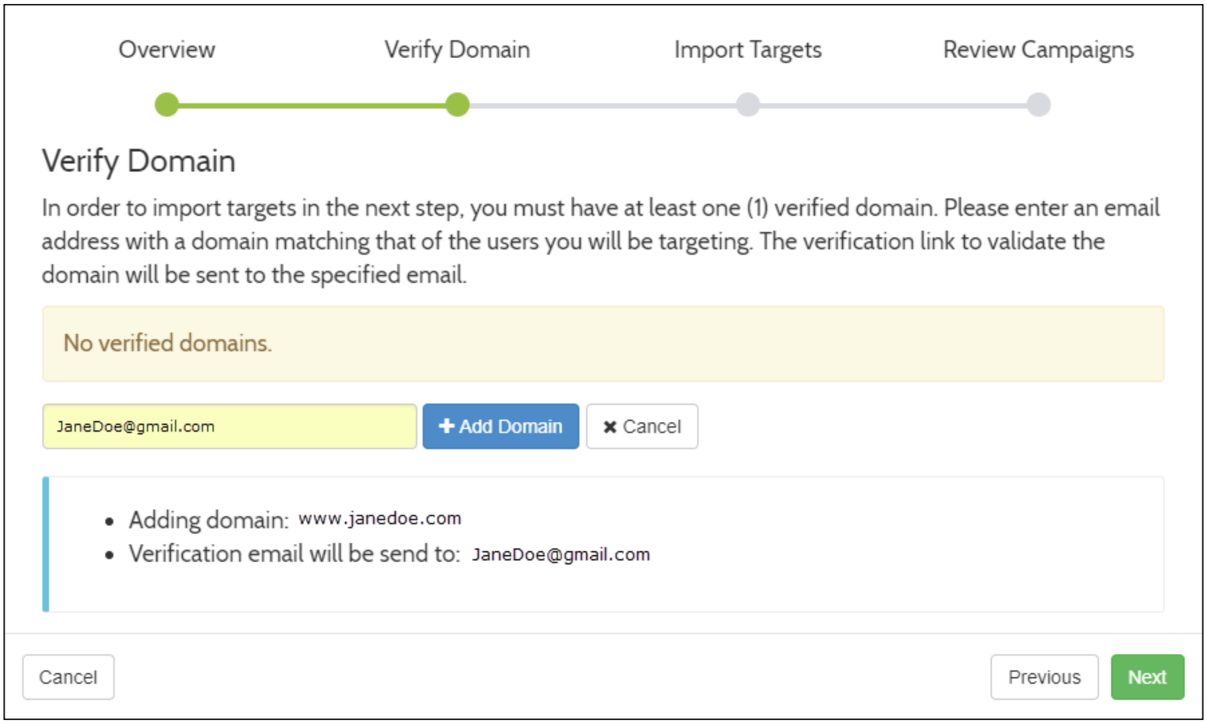
This topic describes the three steps in the Security Awareness Training guided setup:

- Step 1 — Verify Domains
- Step 2 — Import Targets
- Step 3 — Review Campaigns

## Step 1 — Verify Domain

The first step is to verify an email domain that you would like to start sending Security Awareness campaigns to.

In the Email field, enter a valid email address and you will then receive an email to that address asking you to click a link to verify that the domain is correct.



Verify Domain

In order to import targets in the next step, you must have at least one (1) verified domain. Please enter an email address with a domain matching that of the users you will be targeting. The verification link to validate the domain will be sent to the specified email.

No verified domains.

JaneDoe@gmail.com

- Adding domain: www.janedoe.com
- Verification email will be send to: JaneDoe@gmail.com

**Note:** Public domains such as yahoo.com and gmail.com are not permitted.

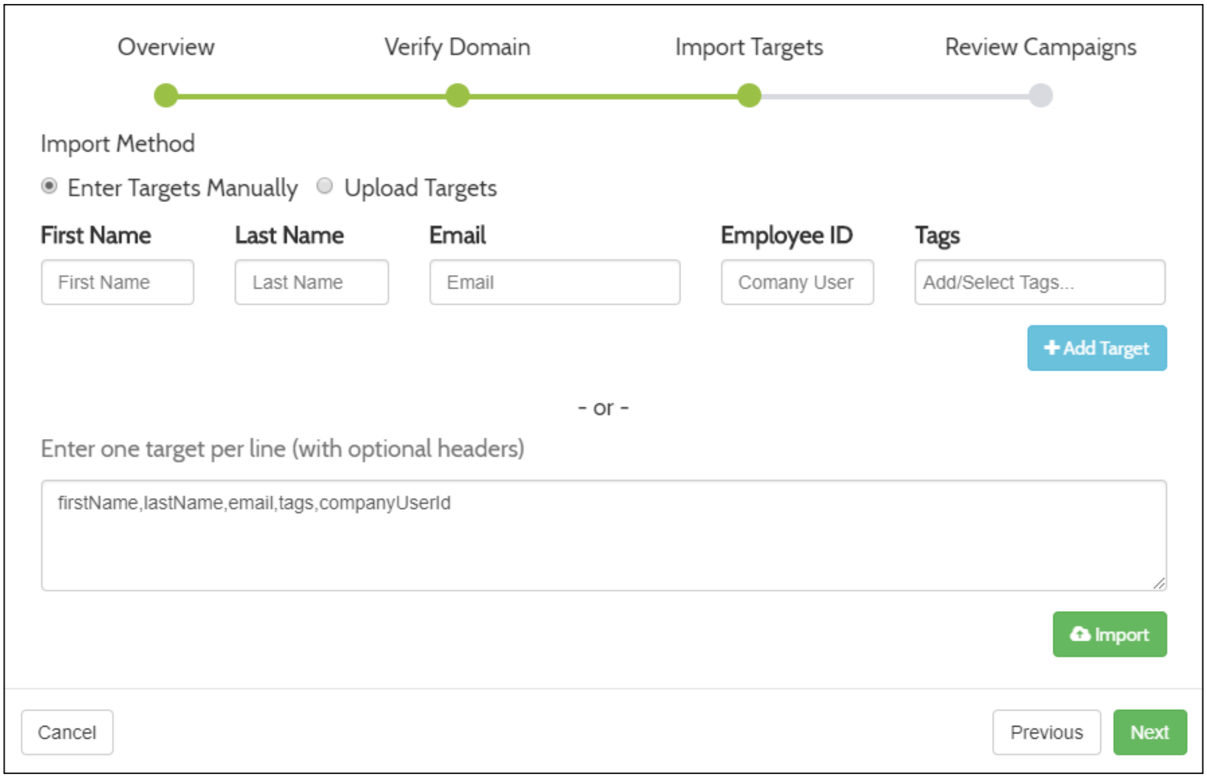
Once you have verified an email domain, click the **Next** button to continue.

## Step 2 — Import Targets

The next step is to import target users who you would like to send your Security Awareness Training campaigns to.

Do either of the following:

- Enter each email address manually.
- Upload targets by entering information in the Enter one target per line field.



Import Method

● Enter Targets Manually ○ Upload Targets

| First Name | Last Name | Email | Employee ID | Tags |
|---|---|---|---|---|
| First Name | Last Name | Email | Comany User | Add/Select Tags... |

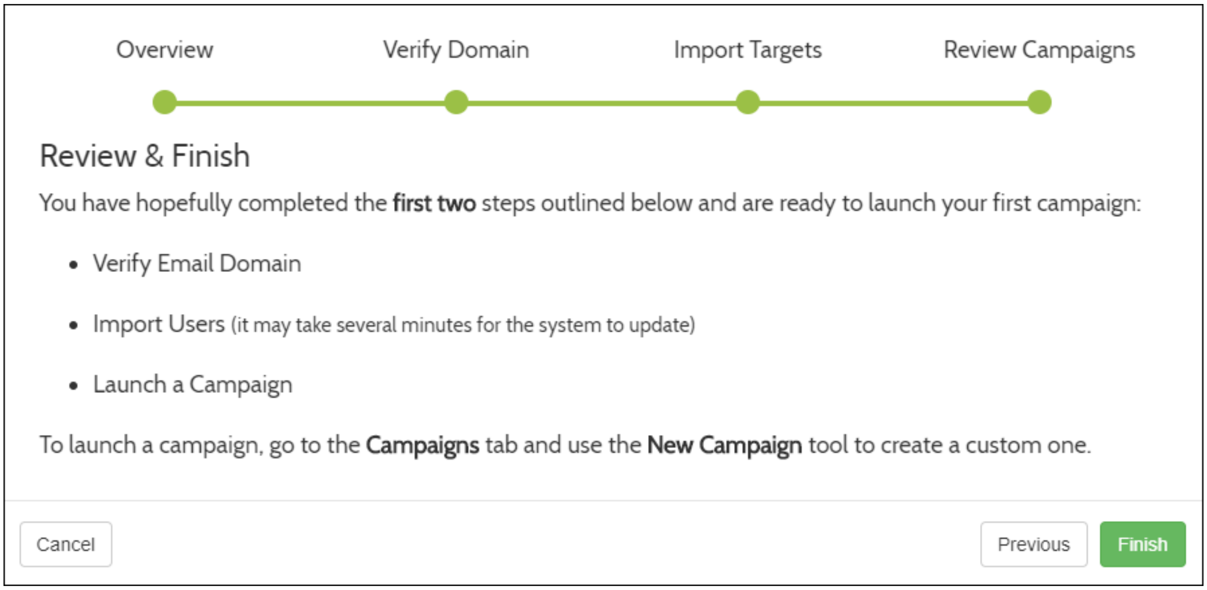
Enter one target per line (with optional headers)

```
firstName,lastName,email,tags,companyUserId
```

Once you have entered your target users click the **Next** button.

## Step 3 — Review Campaigns

The final step is to review the changes you made.



Review & Finish

You have hopefully completed the **first two** steps outlined below and are ready to launch your first campaign:

- Verify Email Domain
- Import Users (it may take several minutes for the system to update)
- Launch a Campaign

To launch a campaign, go to the **Campaigns** tab and use the **New Campaign** tool to create a custom one.

When you're done, click the **Finish** button.

The Security Awareness Training dashboard displays. From there you can set up and launch campaigns, review your settings, and analyze results. For more information, see the Security Awareness Training guides.

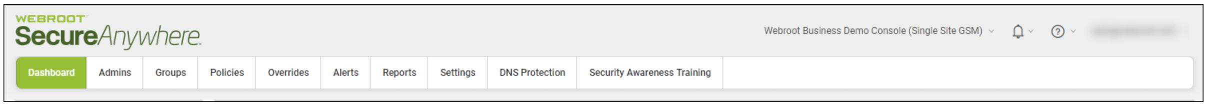
# Chapter 14: Working With the Business Console

For more information about the Business Console, see the following topics:

# Business Console Overview

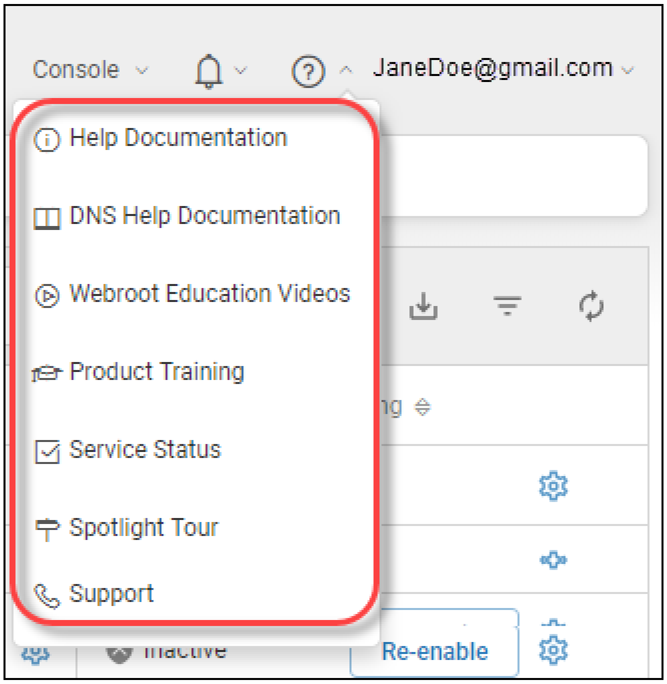
The Business Console allows you to easily manage your devices. The following tabs and functionality can be accessed from the Business Console:

- **Dashboard** — Displays various charts that give you a visual interpretation of your endpoints. From here you can review charts that contain information about the status of your endpoints. For more information, see About the Business Dashboard Tab. Additionally, you can sign up for a free trial of either DNS Protection or Security awareness Training.
- **Admins** — Displays a list of admins, and you can drill down to access information about their permission levels for various sites. For more information, see the Working With Admins section.
- **Groups** — Allows you to add, edit, delete and work with groups. For more information see the Working With Groups section.
- **Policies** — Allows you to create, copy, edit, and rename policies. For more information, see the Working With Policies section.
- **Overrides** — Allows you to create, customize, and import overrides. For more information, see the Working With Overrides section.
- **Alerts** — Allows you to create alerts at the global level. For more information, see the Working With Alerts section.
- **Reports** — Allows you to run reports on the health and performance of products. For more information, see the Working With Reports section.
- **Settings** — Allows you to view and edit account information and advanced settings. For more information see *Viewing and Editing Company Information on page 588* and *Viewing and Editing Advanced Settings on page 590*.
- **DNS Protection** — Displays information about Security Awareness Training and allows you to sign up for a free trial. For more information, see *DNS Protection Trial on page 598*.
- **Security Awareness** — Displays information about Security Awareness Training and allows you to sign up for a free trial. For more information, see *Security Awareness Training Trial on page 603*.

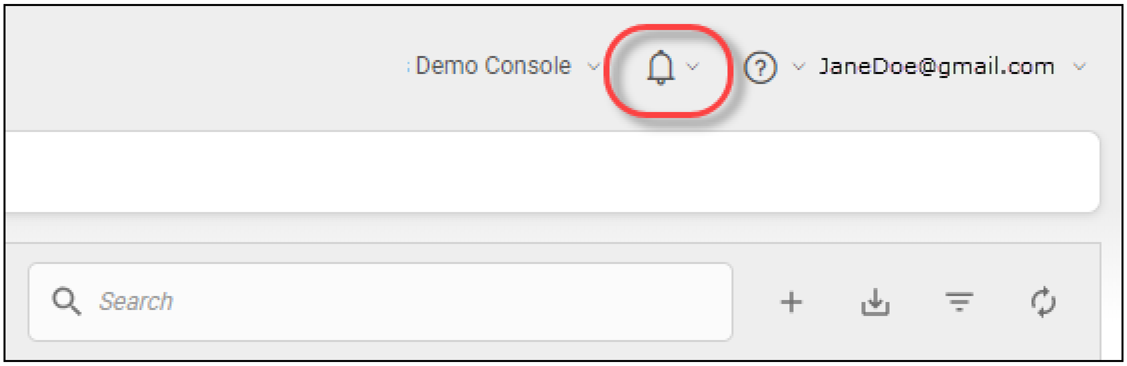


- For additional information, from the Help (?) icon in the upper right corner, click the **Down Arrow** to access any of the following:
  - Help Documentation — In most cases, the help that displays relates to the panel or window you are working in.

- DNS Help Documentation — Displays the business documentation portal where you can access DNS Protection guides.
- Webroot Education Videos — Displays a playlist of Webroot videos.
- Service Status — Displays the status page for your console, where you can view the status of your products and systems.
- Spotlight Tour — Allows you to view the Spotlight Tour, which is a quick tour through the console. For more information, see *About the Spotlight Tour on page 22*.
- Support — Click the link to enter a help ticket. For more information see Accessing Technical Support.



- To review any alerts or notifications, from the Alert Bell icon in the upper right corner, click the **Down Arrow**.

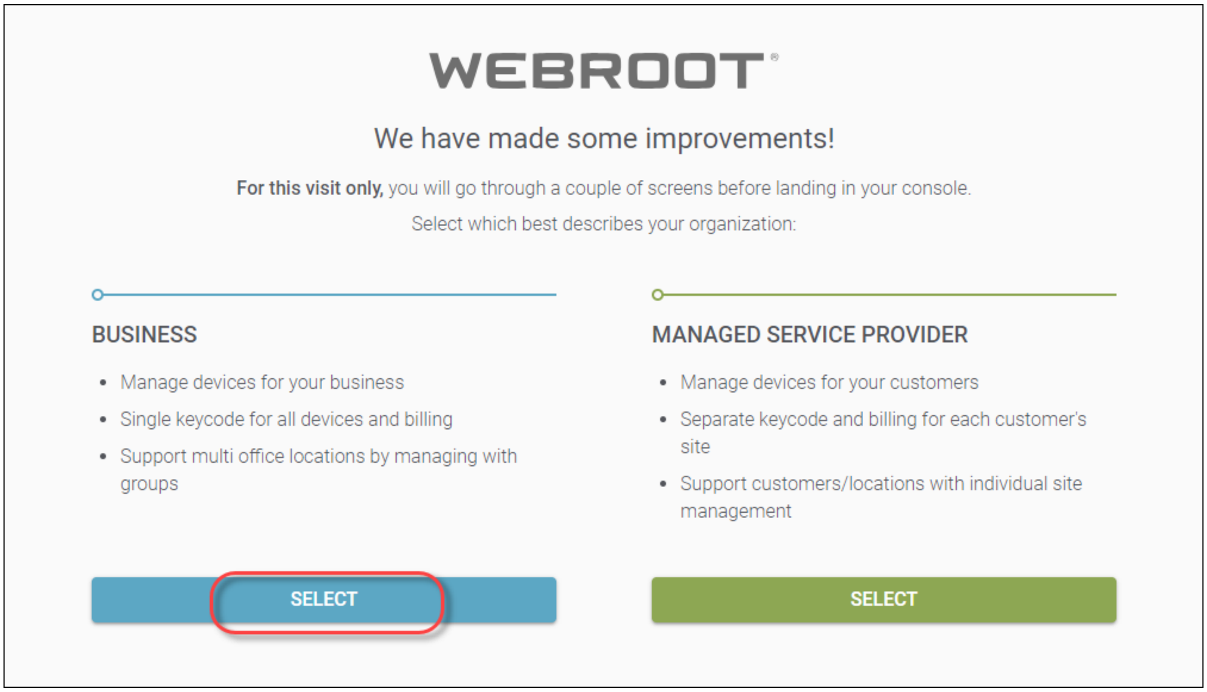

Demo Console
JaneDoe@gmail.com
Search

# Setting Up Your Business Console

After you select a Business console, you will need to enter information about your company.

**To set up your business console:**

1. Log in to the console.
2. Under Business, click the **Select** button.



WEBROOT

We have made some improvements!

**For this visit only,** you will go through a couple of screens before landing in your console.

Select which best describes your organization:

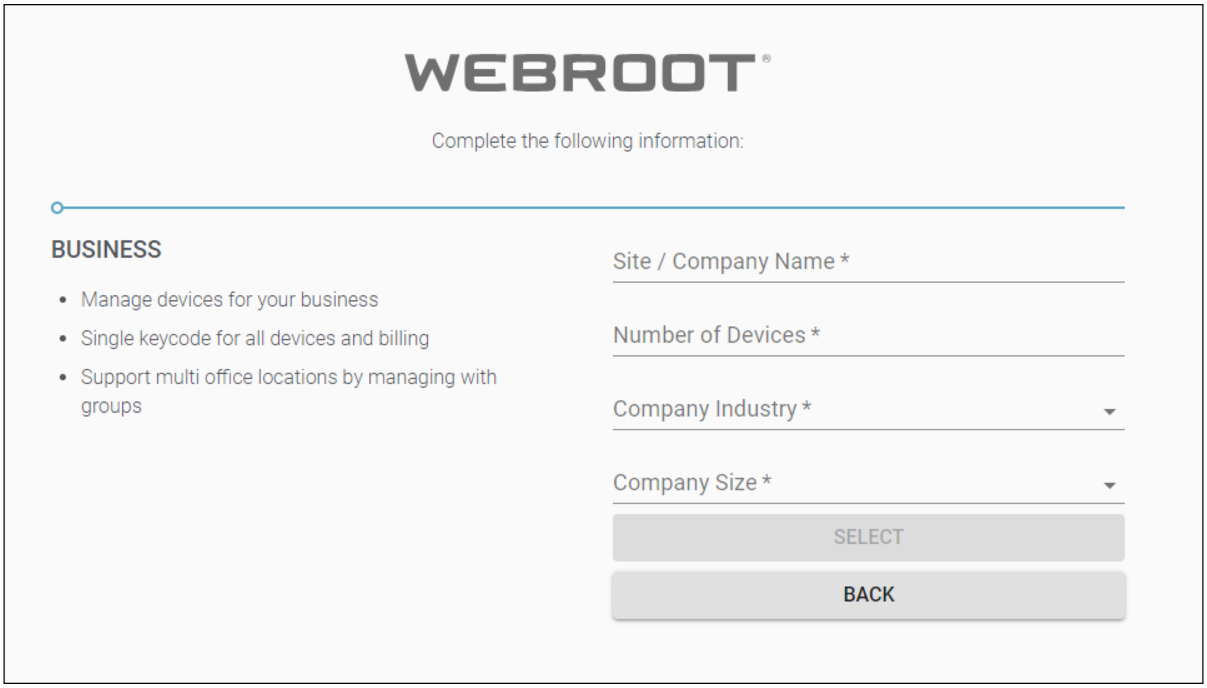
BUSINESS

- Manage devices for your business
- Single keycode for all devices and billing
- Support multi office locations by managing with groups

MANAGED SERVICE PROVIDER

- Manage devices for your customers
- Separate keycode and billing for each customer's site
- Support customers/locations with individual site management

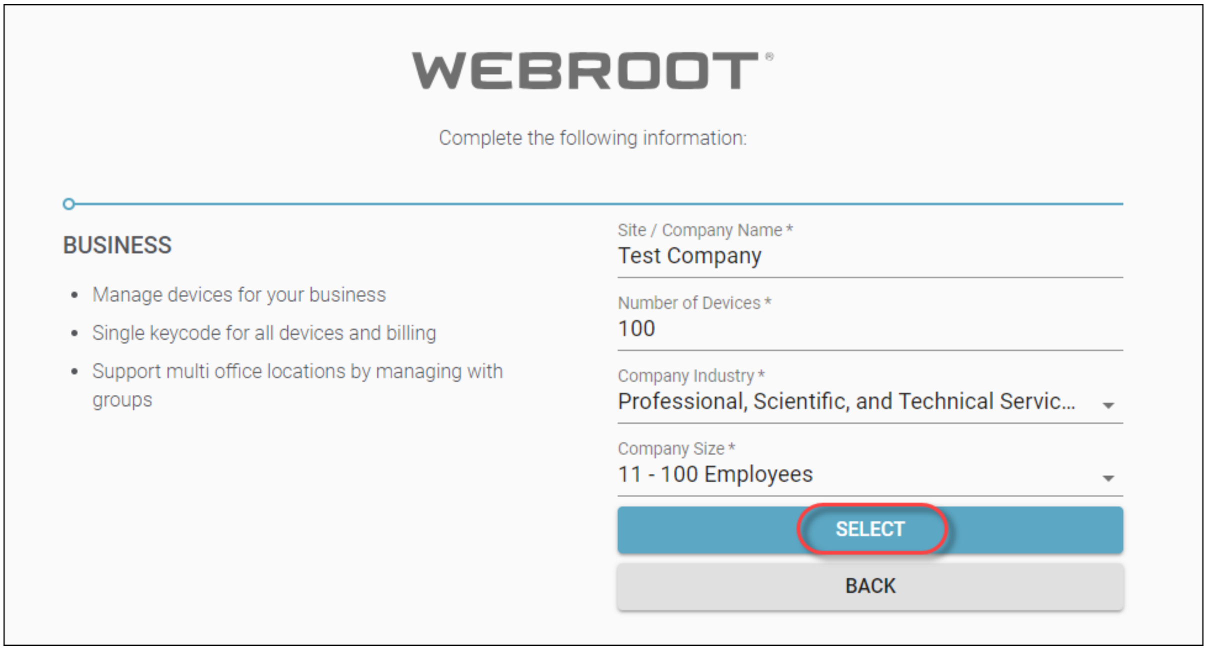
The Business information page displays.



- Manage devices for your business
- Single keycode for all devices and billing
- Support multi office locations by managing with groups

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

7. When you're done, click the **Select** button.



Complete the following information:

BUSINESS

- Manage devices for your business
- Single keycode for all devices and billing
- Support multi office locations by managing with groups

Site / Company Name *
Test Company

Number of Devices *
100

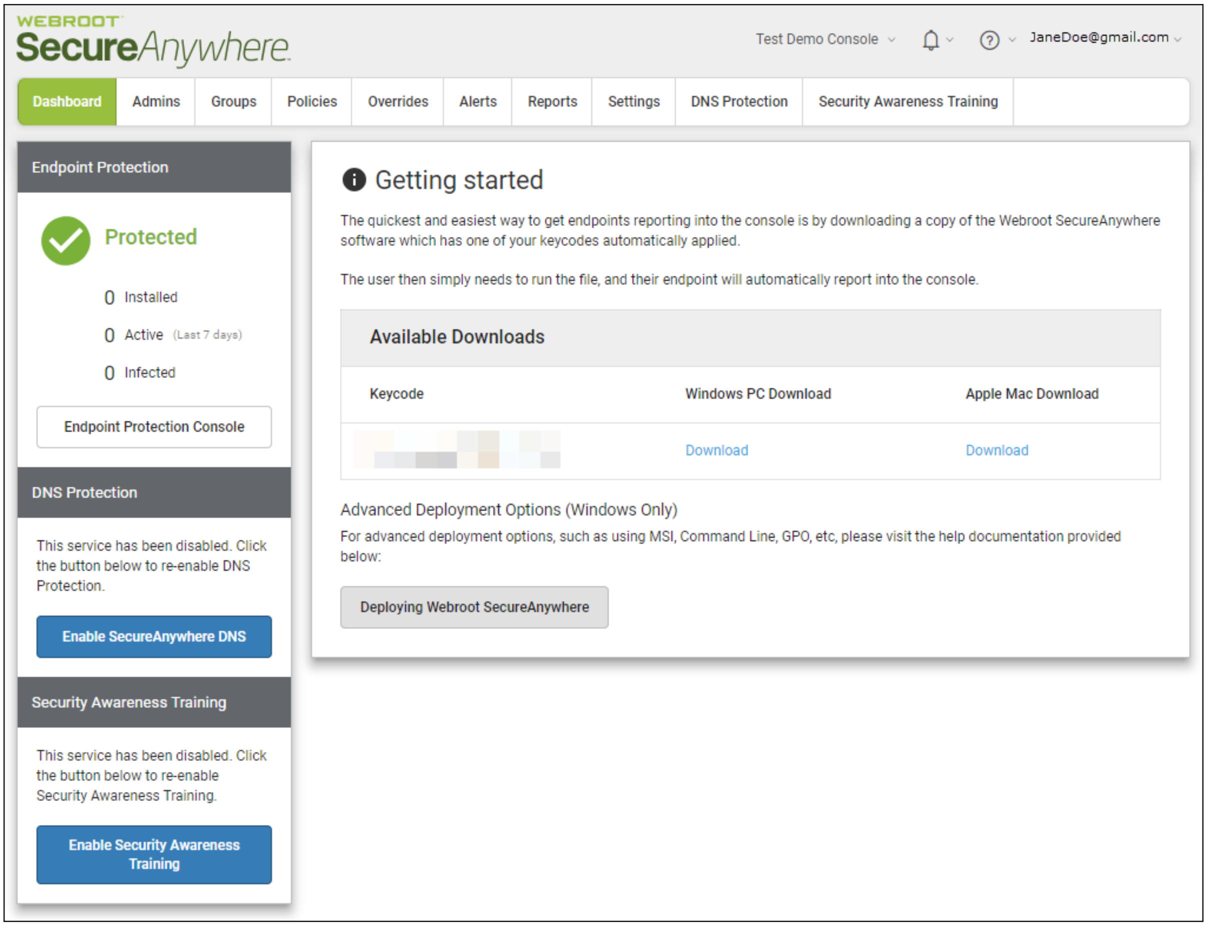
Company Industry *
Professional, Scientific, and Technical Servic...

Company Size *
11 - 100 Employees

The Dashboard for your company displays. Here you can do the following:

- View the Business Spotlight Tour, which is always available from the Help (?) drop-down menu. For more information, see *About the Business Console Spotlight Tour on page 608*.
- Go to Endpoint Protection.
- Start a free Security Awareness Training trial — Click the **Start Free Trial** button to go to the Security Awareness tab, where you can find more information and sign up for Security Awareness Training. For more information, see our Security Awareness Training Admin Guide.
- Start a free DNS Protection trial — Click the **Start Free Trial** button to go to the DNS tab, where you can find more information and sign up for DNS Protection. For more information, see our DNS Protection Admin Guide.

- Download and start using Webroot protection.


WEBROOT SecureAnywhere
Test Demo Console
JaneDoe@gmail.com
Dashboard
Admins
Groups
Policies
Overrides
Alerts
Reports
Settings
DNS Protection
Security Awareness Training
Endpoint Protection
Protected
Endpoint Protection Console
DNS Protection
Enable SecureAnywhere DNS
Security Awareness Training
Enable Security Awareness Training
Deploying Webroot SecureAnywhere

0 Installed

0 Active (Last 7 days)

0 Infected

This service has been disabled. Click the button below to re-enable DNS Protection.

This service has been disabled. Click the button below to re-enable Security Awareness Training.

### Getting started

The quickest and easiest way to get endpoints reporting into the console is by downloading a copy of the Webroot SecureAnywhere software which has one of your keycodes automatically applied.

The user then simply needs to run the file, and their endpoint will automatically report into the console.

**Available Downloads**

| Keycode | Windows PC Download | Apple Mac Download |
|---|---|---|
| [redacted] | Download | Download |

Advanced Deployment Options (Windows Only)

For advanced deployment options, such as using MSI, Command Line, GPO, etc, please visit the help documentation provided below:

8. As needed, you can edit your company's information. For more information, see *Viewing and Editing Company Information on page 588*

# About the Business Dashboard Tab

When you activate the console and devices start reporting in, at the top of the left panel you can get a quick overview of the following:

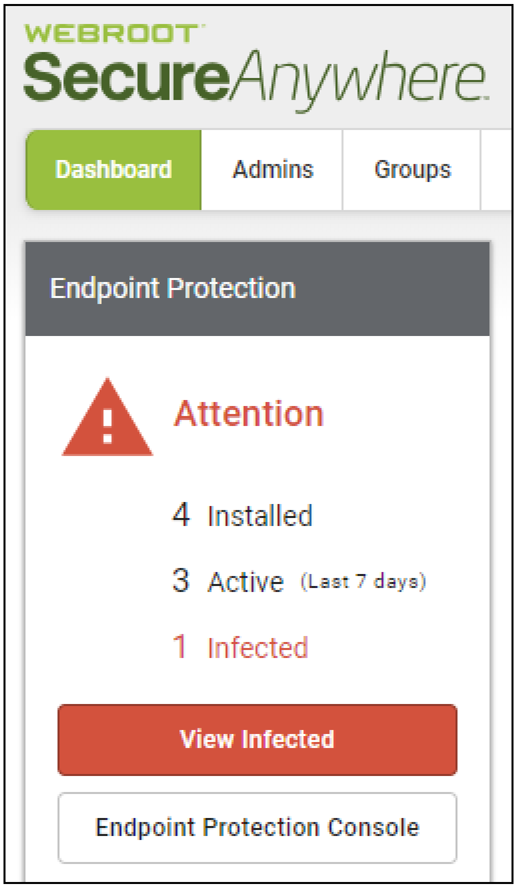
- Endpoint Protection
- DNS Protection
- Security Awareness Training
- Dashboard Charts

## Endpoint Protection

In this area you can see the following:

- How many devices are installed.
- How many devices are active.

- How many devices are infected.



If there is an issue, you can do either of the following:

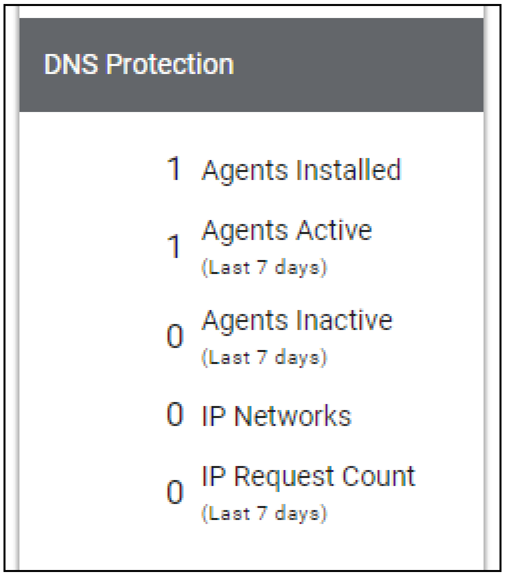
- Click the **View Infected** button.
- Click the **Endpoint Protection Console** button. For more information, see the Endpoint Protection Admin Guide.

## DNS Protection

In this area, when this service is enabled, you can see the following information:

- How many devices are installed.
- How many devices are active
- How many devices have not checked in during the last seven days.

- How many requests in the last seven days.
- Additionally, you can see how many days are left in your subscription.



DNS Protection

1 Agents Installed

1 Agents Active (Last 7 days)

0 Agents Inactive (Last 7 days)

0 IP Networks

0 IP Request Count (Last 7 days)

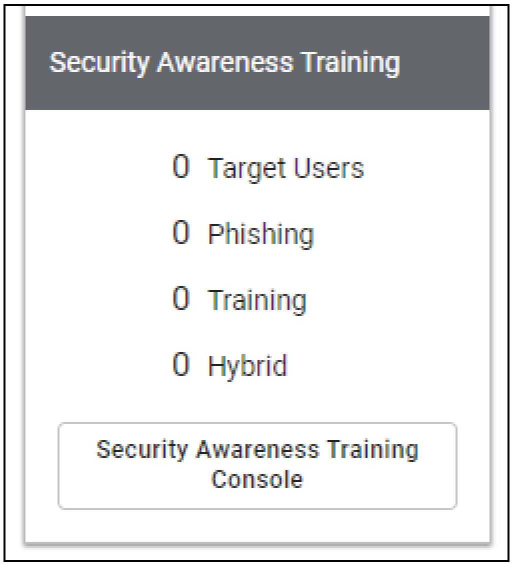
For more information about DNS Protection, see *DNS Protection Trial on page 598* and the DNS Protection Admin Guide.

## Security Awareness Training

In this area, when this service is enabled, you can see the following information:

- How many total active campaigns are running.
- How many phishing campaigns are running
- How many training campaigns are running.

- How many hybrid campaigns are running.



Security Awareness Training

0 Target Users

0 Phishing

0 Training

0 Hybrid

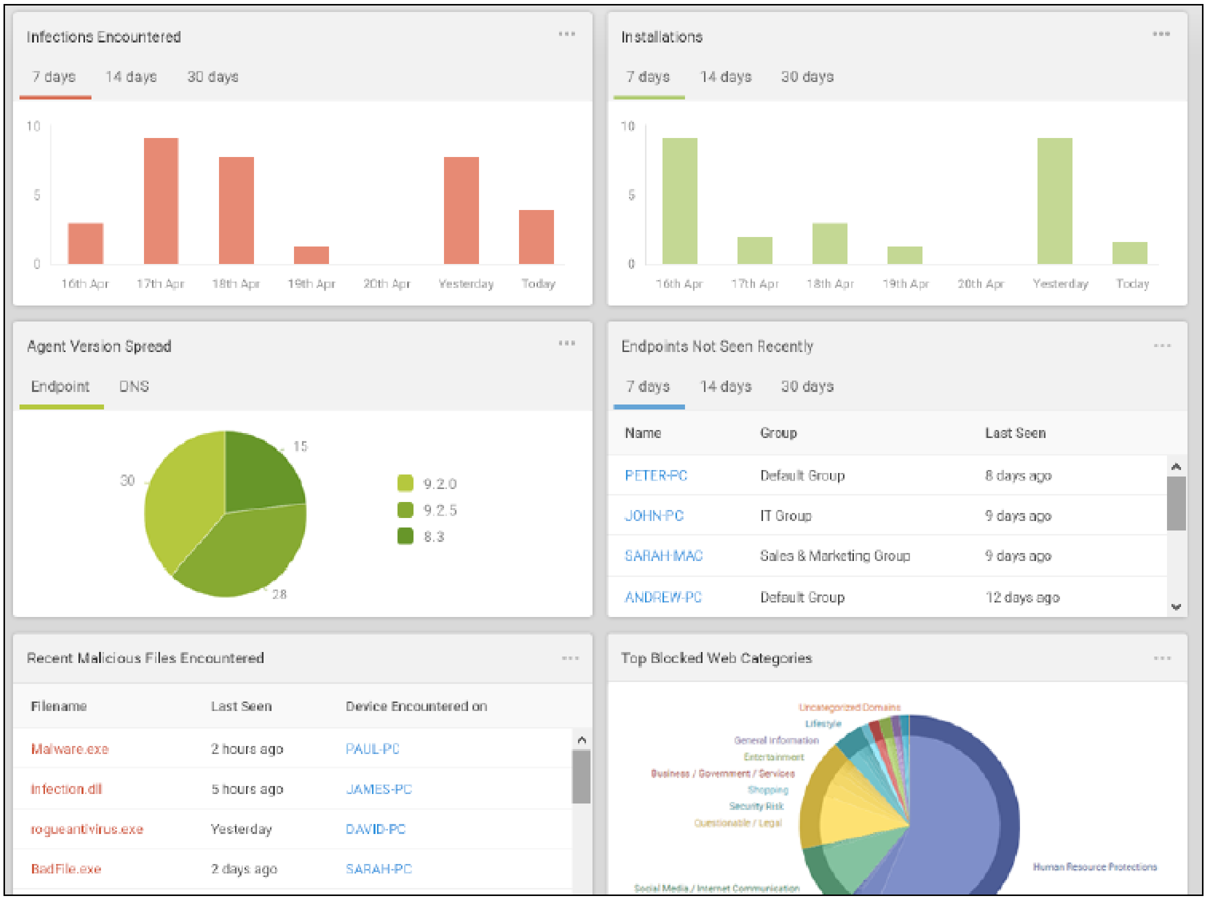
As needed, you can click the Go to Security Awareness button to log in to the Security Awareness Training console. For more information, see Security Awareness Training Trial and the Security Awareness Training Admin Guide.

## Dashboard Charts

The Business Dashboard tab displays the following standard reports that allow you to easily review information about your endpoints.

- Infections Encountered
- Installations
- Agent Version Spread
- Endpoints Not Seen Recently
- Recent Malicious Files Encountered

- Top Blocked Web Categories



Endpoints Not Seen Recently

7 days 14 days 30 days

| Name | Group | Last Seen |
|---|---|---|
| PETER-PC | Default Group | 8 days ago |
| JOHN-PC | IT Group | 9 days ago |
| SARAH-MAC | Sales & Marketing Group | 9 days ago |
| ANDREW-PC | Default Group | 12 days ago |

Recent Malicious Files Encountered

| Filename | Last Seen | Device Encountered on |
|---|---|---|
| Malware.exe | 2 hours ago | PAUL-PC |
| infection.dll | 5 hours ago | JAMES-PC |
| rogueantivirus.exe | Yesterday | DAVID-PC |
| BadFile.exe | 2 days ago | SARAH-PC |

As needed, you can do the following:

- *Drilling Down in Dashboard Charts on page 58*
- *Editing Dashboard Charts on page 51*

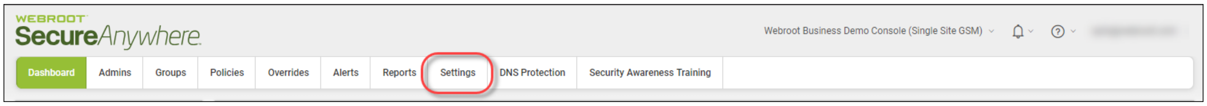
**Note:** Although the Business Dashboard tab has a different layout than our standard Dashboard tab, the functionality is much the same.

# Viewing and Editing Company Information

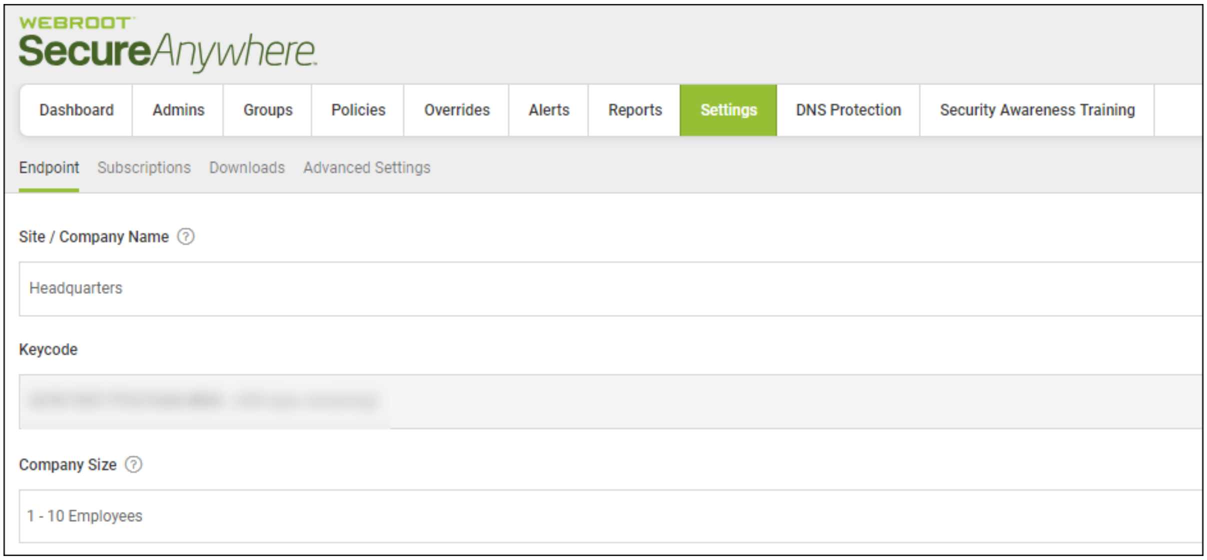
You can view and edit company in formation in the Endpoint tab. This is the information that you entered when you created your site.

**To view and edit company information:**

1. Log in to the management console.
2. Click the **Settings** tab.



The Settings tab displays with the Endpoint tab active.



Site / Company Name

Headquarters

Keycode

[redacted]

Company Size

1 - 10 Employees

3. As needed, you can edit the following fields.
   - Company Name
   - Company Size
   - Company Industry
   - Comments. This is an optional field.
   - Site Seats

- Default Endpoint Policy
- Report Distribution List

**Note:** You cannot edit the information in the Keycode field.

The changes you make are automatically saved.

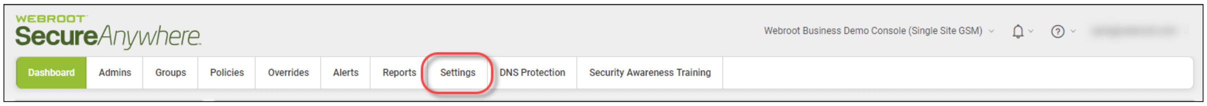
# Viewing and Editing Advanced Settings

In the Advanced settings tab, you can view and edit the following:

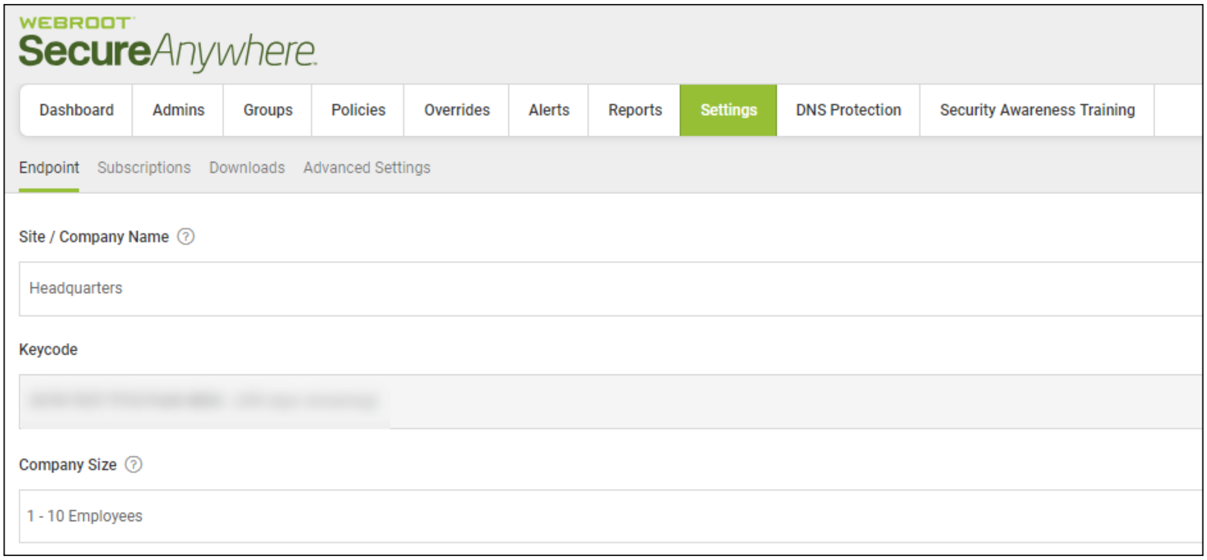
- **Data Filter** — Determine whether to display or the data for endpoints that has not been seen for a period of time.
- **Converting Your Console** — Convert your console to one that manages multiple sites. For more information, see *About the Managed Service Provider Console on page 16*.

**To view and edit company information:**

1. Log in to the management console.
2. Click the **Settings** tab.



The Settings tab displays with the Endpoint tab active.



Site / Company Name

Headquarters

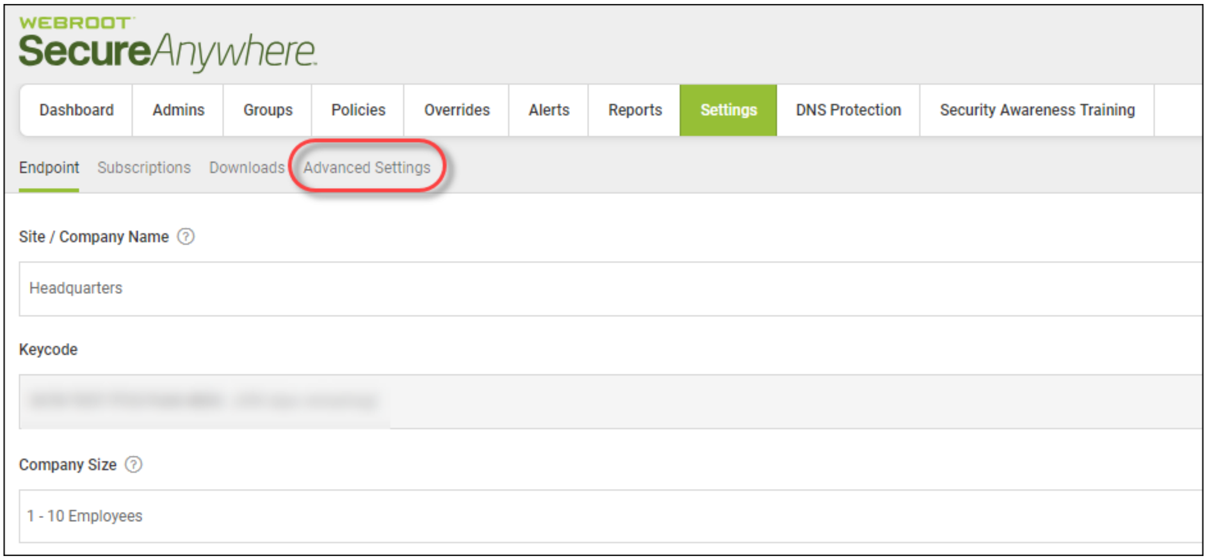
Keycode

[redacted]

Company Size

1 - 10 Employees

3. Click the **Advanced Settings** tab.



Site / Company Name

Headquarters

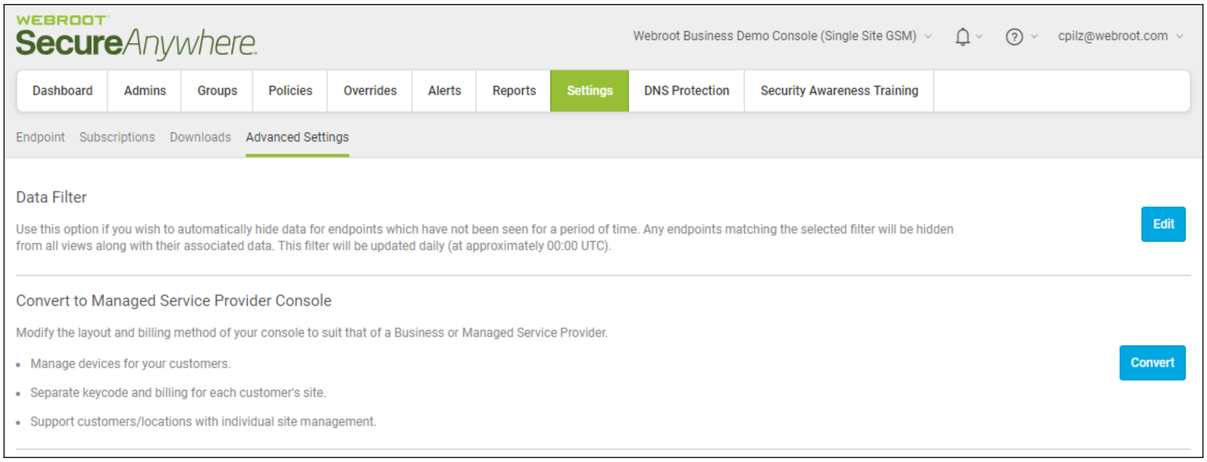
Keycode

[redacted]

Company Size

1 - 10 Employees

The Advanced Settings tab displays.



Data Filter

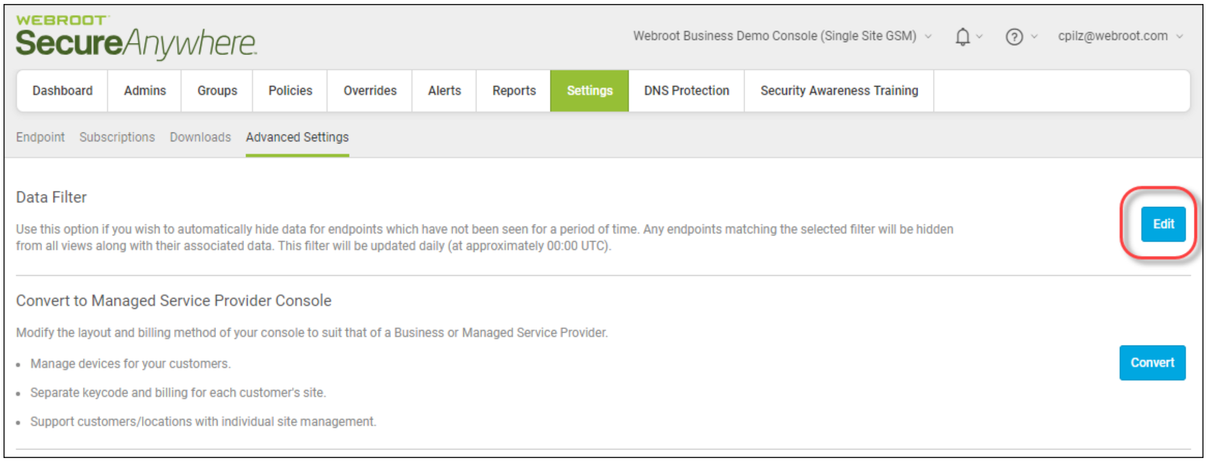
Use this option if you wish to automatically hide data for endpoints which have not been seen for a period of time. Any endpoints matching the selected filter will be hidden from all views along with their associated data. This filter will be updated daily (at approximately 00:00 UTC).

Convert to Managed Service Provider Console

Modify the layout and billing method of your console to suit that of a Business or Managed Service Provider.

- Manage devices for your customers.
- Separate keycode and billing for each customer's site.
- Support customers/locations with individual site management.

4. To hide data for endpoints which have not been seen, click the **Edit** button. This information updates daily.



Data Filter

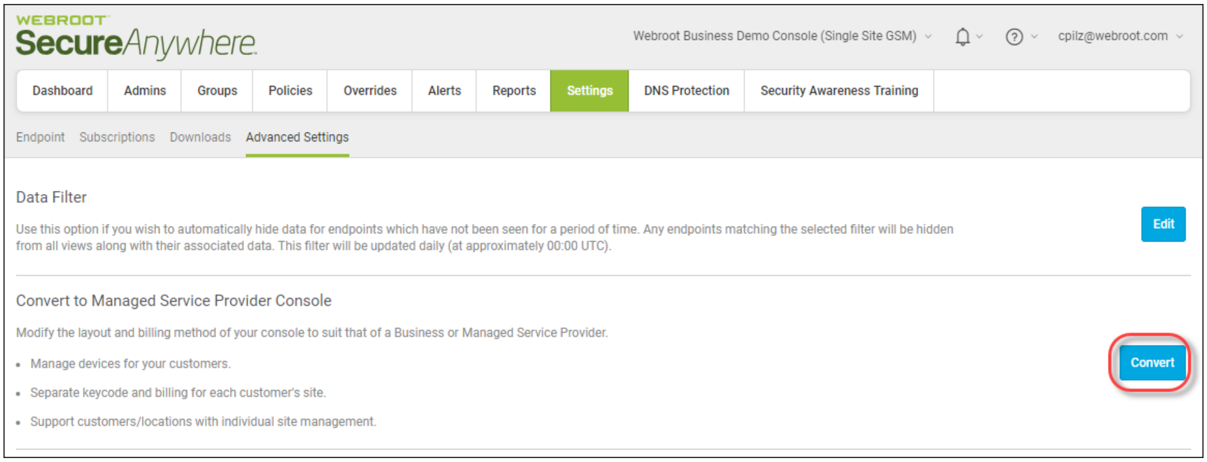
Use this option if you wish to automatically hide data for endpoints which have not been seen for a period of time. Any endpoints matching the selected filter will be hidden from all views along with their associated data. This filter will be updated daily (at approximately 00:00 UTC).

Convert to Managed Service Provider Console

Modify the layout and billing method of your console to suit that of a Business or Managed Service Provider.

- Manage devices for your customers.
- Separate keycode and billing for each customer's site.
- Support customers/locations with individual site management.

5. To change your console to a multi-site or Managed Service Provider, click the **Convert** button.



Data Filter

Use this option if you wish to automatically hide data for endpoints which have not been seen for a period of time. Any endpoints matching the selected filter will be hidden from all views along with their associated data. This filter will be updated daily (at approximately 00:00 UTC).

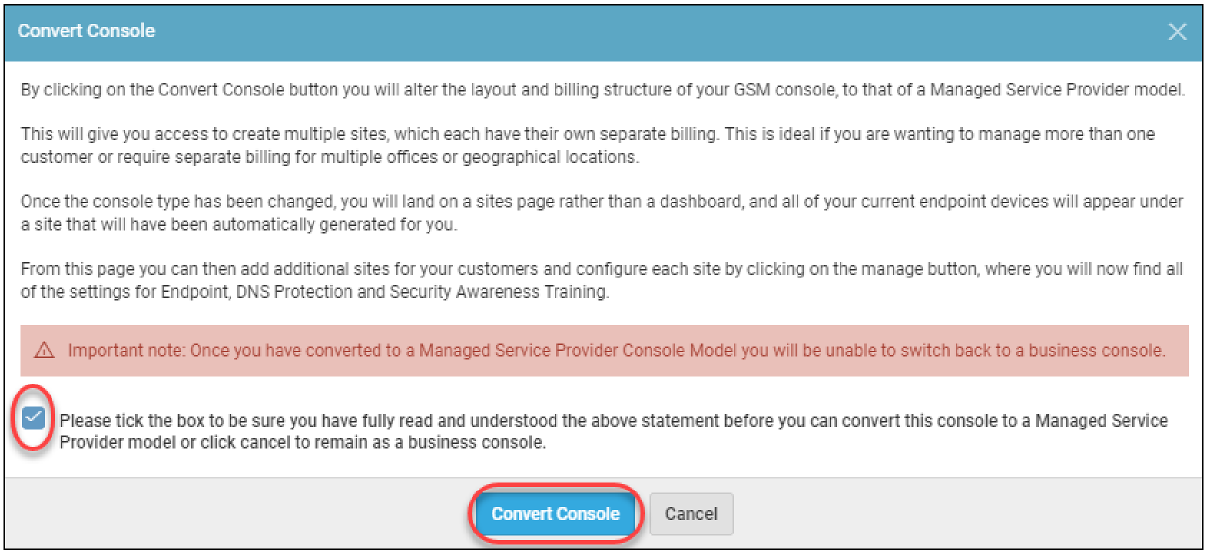
Convert to Managed Service Provider Console

Modify the layout and billing method of your console to suit that of a Business or Managed Service Provider.

- Manage devices for your customers.
- Separate keycode and billing for each customer's site.
- Support customers/locations with individual site management.

6. When the Convert Console window displays, do the following:
   - Review the information about what happens when you convert your console.
   - Select the **Confirm** checkbox to acknowledge that you have fully read and understand the information.

- Click the **Convert Consolee** button.



By clicking on the Convert Console button you will alter the layout and billing structure of your GSM console, to that of a Managed Service Provider model.

This will give you access to create multiple sites, which each have their own separate billing. This is ideal if you are wanting to manage more than one customer or require separate billing for multiple offices or geographical locations.

Once the console type has been changed, you will land on a sites page rather than a dashboard, and all of your current endpoint devices will appear under a site that will have been automatically generated for you.

From this page you can then add additional sites for your customers and configure each site by clicking on the manage button, where you will now find all of the settings for Endpoint, DNS Protection and Security Awareness Training.

⚠ Important note: Once you have converted to a Managed Service Provider Console Model you will be unable to switch back to a business console.

☑ Please tick the box to be sure you have fully read and understood the above statement before you can convert this console to a Managed Service Provider model or click cancel to remain as a business console.

**Note:** Once you convert your console to a multi-site console, you will not be able to convert back to a single site console.

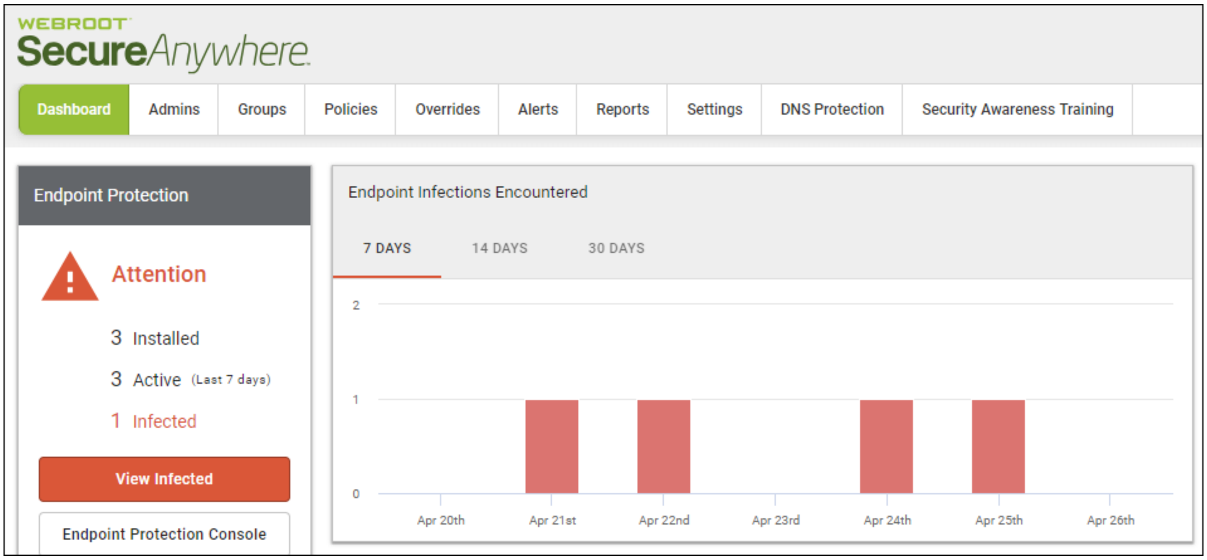
# Purchasing Additional Site Seats

Follow this procedure to purchase additional site seats without having to contact Support.

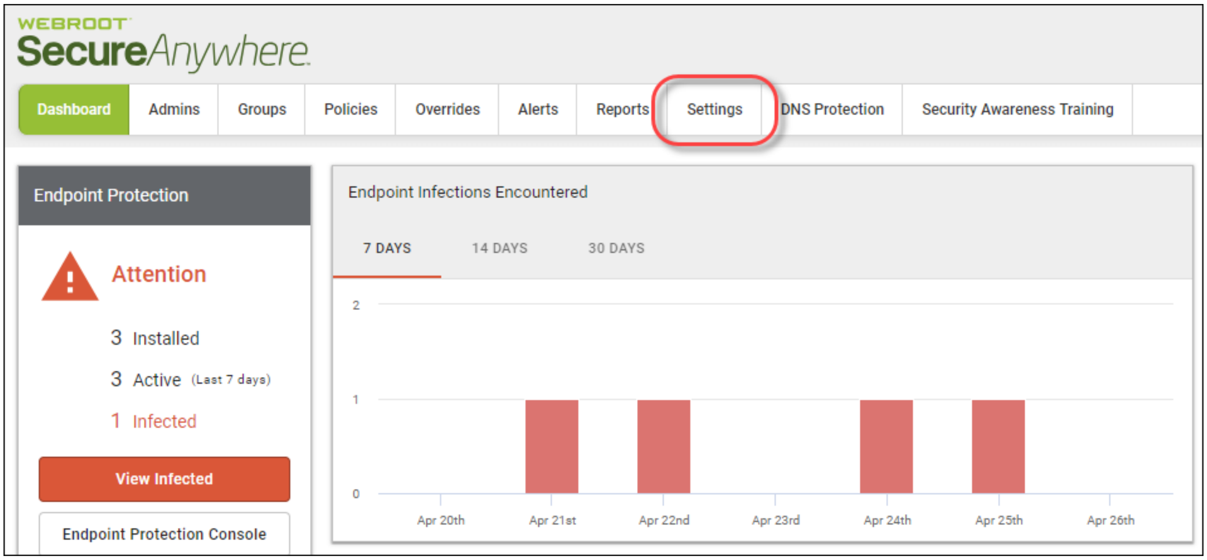
**To purchase an additional site seat:**

1. Log in to the management console.

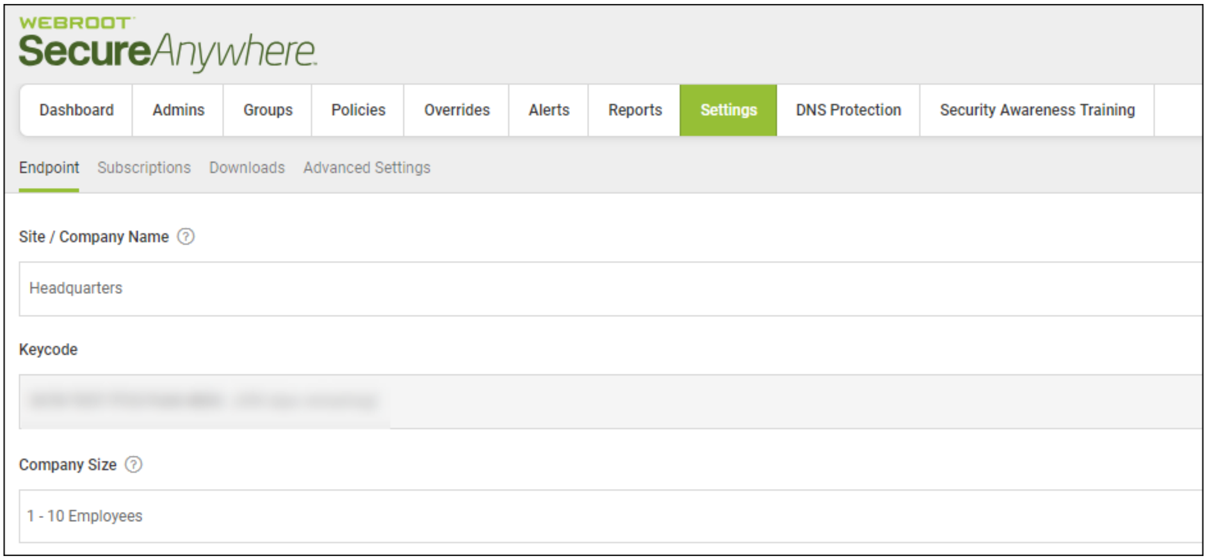
   The management console displays.



2. Click the **Settings** tab.



The Settings tab displays with the Endpoint tab active.



Site / Company Name

Headquarters

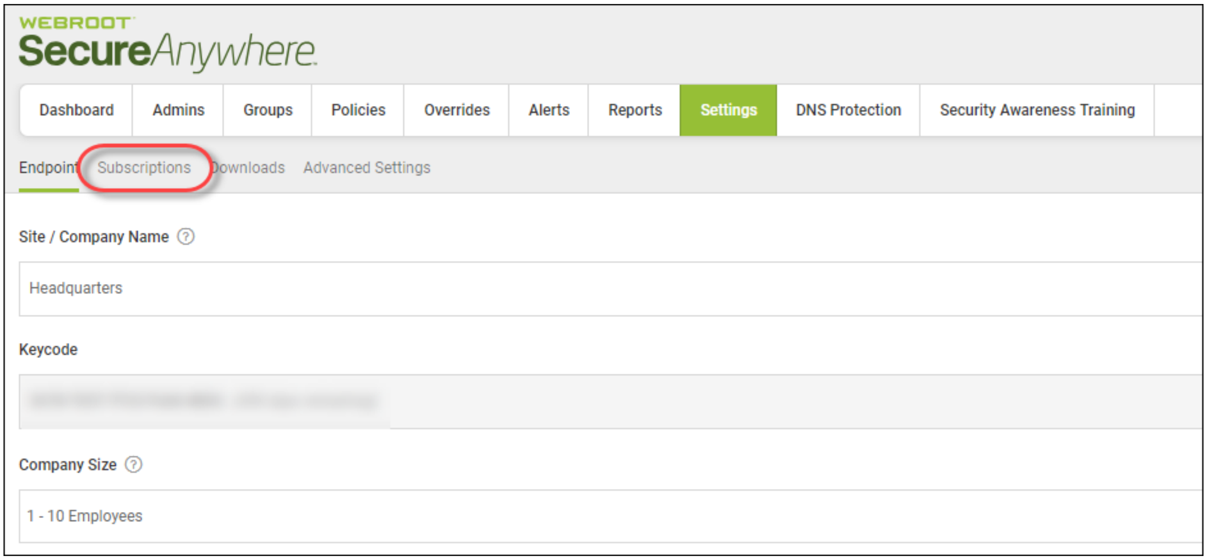
Keycode

[redacted]

Company Size

1 - 10 Employees

3. Click the **Subscriptions** tab.



Site / Company Name

Headquarters

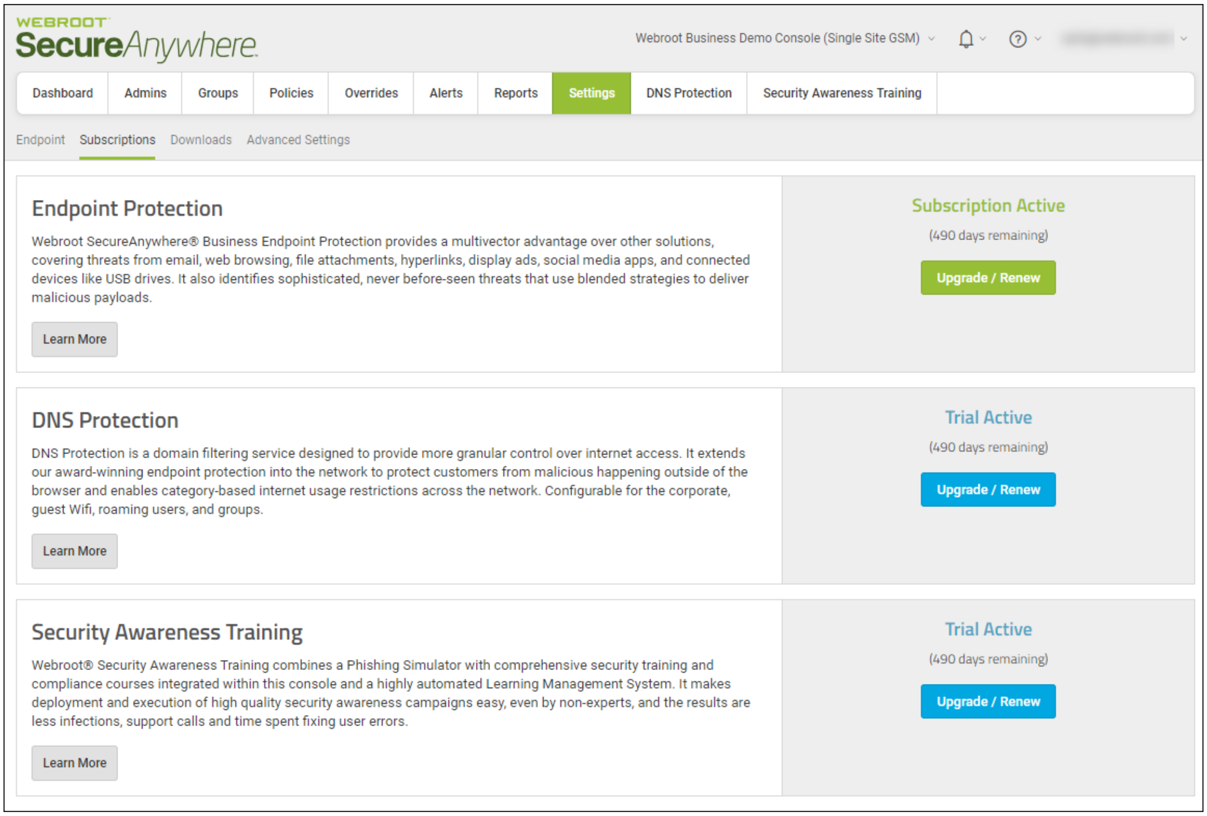
Keycode

[redacted]

Company Size

1 - 10 Employees

The Subscriptions tab displays.



Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multivector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never before-seen threats that use blended strategies to deliver malicious payloads.

DNS Protection

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.

Security Awareness Training

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

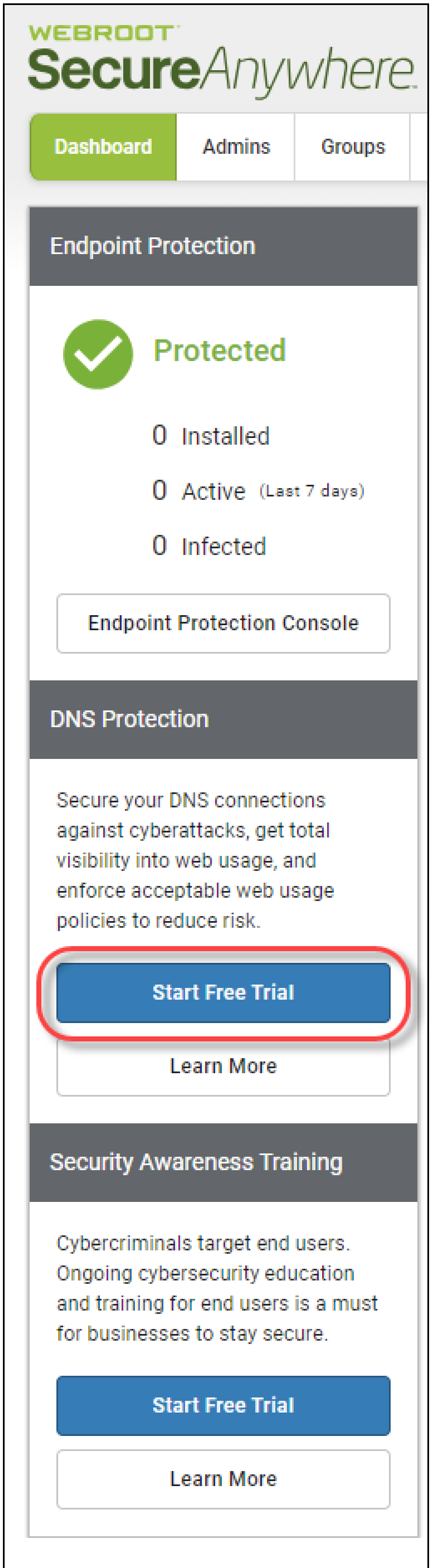
4. From the Subscriptions tab, you can add additional seats for Endpoint, DNS Protection, or Security Awareness Training.

# DNS Protection Trial

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.

**To start a free trial of DNS Protection:**

1. From the Dashboard tab, in the DNS Protection area, click the **Start Free Trial** button.



Endpoint Protection

Protected

0 Installed

0 Active (Last 7 days)

0 Infected

DNS Protection

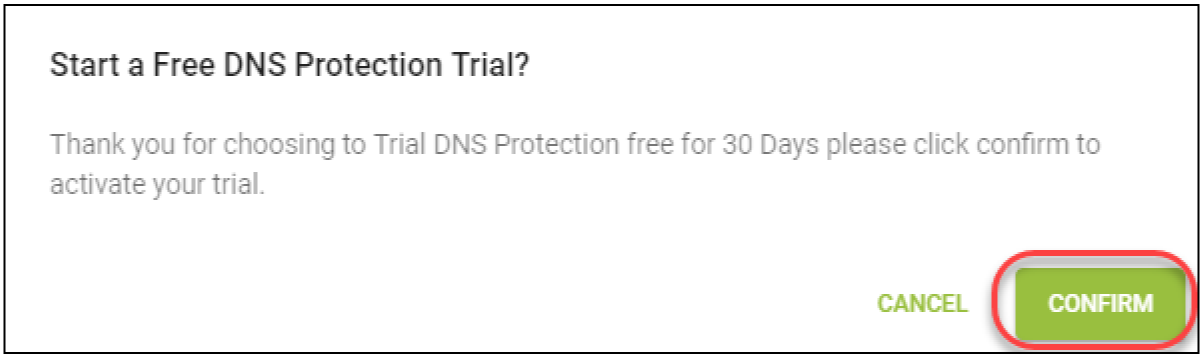
Secure your DNS connections against cyberattacks, get total visibility into web usage, and enforce acceptable web usage policies to reduce risk.

Security Awareness Training

Cybercriminals target end users. Ongoing cybersecurity education and training for end users is a must for businesses to stay secure.

**Note:** If you'd like to learn more before you start a Free Trial, click the **Learn More** button.

2. When the Confirm message displays, click the **Confirm** button.

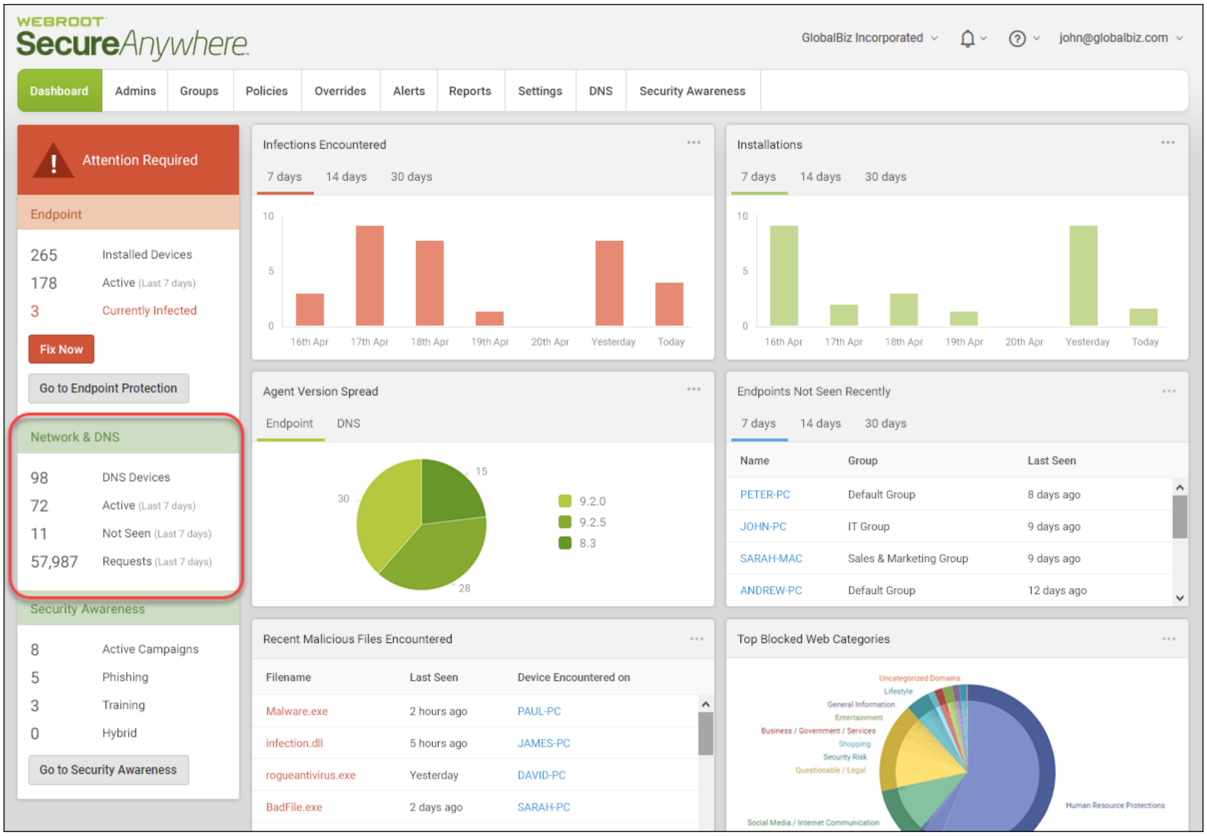


Start a Free DNS Protection Trial?

Thank you for choosing to Trial DNS Protection free for 30 Days please click confirm to activate your trial.

When you have DNS Protection enabled, your Dashboard tab displays information about the following:

- Number of DNS Devices
- Number of Active Devices
- Number of Devices not seen in the last seven days
- Number of requests seen in the last seven days.



Endpoint

| | |
|---|---|
| 265 | Installed Devices |
| 178 | Active (Last 7 days) |
| 3 | Currently Infected |

Fix Now

Go to Endpoint Protection

Network & DNS

| | |
|---|---|
| 98 | DNS Devices |
| 72 | Active (Last 7 days) |
| 11 | Not Seen (Last 7 days) |
| 57,987 | Requests (Last 7 days) |

Security Awareness

| | |
|---|---|
| 8 | Active Campaigns |
| 5 | Phishing |
| 3 | Training |
| 0 | Hybrid |

Go to Security Awareness

Endpoints Not Seen Recently

7 days 14 days 30 days

| Name | Group | Last Seen |
|---|---|---|
| PETER-PC | Default Group | 8 days ago |
| JOHN-PC | IT Group | 9 days ago |
| SARAH-MAC | Sales & Marketing Group | 9 days ago |
| ANDREW-PC | Default Group | 12 days ago |

Recent Malicious Files Encountered

| Filename | Last Seen | Device Encountered on |
|---|---|---|
| Malware.exe | 2 hours ago | PAUL-PC |
| infection.dll | 5 hours ago | JAMES-PC |
| rogueantivirus.exe | Yesterday | DAVID-PC |
| BadFile.exe | 2 days ago | SARAH-PC |

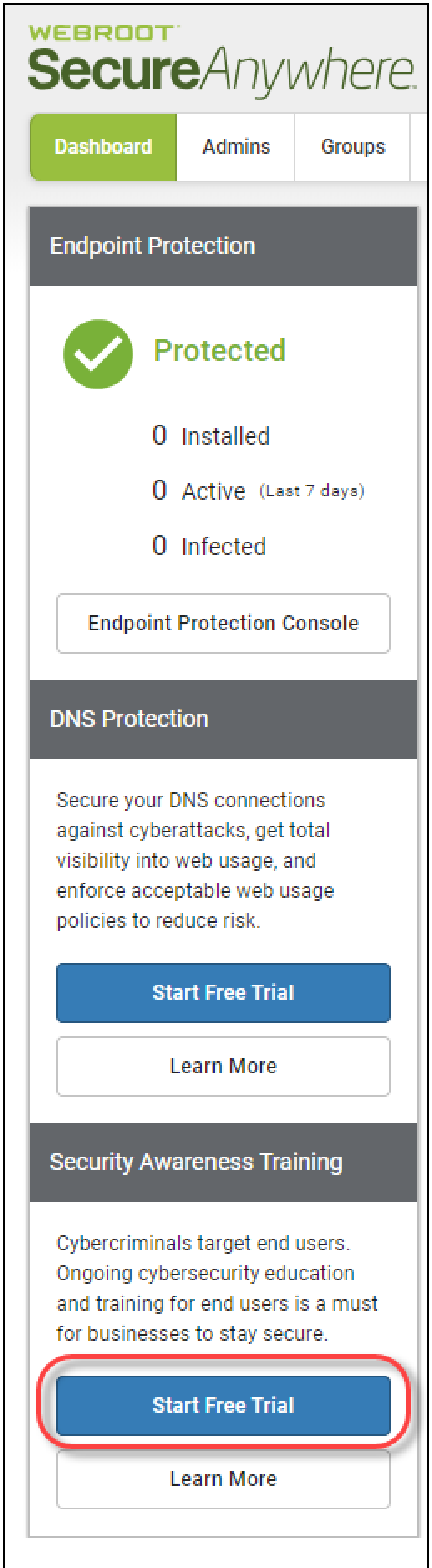
3. For more information, see the DNS Protection Admin Guide.

# Security Awareness Training Trial

Webroot® Security Awareness Training combines a Phishing Simulator with comprehensive security training and compliance courses integrated within this console and a highly automated Learning Management System. It makes deployment and execution of high quality security awareness campaigns easy, even by non-experts, and the results are less infections, support calls and time spent fixing user errors.

**To start a free trial of Security Awareness Training:**

1. From the Dashboard tab, in the Security Awareness Training area, slick the **Start Free Trial** button.



Endpoint Protection

Protected

0 Installed

0 Active (Last 7 days)

0 Infected

DNS Protection

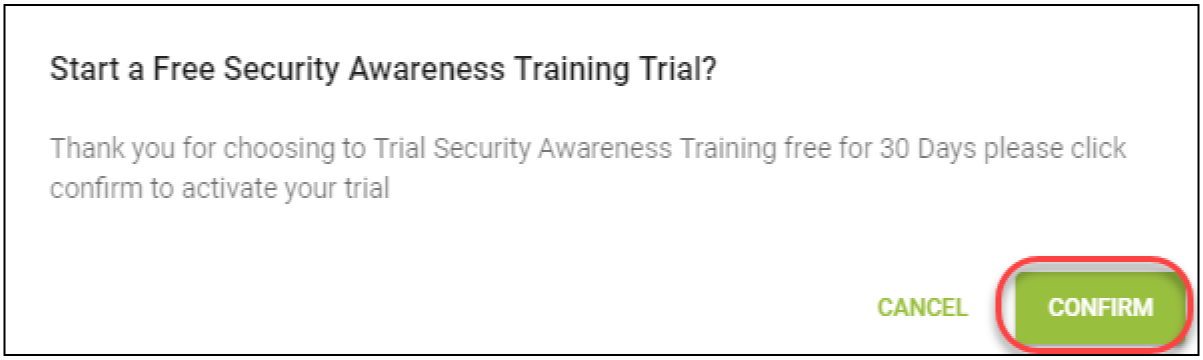
Secure your DNS connections against cyberattacks, get total visibility into web usage, and enforce acceptable web usage policies to reduce risk.

Security Awareness Training

Cybercriminals target end users. Ongoing cybersecurity education and training for end users is a must for businesses to stay secure.

**Note:** If you'd like to learn more before you start a Free Trial, click the **Learn More** button.

2. When the confirmation message displays, click the **Confirm** button.

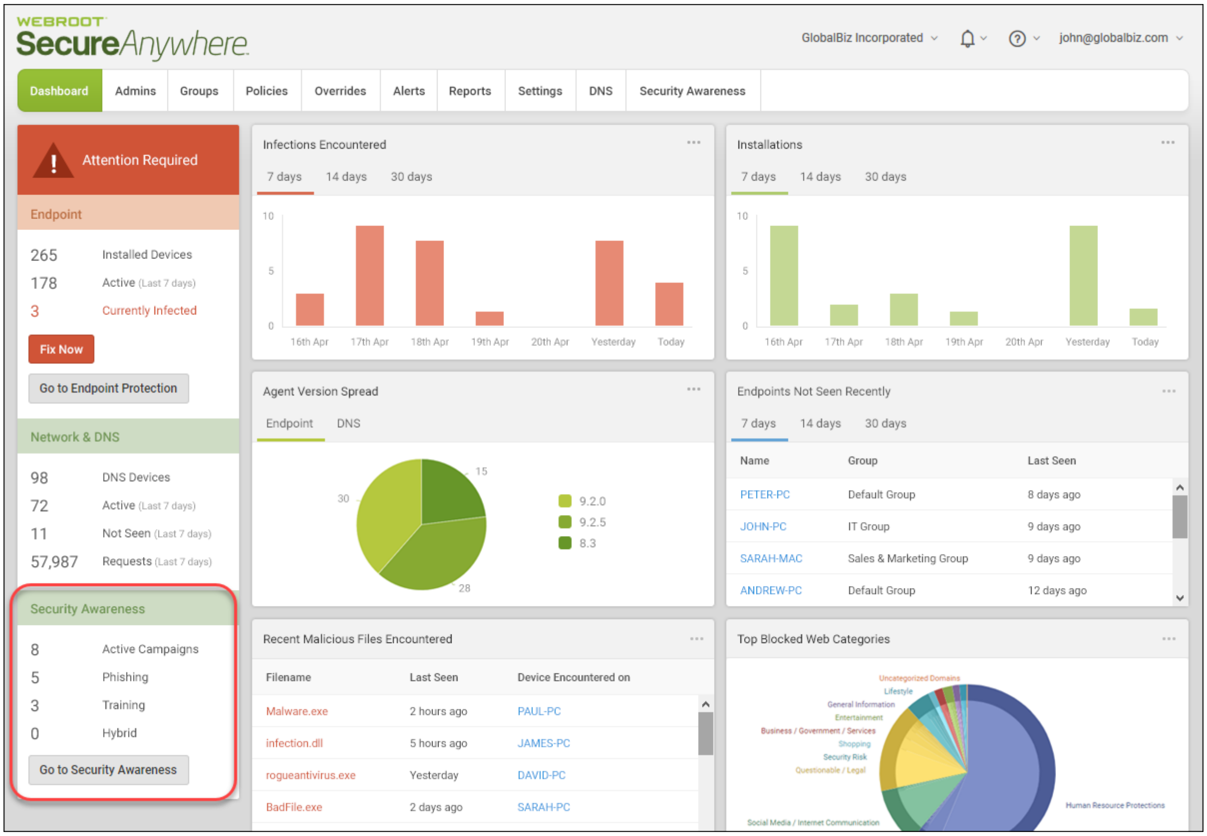


Start a Free Security Awareness Training Trial?

Thank you for choosing to Trial Security Awareness Training free for 30 Days please click confirm to activate your trial

When you have Security Awareness Training enabled, your Dashboard tab displays information about the following:

- Total number of Active Campaigns
- Number of Phishing Campaigns
- Number of Training Campaigns
- Number of Hybrid Campaigns



Endpoint

| | |
|---|---|
| 265 | Installed Devices |
| 178 | Active (Last 7 days) |
| 3 | Currently Infected |

Network & DNS

| | |
|---|---|
| 98 | DNS Devices |
| 72 | Active (Last 7 days) |
| 11 | Not Seen (Last 7 days) |
| 57,987 | Requests (Last 7 days) |

Security Awareness

| | |
|---|---|
| 8 | Active Campaigns |
| 5 | Phishing |
| 3 | Training |
| 0 | Hybrid |

| Name | Group | Last Seen |
|---|---|---|
| PETER-PC | Default Group | 8 days ago |
| JOHN-PC | IT Group | 9 days ago |
| SARAH-MAC | Sales & Marketing Group | 9 days ago |
| ANDREW-PC | Default Group | 12 days ago |

| Filename | Last Seen | Device Encountered on |
|---|---|---|
| Malware.exe | 2 hours ago | PAUL-PC |
| infection.dll | 5 hours ago | JAMES-PC |
| rogueantivirus.exe | Yesterday | DAVID-PC |
| BadFile.exe | 2 days ago | SARAH-PC |

3. For more information, see the Security Awareness Training Admin Guide.

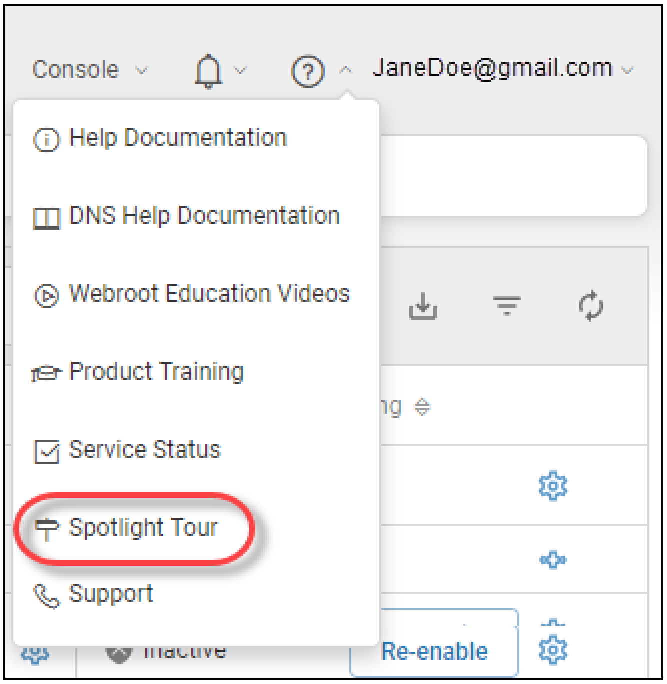
# About the Business Console Spotlight Tour

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

- The tabs in the Main menu
- Additional security layers, such as DNS Protection and Security Awareness Training
- Later, as needed, you can view the tour again.

**To view the Spotlight Tour:**

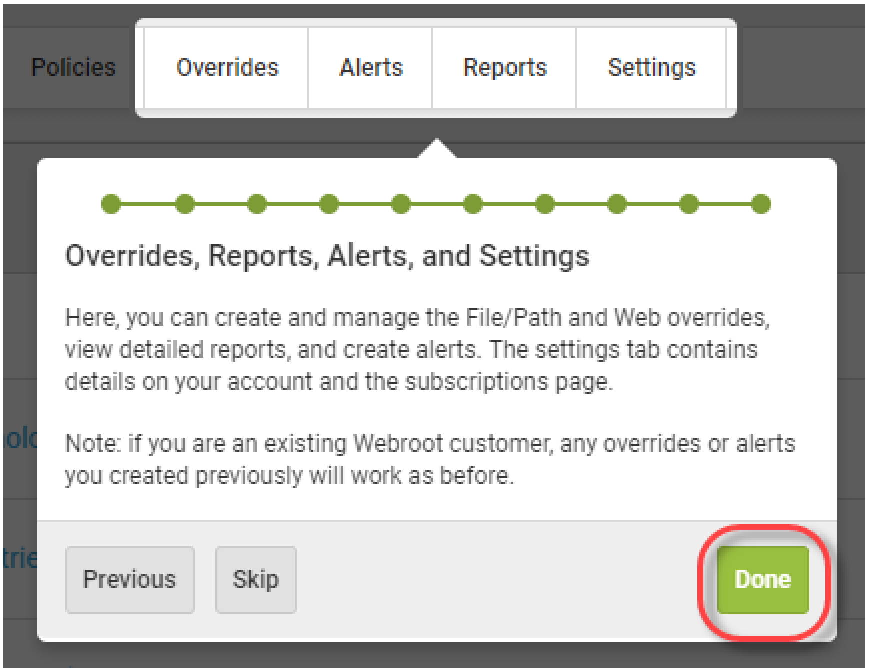
1. From the **Help (?)** drop-down menu, select **Spotlight Tour**.



The first window in the tour displays.

2. Click the **Skip** or **Next** button, as needed, until you're done viewing the tour.

3. When you're done viewing the tour, click the **Done** button.



Overrides, Reports, Alerts, and Settings

Here, you can create and manage the File/Path and Web overrides, view detailed reports, and create alerts. The settings tab contains details on your account and the subscriptions page.

Note: if you are an existing Webroot customer, any overrides or alerts you created previously will work as before.

As needed, to view the tour again, you can always select Spotlight Tour from the Help (?) drop-down menu.

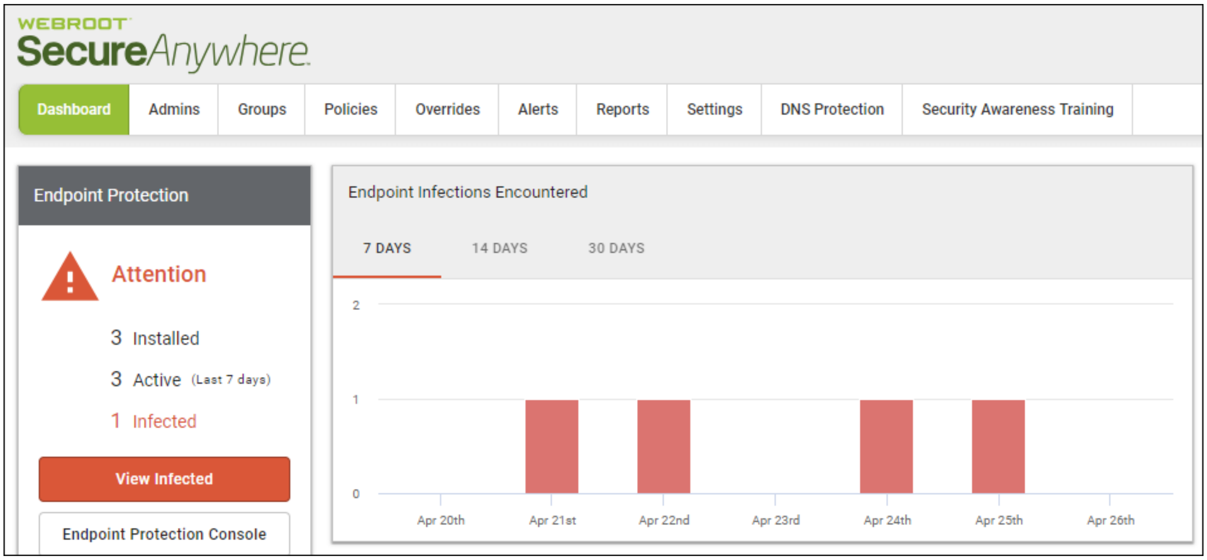
# Going to the Endpoint Console

Follow this procedure to go to the Endpoint console when you are in the management console.

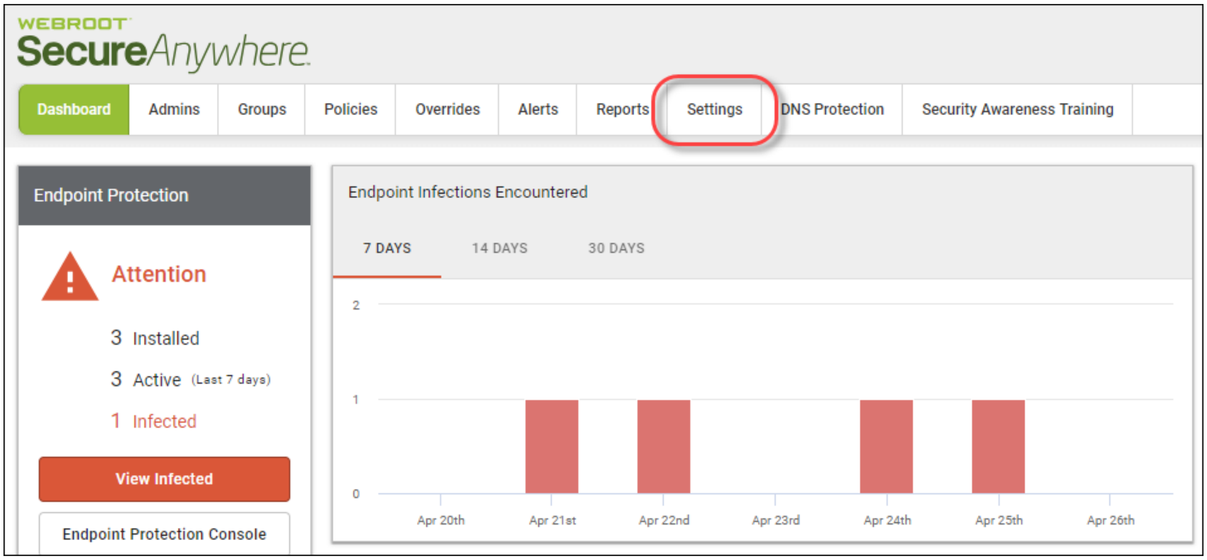
**To go to the Endpoint console:**

1. Log in to the management console.

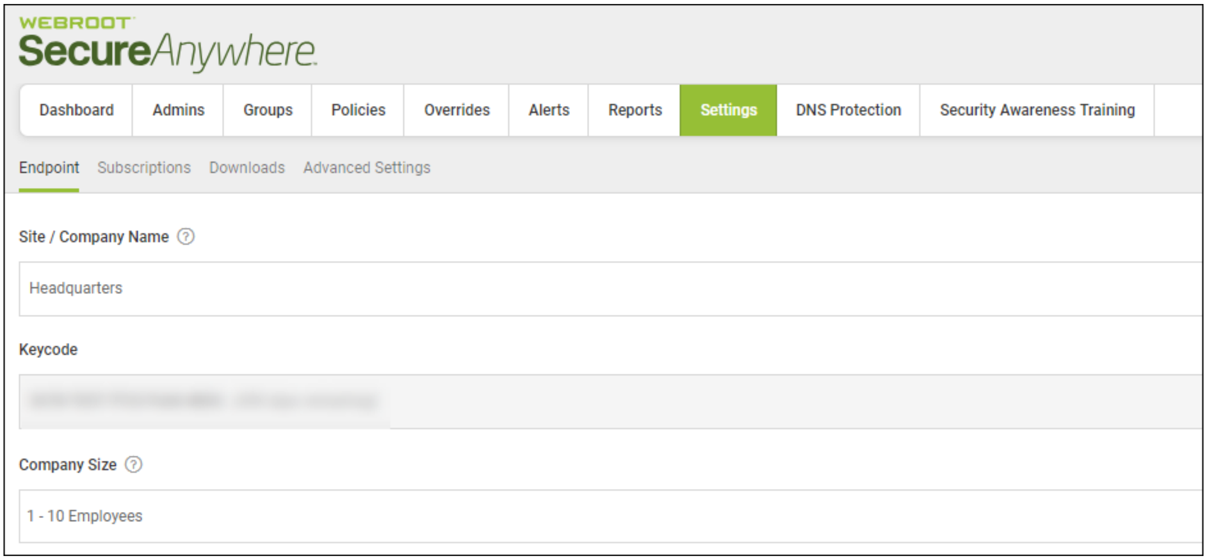
   The management console displays.



2. Click the **Settings** tab.



The Settings tab displays with the Endpoint tab active.



Site / Company Name

Headquarters

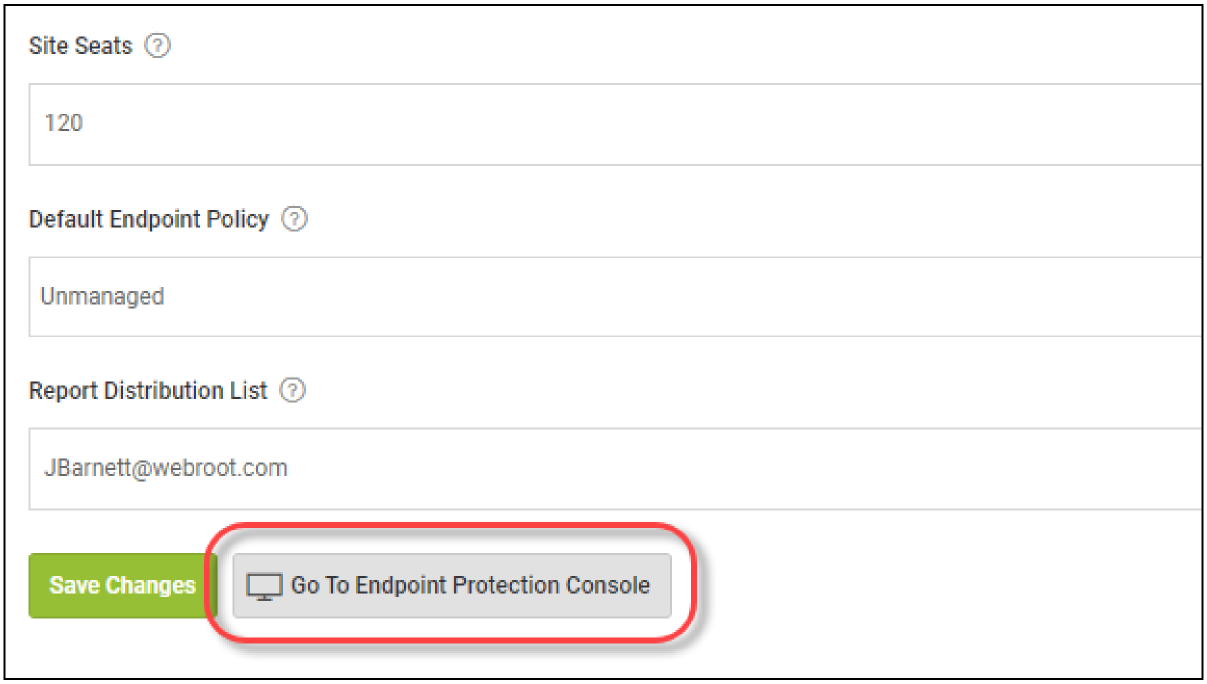
Keycode

[redacted]

Company Size

1 - 10 Employees

3. Scroll down and click the **Go To Endpoint Protection Console** button.



Site Seats

120

Default Endpoint Policy

Unmanaged

Report Distribution List

JBarnett@webroot.com

# Chapter 15: Global Site Manager 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