Copyright

Copyright 2020, Webroot. All rights reserved.

GSM Admin Guide

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Webroot.
# Table of Contents

## Chapter 1: Global Site Manager Admin Guide

- Creating Accounts ................................................................. 2
- Enabling two-factor authentication (2FA) .................................. 5
- Selecting Your Console .......................................................... 13
- About the Managed Service Provider Console .......................... 16
- About The Business Console .................................................. 19
- About the Spotlight Tour ....................................................... 22
- Communicating Through Firewalls ......................................... 24
- Enhanced Mobile Device Display ........................................... 26
- Changing Consoles ............................................................... 28
- Renaming Consoles .............................................................. 32
- Accessing the Endpoint Console ............................................ 36
- System Requirements ............................................................ 42

## Chapter 2: Working With Dashboards

- Creating Dashboard Charts .................................................... 44
- Editing Dashboard Charts ....................................................... 51
- Drilling Down in Dashboard Charts ........................................ 58
- Deleting Dashboard Charts ..................................................... 65

## Chapter 3: Working With Sites

- Management Console Sites Tab Overview ............................... 69
- Adding Sites ............................................................................ 73
- Filtering Sites ......................................................................... 81
- Searching for Sites .............................................................. 86
- Downloading CSV Files ......................................................... 88
- Sorting Sites ........................................................................... 90
- Viewing Site Summaries ........................................................ 92
  - Inside the Manage Button .................................................... 93
  - Summary Tab ........................................................................ 93
  - Details Tab .......................................................................... 94
  - Permissions Tab .................................................................... 94
  - Endpoint Protection Tab ..................................................... 95
  - DNS Protection Tab ........................................................... 95
  - Security Awareness Training Tab ...................................... 95
  - Downloads Tab ..................................................................... 95
- Viewing Multi-Site Summaries ................................................ 96
<table>
<thead>
<tr>
<th>Heading</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspending and Resuming Site Protection</td>
<td>108</td>
</tr>
<tr>
<td>Deactivating Site Protection</td>
<td>111</td>
</tr>
<tr>
<td>Editing Site Details</td>
<td>114</td>
</tr>
<tr>
<td>Tagging Sites</td>
<td>122</td>
</tr>
<tr>
<td>Updating Site Admin Permissions</td>
<td>132</td>
</tr>
<tr>
<td>Editing Site Settings</td>
<td>136</td>
</tr>
<tr>
<td>Setting Site-Level Data Filters</td>
<td>142</td>
</tr>
<tr>
<td>Downloading Webroot</td>
<td>149</td>
</tr>
<tr>
<td>Chapter 4: Working With Admins</td>
<td>153</td>
</tr>
<tr>
<td>Adding Admins</td>
<td>154</td>
</tr>
<tr>
<td>Updating Admin Information</td>
<td>160</td>
</tr>
<tr>
<td>Changing your account security settings</td>
<td>166</td>
</tr>
<tr>
<td>Deleting Admins</td>
<td>175</td>
</tr>
<tr>
<td>About Management Console Admin Permissions</td>
<td>179</td>
</tr>
<tr>
<td>Management Console Platform - Management Console Access</td>
<td>179</td>
</tr>
<tr>
<td>Management Console Platform - Endpoint Protection Console Access</td>
<td>181</td>
</tr>
<tr>
<td>SecureAnywhere Platform - Admin Level - Endpoint Protection</td>
<td>182</td>
</tr>
<tr>
<td>SecureAnywhere Platform - Basic Level - Endpoint Protection</td>
<td>183</td>
</tr>
<tr>
<td>SecureAnywhere Platform - No Access Level - Endpoint Protection</td>
<td>185</td>
</tr>
<tr>
<td>Chapter 5: Working With Groups</td>
<td>187</td>
</tr>
<tr>
<td>Adding Groups</td>
<td>188</td>
</tr>
<tr>
<td>Editing Groups</td>
<td>198</td>
</tr>
<tr>
<td>Deleting Groups</td>
<td>204</td>
</tr>
<tr>
<td>Chapter 6: Working With Devices</td>
<td>208</td>
</tr>
<tr>
<td>Device Management Overview</td>
<td>209</td>
</tr>
<tr>
<td>Groups Tab Filters</td>
<td>209</td>
</tr>
<tr>
<td>Groups Tab Columns</td>
<td>210</td>
</tr>
<tr>
<td>Groups Tab Page-Through Functionality</td>
<td>211</td>
</tr>
<tr>
<td>Editing Policies Applied To Devices</td>
<td>214</td>
</tr>
<tr>
<td>Adding Web Overrides to Devices</td>
<td>219</td>
</tr>
<tr>
<td>Whitelisting Files on Devices</td>
<td>224</td>
</tr>
<tr>
<td>Restoring Files From Quarantine</td>
<td>228</td>
</tr>
<tr>
<td>Viewing Protected Devices</td>
<td>233</td>
</tr>
<tr>
<td>Viewing Devices Not Seen Recently</td>
<td>236</td>
</tr>
<tr>
<td>Viewing Devices That Need Attention</td>
<td>239</td>
</tr>
<tr>
<td>Viewing Devices That Have Expired</td>
<td>245</td>
</tr>
<tr>
<td>Viewing Devices That Need Attention And Are Expired</td>
<td>248</td>
</tr>
</tbody>
</table>
Viewing Device Summaries ................................................................. 252
Status and Last Seen ........................................................................ 254
Summary Tab ..................................................................................... 255
Infections Encountered Tab ................................................................. 256
Blocked URLs Tab ............................................................................. 256
Scan History Tab ................................................................................ 257
Searching for Devices ........................................................................ 258
Filtering Devices By Site Names ......................................................... 261
Filtering Devices by Site Statuses ....................................................... 264
Filtering Devices Within Groups ....................................................... 267
Moving Devices Between Groups ....................................................... 270
Sorting Devices Within Groups ......................................................... 275
Displaying Scan Histories ................................................................. 277
Issuing Agent Commands ................................................................. 283
Viewing Agent Command Logs ......................................................... 288

Chapter 7: Working With Policies ......................................................... 295
Creating Policies ................................................................................ 296
Editing Policies .................................................................................. 302
  Basic Configuration Settings ........................................................... 311
  Scan Schedule ............................................................................... 315
  Scan Settings .............................................................................. 317
  Self Protection Settings ................................................................. 321
  Heuristics .................................................................................... 322
  Realtime Shield Settings ............................................................... 326
  Behavior Shield Settings ............................................................... 329
  Core System Shield ..................................................................... 330
  Web Threat Shield ..................................................................... 332
  Identity Shield ........................................................................... 335
  Firewall ...................................................................................... 338
  User Interface ............................................................................. 340
  System Optimizer ....................................................................... 341
  Evasion Shield Settings ............................................................... 350
Renaming Policies ............................................................................ 352
Copying Policies ............................................................................... 355
Importing Policies Manually ............................................................. 359
Deleting Policies ............................................................................... 364

Chapter 8: Working With Overrides ..................................................... 368
Chapter 1: Global Site Manager Admin Guide

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

Creating Accounts ................................................................. 2
Enabling two-factor authentication (2FA) .................................. 5
Selecting Your Console .......................................................... 13
About the Managed Service Provider Console ......................... 16
About The Business Console .................................................. 19
About the Spotlight Tour .......................................................... 22
Communicating Through Firewalls .......................................... 24
Enhanced Mobile Device Display ............................................. 26
Changing Consoles .................................................................. 28
Renaming Consoles ................................................................. 32
Accessing the Endpoint Console ................................................ 36
System Requirements ............................................................... 42
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.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webroot Product Keycode</td>
<td>Enter the license keycode you received when you purchased Endpoint Protection.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address for the administrator who will manage Endpoint Protection. The account activation confirmation is sent to this email address, which is also the username for logging in to the Management Portal.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a minimum of nine characters. Your password must contain at least six alphabetic characters and three numeric characters. It can include special characters, except for the angle brackets: &lt;&gt;. Your password is case sensitive. 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.</td>
</tr>
<tr>
<td>Your Personal Security Code</td>
<td>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. 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.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Question</td>
<td>Select a question from the drop-down list. If you forget details of your login later, you will need to provide the answer to this question to retrieve the information.</td>
</tr>
<tr>
<td>Security Answer</td>
<td>Type an answer to your security question. The Security Answer is case-sensitive.</td>
</tr>
</tbody>
</table>

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.

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.
3. Next, the **Setup 2FA** screen displays and will prompt you to pick two security questions and provide your answers, and then click **Continue**.
Chapter 1: Global Site Manager Admin Guide

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

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

Examples of mobile authentication apps include:

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- 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.
6. Enter the verification code from the authenticator app in the box under **Step 4**, and click **Verify Code**.
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](image)

**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.

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.

   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.

- 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.
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.
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

[SELECT] [SELECT]
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.

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, see 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](#).

![Support Link](image)

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

![Alert Bell](image)
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.

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.

<table>
<thead>
<tr>
<th>PATH</th>
<th>PORT</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.webrootcloudav.com</td>
<td>Port 443 (https)</td>
<td>Agent communication and updates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Some firewalls do not support double dotted subdomain names with a single wildcard mask, for example, g1.p4.webrootcloudav.com being represented by <em>.webrootcloudav.com, so some environments might require either <em>.p4.webrootcloudav.com or **.</em>.webrootcloudav.com.</em>*</td>
</tr>
<tr>
<td>*.webroot.com</td>
<td>Port 443 (https)</td>
<td>Agent messaging.</td>
</tr>
<tr>
<td>PATH</td>
<td>PORT</td>
<td>INFORMATION</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>WSAWebFilteringPortal.elasticbeanstalk.com</td>
<td>Port 80 (http) &amp; 443 (https)</td>
<td>Required for agent Web Filtering, elasticbeanstalk is an amazon AWS domain.</td>
</tr>
<tr>
<td>*.webrootanywhere.com</td>
<td>Port 80 (http) &amp; 443 (https)</td>
<td>Management portal and support ticket logs upload.</td>
</tr>
</tbody>
</table>
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.
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.
2. Select a console to open it.

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.
### Chapter 1: Global Site Manager Admin Guide

#### SecureAnywhere

![SecureAnywhere Dashboard](image)

### Sites

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Status</th>
<th>IMPEC</th>
<th>DNS Protection</th>
<th>Select Site Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cats Cheese</td>
<td>Protected</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Grand The Pet Emporium</td>
<td>Protected</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hammond Titus</td>
<td>Protected</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prestige Direct Sales Solutions</td>
<td>Protected</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **IMPEC**: Indicates if the site is protected.
- **DNS Protection**: Indicates if the DNS protection is enabled.
- **Select Site Training**: Indicates if the site training is selected.
Renaming Consoles

Follow this procedure to rename consoles.

To rename a console:

1. Log in to the management console.

The Console Selection screen displays.
2. Select a console to open it.

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

5. Click the Save button.

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.

2. Click the Manage button for the site you want to access the Endpoint console for.
   
The Manage Sites panel displays, with the Summary tab active.
3. Click the **Endpoint Protection** tab.

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

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 ................................................................. 44
Editing Dashboard Charts ................................................................. 51
Drilling Down in Dashboard Charts ....................................................... 58
Deleting Dashboard Charts ................................................................. 65
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.
   
The management console displays with the Sites tab active.

2. From the main menu, click the Dashboard tab.
   
The Dashboard tab displays.
3. Click the **Add chart** button.

The Add chart window displays.
4. From the Chart Data Field drop-down menu, select any of the following options:

<table>
<thead>
<tr>
<th>Agent Version Spread</th>
<th>Firewall Status</th>
<th>Operating System Language</th>
<th>Rootkit Shield Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attention Required</td>
<td>Identity Shield Status</td>
<td>Operating System Platform</td>
<td>Scheduled Scans Status</td>
</tr>
<tr>
<td>Device Activations</td>
<td>Infrared Status</td>
<td>Phishing Shield Status</td>
<td>Silent Mode</td>
</tr>
<tr>
<td>Device Type</td>
<td>Installation Status</td>
<td>Primary Browser</td>
<td>Threat Detection History</td>
</tr>
<tr>
<td>Endpoint Status</td>
<td>Managed by Policy</td>
<td>Realtime Shield Status</td>
<td>USB Shield Status</td>
</tr>
<tr>
<td>Expired Status</td>
<td>Offline Shield Status</td>
<td>Remediation Status</td>
<td>Web Threat Shield Status</td>
</tr>
</tbody>
</table>

**Note:** The following data points are unsupported in the Mac agent: Firewall Status, Rootkit Shield Status, Infrared 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.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar</td>
<td><img src="image1.png" alt="Bar Chart" /></td>
</tr>
<tr>
<td>Bar Stacked</td>
<td><img src="image2.png" alt="Bar Stacked Chart" /></td>
</tr>
<tr>
<td>NAME</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Column**

![Column Chart]

**Column Stacked**

![Column Stacked Chart]
### Table 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
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:

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 hours</td>
<td>2 days</td>
</tr>
<tr>
<td>14 days</td>
<td>30 days</td>
</tr>
<tr>
<td></td>
<td>60 days</td>
</tr>
<tr>
<td></td>
<td>90 days</td>
</tr>
</tbody>
</table>

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

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.

2. Click the Dashboard tab.

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

<table>
<thead>
<tr>
<th>Agent Version Spread</th>
<th>Firewall Status</th>
<th>Operating System Language</th>
<th>Rootkit Shield Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attention Required</td>
<td>Identity Shield Status</td>
<td>Operating System Platform</td>
<td>Scheduled Scans Status</td>
</tr>
<tr>
<td>Device Activations</td>
<td>Infrared Status</td>
<td>Phishing Shield Status</td>
<td>Silent Mode</td>
</tr>
<tr>
<td>Device Type</td>
<td>Installation Status</td>
<td>Primary Browser</td>
<td>Threat Detection History</td>
</tr>
<tr>
<td>Endpoint Status</td>
<td>Managed by Policy</td>
<td>Realtime Shield Status</td>
<td>USB Shield Status</td>
</tr>
<tr>
<td>Expired Status</td>
<td>Offline Shield Status</td>
<td>Remediation Status</td>
<td>Web Threat Shield Status</td>
</tr>
</tbody>
</table>

**Note:** The following data points are unsupported in the Mac agent: Firewall Status, Rootkit Shield Status, Infrared 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.
<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar</td>
<td><img src="image1" alt="Agent Version Spread" /></td>
</tr>
<tr>
<td>Bar Stacked</td>
<td><img src="image2" alt="Agent Version Spread" /></td>
</tr>
<tr>
<td>NAME</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Column</td>
<td><img src="image1.png" alt="Column Chart" /></td>
</tr>
<tr>
<td>Column Stacked</td>
<td><img src="image2.png" alt="Stacked Column Chart" /></td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 hours</td>
</tr>
<tr>
<td>2 days</td>
</tr>
<tr>
<td>3 days</td>
</tr>
<tr>
<td>7 days</td>
</tr>
<tr>
<td>14 days</td>
</tr>
<tr>
<td>30 days</td>
</tr>
<tr>
<td>60 days</td>
</tr>
<tr>
<td>90 days</td>
</tr>
</tbody>
</table>

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

**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.

2. Click the Dashboard tab.

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

The drill-down expands to include information about the host name and the keycode associated with each endpoint.
5. In the Hostname column, click on the host name to display in-depth information about the host.

The Endpoint Information window displays information about the following:

- Endpoint
- Webroot SecureAnywhere
- Scan Information
- Shields
<table>
<thead>
<tr>
<th>Endpoint Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint</strong></td>
<td>Webroot SecureAnywhere</td>
</tr>
<tr>
<td>Hostname</td>
<td>DESKTOP-RQC3NE0</td>
</tr>
<tr>
<td>Current User</td>
<td>QA</td>
</tr>
<tr>
<td>Device Type</td>
<td>PC</td>
</tr>
<tr>
<td>Primary Browser</td>
<td>IE</td>
</tr>
<tr>
<td>Primary Browser Version</td>
<td>9.11.10240.16384</td>
</tr>
<tr>
<td>Operating System Firewall Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>No</td>
</tr>
<tr>
<td>Internal IP</td>
<td>10.0.2.15</td>
</tr>
<tr>
<td>MAC Address</td>
<td>08:00:27:B3:4C:D3</td>
</tr>
</tbody>
</table>

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

2. Click the **Dashboard** tab.
   
The Dashboard tab displays.
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.

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 ................................................................. 69
- Adding Sites .................................................................................................................. 73
- Filtering Sites ............................................................................................................... 81
- Searching for Sites ..................................................................................................... 86
- Downloading CSV Files ........................................................................................... 88
- Sorting Sites ................................................................................................................ 90
- Viewing Site Summaries ............................................................................................ 92
  - Inside the Manage Button ....................................................................................... 93
  - Summary Tab ........................................................................................................... 93
  - Details Tab ............................................................................................................... 94
  - Permissions Tab ...................................................................................................... 94
  - Endpoint Protection Tab ......................................................................................... 95
  - DNS Protection Tab ............................................................................................... 95
  - Security Awareness Training Tab ......................................................................... 95
  - Downloads Tab ....................................................................................................... 95
- Viewing Multi-Site Summaries .................................................................................... 96
- Suspending and Resuming Site Protection ............................................................... 108
- Deactivating Site Protection ..................................................................................... 111
- Editing Site Details .................................................................................................. 114
- Tagging Sites ............................................................................................................ 122
- Updating Site Admin Permissions .......................................................................... 132
- Editing Site Settings ................................................................................................. 136
- Setting Site-Level Data Filters ................................................................................. 142
- Downloading Webroot ............................................................................................. 149
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.

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** — Lets you download CSV files. For more information, see *Downloading CSV Files on page 88*.
• **Filters Button** — Lets you choose 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.

![Console Screen](image)

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.

![Table of Sites](image)

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*

![Site Management Interface](image)

**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.

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

   The Add Site panel displays with the Details area active.
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.

The system displays the Permissions area.
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.

The system displays the Endpoint Protection area.
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.

![Image](image1.png)

The system displays the DNS Protection area.

![Image](image2.png)

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.

![Image of SecureAnywhere interface]

The system displays the Security Awareness Training area.

![Image of SecureAnywhere interface with Security Awareness Training enabled]

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 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.
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.

2. Click the **Filters** button.

   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.

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select any or all of the following statuses:</td>
</tr>
<tr>
<td></td>
<td>• Protected</td>
</tr>
<tr>
<td></td>
<td>• Needs Attention</td>
</tr>
<tr>
<td></td>
<td>• Expiring</td>
</tr>
<tr>
<td></td>
<td>• Expired</td>
</tr>
<tr>
<td></td>
<td>• Suspended</td>
</tr>
<tr>
<td></td>
<td>• Deactivated</td>
</tr>
<tr>
<td>Keycode Type</td>
<td>Select either or both of the following keycode types:</td>
</tr>
<tr>
<td></td>
<td>• Full</td>
</tr>
<tr>
<td></td>
<td>• Trial</td>
</tr>
<tr>
<td>Site Seats</td>
<td>Select any or all of the following number of seats:</td>
</tr>
<tr>
<td></td>
<td>• Less than 50</td>
</tr>
<tr>
<td></td>
<td>• 50 - 100</td>
</tr>
<tr>
<td></td>
<td>• 101 - 250</td>
</tr>
<tr>
<td></td>
<td>• 251 - 500</td>
</tr>
<tr>
<td></td>
<td>• More than 500</td>
</tr>
<tr>
<td>BUTTON</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Active Devices</strong></td>
<td>Select any or all of the following number of seats:</td>
</tr>
<tr>
<td></td>
<td>• Less than 50</td>
</tr>
<tr>
<td></td>
<td>• 50 - 100</td>
</tr>
<tr>
<td></td>
<td>• 101 - 250</td>
</tr>
<tr>
<td></td>
<td>• 251 - 500</td>
</tr>
<tr>
<td></td>
<td>• More than 500</td>
</tr>
<tr>
<td><strong>Billing Cycle</strong></td>
<td>Select any or all of the following billing cycles:</td>
</tr>
<tr>
<td></td>
<td>• Annually</td>
</tr>
<tr>
<td></td>
<td>• Quarterly</td>
</tr>
<tr>
<td></td>
<td>• Monthly</td>
</tr>
<tr>
<td></td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Not applicable</td>
</tr>
<tr>
<td><strong>Created By</strong></td>
<td>Select any email address of the person who created that site.</td>
</tr>
<tr>
<td></td>
<td>If there are more than six email addresses, there is a scroll bar to the right of the list.</td>
</tr>
<tr>
<td><strong>Tags</strong></td>
<td>Select any tags that have been created and applied to a site.</td>
</tr>
<tr>
<td></td>
<td>If there are more than six email addresses, there is a scroll bar to the right of the list.</td>
</tr>
</tbody>
</table>
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.

   ![Management Console with Sites Tab Active]

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

   ![Search Field in Management Console]

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

![Management Console](image)

2. Click the [Download](#) icon.

   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
Chapter 3: Working With Sites

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

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.
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.

   ![Management Console with Sites Tab Active]

2. Click the Manage button.

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

   ![Manage Sites Panel with 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 trial 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 trial 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.

2. Click the Dashboard tab.

   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.
In the upper left corner is a Dashboard Summary bar, which gives you an overview of all of your sites.
3. To view additional site information, hover over the word **Sites**.

The system displays a site overview.
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 Realtime shield 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.
The system displays the Site Filter window.

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.

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

The Hostname and Keycode information display.
11. In the Hostname column, click the link to drill further down.

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.
### Endpoint Information

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Webroot SecureAnywhere</th>
<th>Scan Information</th>
<th>Shields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname</strong></td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>Current User</strong></td>
<td>cwilliams</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>Device Type</strong></td>
<td>PC</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>Primary Browser</strong></td>
<td>IE</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>Primary Browser Version</strong></td>
<td>9.11.10666.0</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>Operating System Firewall Enabled</strong></td>
<td>Yes</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>Virtual Machine</strong></td>
<td>No</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>Internal IP</strong></td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
</tbody>
</table>

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

![Endpoint information table]

<table>
<thead>
<tr>
<th>Endpoint Information</th>
<th>Hostname</th>
<th>Current User</th>
<th>Device Type</th>
<th>Primary Browser</th>
<th>Primary Browser Version</th>
<th>Operating System Firewall Enabled</th>
<th>Virtual Machine</th>
<th>Internal IP</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webroot SecureAnywhere</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Endpoint information table]

**Close** button highlighted on the bottom right.
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.

   ![Management Console](image1)

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

   ![Manage Button](image2)

   The Manage Sites panel displays, with the Summary tab active.
3. Scroll down the page and click the **Suspend Protection** button to suspend protection for that site.

The system displays a Suspend Protection warning message.
4. Click the Yes button to continue with suspending protection.

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

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.

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

   The Manage Sites panel displays, with the Summary tab active.
3. Scroll down and click the **Deactivate** button.

The system deactivates the site, and displays a Deactivate warning message.
4. Click the **Yes** button to continue.

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.

   ![Management Console](image1)

2. Click the Manage button.

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

   ![Manage Sites Panel](image2)
3. Click the **Details** tab.
The Details tab displays.
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*. 

- 118 -
13. When you're done, click the **Save Changes** button, which is located at the bottom of the tab.
<table>
<thead>
<tr>
<th>Site / Company Name</th>
<th>Haymont Tires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keycode</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Site Type</td>
<td>External Company</td>
</tr>
<tr>
<td>Company Size</td>
<td>11 - 100 Employees</td>
</tr>
<tr>
<td>Company Industry</td>
<td>Other</td>
</tr>
<tr>
<td>Billing Cycle</td>
<td>Annually</td>
</tr>
<tr>
<td>Billing Date</td>
<td>Jan 1st</td>
</tr>
<tr>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>Created By</td>
<td>Craig Pappo</td>
</tr>
<tr>
<td>Tags</td>
<td>Add Tag...</td>
</tr>
</tbody>
</table>

Save Changes
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.

   ![Management Console with Sites Tab Active](image1)

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

   ![Manage Sites Panel with Summary Tab Active](image2)

   The Manage Sites panel displays with the Summary tab active.
3. Click the **Details** tab.

The Details tab displays.
Chapter 3: Working With Sites

### 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
- Blank

### Created By
- Craig Papke

### Tags
- Add Tag... Add
4. In the Tags field, 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.

**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.
6. To remove a tag, click the X to the left of each tag.
7. When you're done, click the **Save Changes** button.

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.

2. Click the Manage button.

   The Manage Sites panel displays, with the Summary tab active.
3. Click the **Permissions** tab.

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.

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.

2. Click the Manage button.

   The Manage Sites panel displays, with the Summary tab active.
3. Click the **Endpoint Protection** tab.

The Endpoint Protection tab displays.
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 policies 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.
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.

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

   The Manage Sites panel displays, with the Summary tab active.
3. Click the **Endpoint Protection** tab.

The Endpoint Protection tab displays.
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

**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.

The system updates the setting.
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.

   ![Management Console with Sites Tab Active]

2. Click the Manage button.

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

   ![Manage Sites Panel with Summary Tab Active]
3. Click the **Downloads** button.

The Downloads tab displays.
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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding Admins</td>
<td>154</td>
</tr>
<tr>
<td>Updating Admin Information</td>
<td>160</td>
</tr>
<tr>
<td>Changing your account security settings</td>
<td>166</td>
</tr>
<tr>
<td>Deleting Admins</td>
<td>175</td>
</tr>
<tr>
<td>About Management Console Admin Permissions</td>
<td>179</td>
</tr>
<tr>
<td>Management Console Platform - Management Console Access</td>
<td>179</td>
</tr>
<tr>
<td>Management Console Platform - Endpoint Protection Console Access</td>
<td>181</td>
</tr>
<tr>
<td>SecureAnywhere Platform - Admin Level - Endpoint Protection</td>
<td>182</td>
</tr>
<tr>
<td>SecureAnywhere Platform - Basic Level - Endpoint Protection</td>
<td>183</td>
</tr>
<tr>
<td>SecureAnywhere Platform - No Access Level - Endpoint Protection</td>
<td>185</td>
</tr>
</tbody>
</table>
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.

   ![Management Console with Sites Tab]

2. Click the Admins tab.

   The system displays the Admins tab.

   ![Management Console with Admins Tab]
3. Click the **Add** button.

The system displays the Create Admin window.
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.
The system displays the Site Permissions tab.

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.
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.

2. Click the Admins tab.

   The system displays the Admins panel with the following information:
- Name — The name of the admin.
- Email — The email address of the admin.

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

The system displays admin information with the Details tab active.
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.
- Chapter 4: Working With Admins -

- **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.
The system displays the Site Permissions tab.
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.

---

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.

![Management Console screenshot]
3. Enter your current password, a new password, and then click Change 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.
3. The Disable 2FA screen displays, and you will need to enter your Email / Phone and your Password, and then click **Continue**.

![Disable 2FA screen](image)

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

![Authentication Code screen](image)
5. Click **Disable 2FA**.

![Disable 2FA](image)

**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.

![Email](image)

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

![Change Security Code](image)

**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.
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**.
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.

2. Click the Admins tab.

   The system displays the Admins tab.
3. Double-click an admin's email address 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.

5. Click the Confirm Delete button.

The system displays an information message.
6. Click the **OK** button.

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

<table>
<thead>
<tr>
<th>Super Admin</th>
<th>Limited Admin</th>
<th>Site Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard - Yes</td>
<td>Dashboard - Yes</td>
<td>Dashboard - No Access</td>
</tr>
<tr>
<td>Sites Page - Yes*</td>
<td>Sites Page - Yes*</td>
<td>Sites Page - No Access</td>
</tr>
<tr>
<td>Admins - Yes</td>
<td>Admins - View Only</td>
<td>Admins - No Access</td>
</tr>
<tr>
<td>Groups - Yes</td>
<td>Groups - Yes</td>
<td>Groups - No Access</td>
</tr>
<tr>
<td>Policies - Yes</td>
<td>Policies - No</td>
<td>Policies - No Access</td>
</tr>
<tr>
<td>Super Admin</td>
<td>Limited Admin</td>
<td>Site Only</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Overrides - Yes</td>
<td>Overrides - No</td>
<td>Overrides - No Access</td>
</tr>
<tr>
<td>Alerts - Yes</td>
<td>Alerts - No</td>
<td>Alerts - No Access</td>
</tr>
<tr>
<td>Commands - N/A</td>
<td>Commands - N/A</td>
<td>Commands - No Access</td>
</tr>
<tr>
<td>Reports - Yes</td>
<td>Reports - Yes</td>
<td>Reports - No Access</td>
</tr>
<tr>
<td>DNS - Yes</td>
<td>DNS - Yes</td>
<td>DNS - No</td>
</tr>
<tr>
<td>WSAT - Yes</td>
<td>WSAT - Yes</td>
<td>WSAT - Yes</td>
</tr>
<tr>
<td>Settings - Yes</td>
<td>Settings - No</td>
<td>Settings - No Access</td>
</tr>
<tr>
<td>Logs - N/A</td>
<td>Logs - N/A</td>
<td>Logs - No Access</td>
</tr>
<tr>
<td>Resources - N/A</td>
<td>Resources - N/A</td>
<td>Resources - No Access</td>
</tr>
<tr>
<td>Downloads - Yes</td>
<td>Downloads - Yes</td>
<td>Downloads - No Access</td>
</tr>
</tbody>
</table>
## Management Console Platform - Endpoint Protection Console

### Access

<table>
<thead>
<tr>
<th>Super Admin</th>
<th>Limited Admin</th>
<th>Site Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard - Yes</td>
<td>Dashboard - Yes</td>
<td>Dashboard - Yes</td>
</tr>
<tr>
<td>Sites Page - Yes*</td>
<td>Sites Page - Yes*</td>
<td>Sites Page - N/A</td>
</tr>
<tr>
<td>Admins - Yes</td>
<td>Admins - Yes</td>
<td>Admins - Yes</td>
</tr>
<tr>
<td>Groups - Yes*</td>
<td>Groups - Yes*</td>
<td>Groups - Yes*</td>
</tr>
<tr>
<td>Policies - Yes*</td>
<td>Policies - Yes*</td>
<td>Policies - Yes*</td>
</tr>
<tr>
<td>Overrides - Yes*</td>
<td>Overrides - Yes*</td>
<td>Overrides - Yes*</td>
</tr>
<tr>
<td>Alerts - Yes*</td>
<td>Alerts - Yes*</td>
<td>Alerts - Yes*</td>
</tr>
<tr>
<td>Commands - Yes*</td>
<td>Commands - Yes*</td>
<td>Commands - Yes*</td>
</tr>
<tr>
<td>Reports - Yes</td>
<td>Reports - Yes</td>
<td>Reports - Yes</td>
</tr>
<tr>
<td>DNS - No</td>
<td>DNS - No</td>
<td>DNS - No</td>
</tr>
<tr>
<td>WSAT - Yes</td>
<td>WSAT - Yes</td>
<td>WSAT - Yes</td>
</tr>
<tr>
<td>Settings - Yes</td>
<td>Settings - Yes</td>
<td>Settings - Yes</td>
</tr>
</tbody>
</table>
### Super Admin

<table>
<thead>
<tr>
<th>Logs</th>
<th>Logs</th>
<th>Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>Resources</td>
<td>Resources</td>
</tr>
<tr>
<td>Downloads</td>
<td>Downloads</td>
<td>Downloads</td>
</tr>
</tbody>
</table>

### Limited Admin

<table>
<thead>
<tr>
<th>Logs</th>
<th>Logs</th>
<th>Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>Resources</td>
<td>Resources</td>
</tr>
<tr>
<td>Downloads</td>
<td>Downloads</td>
<td>Downloads</td>
</tr>
</tbody>
</table>

### Site Only

<table>
<thead>
<tr>
<th>Logs</th>
<th>Logs</th>
<th>Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>Resources</td>
<td>Resources</td>
</tr>
<tr>
<td>Downloads</td>
<td>Downloads</td>
<td>Downloads</td>
</tr>
</tbody>
</table>

### SecureAnywhere Platform - Admin Level - Endpoint Protection

<table>
<thead>
<tr>
<th>Admin</th>
<th>Basic</th>
<th>No Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status</td>
<td>Status</td>
</tr>
<tr>
<td>Admins</td>
<td>Admins</td>
<td>Admins</td>
</tr>
<tr>
<td>Groups</td>
<td>Groups - View Only</td>
<td>Groups - No</td>
</tr>
<tr>
<td>Policies</td>
<td>Policies - View Only</td>
<td>Policies - No</td>
</tr>
<tr>
<td>Overrides</td>
<td>Overrides - No</td>
<td>Overrides - No</td>
</tr>
<tr>
<td>Alerts</td>
<td>Alerts - No</td>
<td>Alerts - No</td>
</tr>
<tr>
<td>Commands</td>
<td>Commands - No</td>
<td>Commands - No</td>
</tr>
<tr>
<td>Reports</td>
<td>Reports - Yes</td>
<td>Reports - No</td>
</tr>
</tbody>
</table>
### Admin

<table>
<thead>
<tr>
<th>Feature</th>
<th>Basic</th>
<th>No Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>WSAT</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Settings</td>
<td>Yes</td>
<td>View Only</td>
</tr>
<tr>
<td>Logs</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resources</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Downloads</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### SecureAnywhere Platform - Basic Level - Endpoint Protection

<table>
<thead>
<tr>
<th>Feature</th>
<th>Basic</th>
<th>No Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Admins</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Groups</td>
<td>Yes*</td>
<td>View Only</td>
</tr>
<tr>
<td>Policies</td>
<td>Yes*</td>
<td>View Only</td>
</tr>
<tr>
<td>Overrides</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>Admin</td>
<td>Basic</td>
<td>No Access</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Alerts - Yes*</td>
<td>Alerts - No</td>
<td>Alerts - No</td>
</tr>
<tr>
<td>Commands - Yes*</td>
<td>Commands - No</td>
<td>Commands - No</td>
</tr>
<tr>
<td>Reports - Yes</td>
<td>Reports - Yes</td>
<td>Reports - No</td>
</tr>
<tr>
<td>DNS - No</td>
<td>DNS - No</td>
<td>DNS - No</td>
</tr>
<tr>
<td>WSAT - Yes</td>
<td>WSAT - No</td>
<td>WSAT - No</td>
</tr>
<tr>
<td>Settings - Yes</td>
<td>Settings - View Only</td>
<td>Settings - No</td>
</tr>
<tr>
<td>Logs - Yes</td>
<td>Logs - Yes</td>
<td>Logs - No</td>
</tr>
<tr>
<td>Resources - Yes</td>
<td>Resources - Yes</td>
<td>Resources - No</td>
</tr>
<tr>
<td>Downloads - Yes</td>
<td>Downloads - Yes</td>
<td>Downloads - No</td>
</tr>
</tbody>
</table>
## SecureAnywhere Platform - No Access Level - Endpoint Protection

<table>
<thead>
<tr>
<th>Admin</th>
<th>Basic</th>
<th>No Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status - No</td>
<td>Status - No</td>
<td>Status - No</td>
</tr>
<tr>
<td>Admins - No</td>
<td>Admins - No</td>
<td>Admins - No</td>
</tr>
<tr>
<td>Groups - No</td>
<td>Groups - No</td>
<td>Groups - No</td>
</tr>
<tr>
<td>Policies - No</td>
<td>Policies - No</td>
<td>Policies - No</td>
</tr>
<tr>
<td>Overrides - No</td>
<td>Overrides - No</td>
<td>Overrides - No</td>
</tr>
<tr>
<td>Alerts - No</td>
<td>Alerts - No</td>
<td>Alerts - No</td>
</tr>
<tr>
<td>Commands - No</td>
<td>Commands - No</td>
<td>Commands - No</td>
</tr>
<tr>
<td>Reports - No</td>
<td>Reports - No</td>
<td>Reports - No</td>
</tr>
<tr>
<td>DNS - No</td>
<td>DNS - No</td>
<td>DNS - No</td>
</tr>
<tr>
<td>WSAT - No</td>
<td>WSAT - No</td>
<td>WSAT - No</td>
</tr>
<tr>
<td>Settings - No</td>
<td>Settings - No</td>
<td>Settings - No</td>
</tr>
<tr>
<td>Logs - No</td>
<td>Logs - No</td>
<td>Logs - No</td>
</tr>
<tr>
<td>Admin</td>
<td>Basic</td>
<td>No Access</td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Resources - No</td>
<td>Resources - No</td>
<td>Resources - No</td>
</tr>
<tr>
<td>Downloads - No</td>
<td>Downloads - No</td>
<td>Downloads - No</td>
</tr>
</tbody>
</table>
Chapter 5: Working With Groups

To work with groups, see the following topics:

- Adding Groups ................................................................. 188
- Editing Groups ................................................................. 198
- Deleting Groups ............................................................... 204
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.

2. Click the Groups tab.

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

The Plus (+) button becomes active.
4. Click the **Plus (+)** button.

![Image of the Create Group window](image)

The Create Group window displays.

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
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.
11. Click the **Move** button.

The **Move Group** window displays.
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.

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.

2. Click the Groups tab.
   
The Groups tab displays.
3. In the left column, select a site that contains a group you want to edit.

The Edit button becomes active.
4. Click the **Edit** button.

The Edit Group window displays.
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.
9. When you're done, click the **Save** button.

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.

2. Click the Groups tab.

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

The Minus (-) button becomes active.
4. Click the **Minus (-)** button.

The **Delete Group** window displays.

---

*GSM Admin Guide*
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 Window]

   The group is deleted.
Chapter 6: Working With Devices

To work with devices, see the following topics:

- **Device Management Overview**: 209
- **Groups Tab Filters**: 209
- **Groups Tab Columns**: 210
- **Groups Tab Page-Through Functionality**: 211
- **Editing Policies Applied To Devices**: 214
- **Adding Web Overrides to Devices**: 219
- **Whitelisting Files on Devices**: 224
- **Restoring Files From Quarantine**: 228
- **Viewing Protected Devices**: 233
- **Viewing Devices Not Seen Recently**: 236
- **Viewing Devices That Need Attention**: 239
- **Viewing Devices That Have Expired**: 245
- **Viewing Devices That Need Attention And Are Expired**: 248
- **Viewing Device Summaries**: 252
  - **Status and Last Seen**: 254
  - **Summary Tab**: 255
  - **Infections Encountered Tab**: 256
  - **Blocked URLs Tab**: 256
  - **Scan History Tab**: 257
- **Searching for Devices**: 258
- **Filtering Devices By Site Names**: 261
- **Filtering Devices by Site Statuses**: 264
- **Filtering Devices Within Groups**: 267
- **Moving Devices Between Groups**: 270
- **Sorting Devices Within Groups**: 275
- **Displaying Scan Histories**: 277
- **Issuing Agent Commands**: 283
- **Viewing Agent Command Logs**: 288
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.

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
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.

<table>
<thead>
<tr>
<th>DEVICE ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Indicates that the device is a Windows PC.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Indicates that the device is a Windows server.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Indicates that the device is an Apple Mac.</td>
</tr>
</tbody>
</table>
**Status** — Displays the current status of the device, as described in the following table:

<table>
<thead>
<tr>
<th>STATUS ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅ Protected</td>
<td>Protected — Indicates that the device is protected</td>
</tr>
<tr>
<td>⚠ Needs Attention</td>
<td>Needs Attention — Indicates that the device needs attention.</td>
</tr>
<tr>
<td>⚠ Expired</td>
<td>Expired — Indicates that the device license has expired and is no longer being protected by Webroot SecureAnywhere.</td>
</tr>
<tr>
<td>⚠ Attention &amp; Expired</td>
<td>Attention &amp; Expired — Indicates that as well as needing attention, the device license has expired and is no longer being protected by Webroot SecureAnywhere.</td>
</tr>
<tr>
<td>⚠ Not Seen Recently</td>
<td>Not Seen Recently — Indicates that the device has not checked in recently.</td>
</tr>
</tbody>
</table>

**Groups Tab Page-Through Functionality**

The bottom of the Devices tab has the page-through functionality, as described in the following table.
<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Double Left Arrow" /> <img src="image" alt="Left Arrow" /></td>
<td>Click the <strong>Double Left</strong> arrow to go to the first page in the list.</td>
</tr>
<tr>
<td><img src="image" alt="Left Arrow" /> <img src="image" alt="2" /> <img src="image" alt="Right Arrow" /></td>
<td>Click the <strong>Left</strong> arrow to go to the previous page in the list.</td>
</tr>
<tr>
<td><img src="image" alt="Left Arrow" /> <img src="image" alt="2" /> <img src="image" alt="Up Arrow" /></td>
<td>Indicates which page in the list displays.</td>
</tr>
<tr>
<td><img src="image" alt="Left Arrow" /> <img src="image" alt="2" /> <img src="image" alt="Right Arrow" /></td>
<td>Click the <strong>Right</strong> arrow to go to the next page in the list. From the drop-down menu, select any page in the list to go directly to that page.</td>
</tr>
<tr>
<td><img src="image" alt="Double Right Arrow" /> <img src="image" alt="Left Arrow" /> <img src="image" alt="2" /> <img src="image" alt="Right Arrow" /></td>
<td>Click the <strong>Double Right</strong> arrow to go to the last page in the list.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh Icon" /></td>
<td>Click the Refresh icon to refresh the information on the page.</td>
</tr>
</tbody>
</table>
## FUNCTION

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates how many rows display on a page. From the drop-down menu, you can select any of the following increments:</td>
</tr>
<tr>
<td>- 50</td>
</tr>
<tr>
<td>- 100</td>
</tr>
<tr>
<td>- 200</td>
</tr>
<tr>
<td>- 500</td>
</tr>
</tbody>
</table>

Gives a numerical indicator as to which page out of how many pages in the list that displays.

---

![Image of the interface displaying rows and page information](image)
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.

2. Click the Groups tab.
   
   The Groups tab displays.
3. In the left column, select the site that contains the group and device you want to edit the policy for.

![Image of a web interface showing a list of sites and devices]

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

![Image of a web interface showing a list of devices]

To select all devices, select the checkbox at the top of the column.
5. Click the Edit Policy button.

The Edit Policy window displays.

![Edit Policy Window](image)

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.

2. Click the Groups tab.

   The Groups tab displays.
3. Select the device that has blocked URLs that you want to override.

The Status Panel for the device you selected displays.
4. Click the **Blocked URLs** tab.

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.

![Blocked URLs Tab](#)

<table>
<thead>
<tr>
<th>URL</th>
<th>Category</th>
<th>Reputation</th>
<th>User Action</th>
<th>Date</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://free.freedoctopdf.com">http://free.freedoctopdf.com</a></td>
<td>Spyware and Adware</td>
<td>High Risk</td>
<td>Block</td>
<td>Mon 4 2018, 01:17</td>
<td></td>
</tr>
</tbody>
</table>

**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.

The Create New Entry window displays.

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.

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.

2. Click the Groups tab.

   The Groups tab displays.
3. Select the device that has blocked URLs that you want to override.

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

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

2. Click the Groups tab.

   The Groups tab displays.
3. Select the device that has blocked URLs that you want to override.

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

![Image of Webroot SecureAnywhere interface showing infections encountered]

<table>
<thead>
<tr>
<th>Filename</th>
<th>Pathname</th>
<th>Malware Group</th>
<th>Last Seen</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM_DELETE.AEXE</td>
<td>%cache%</td>
<td>902:Rogue Gen</td>
<td>Feb 27th 2018, 15:16</td>
<td></td>
</tr>
<tr>
<td>AM_DELETE.AEXE</td>
<td>%cache%</td>
<td>902:Rogue Gen</td>
<td>Feb 27th 2018, 15:16</td>
<td></td>
</tr>
<tr>
<td>RR626938F7F1C8B2C57215138328202745496022...</td>
<td>%cache% (view folder)</td>
<td>902: Trojan</td>
<td>Feb 12th 2018, 22:25</td>
<td></td>
</tr>
<tr>
<td>220519L4B1C8C8B7B1C16704A2C061A2D70F2495A0B8L</td>
<td>%cache% (view folder)</td>
<td>902: Trojan</td>
<td>Feb 12th 2018, 22:20</td>
<td></td>
</tr>
<tr>
<td>B82F68A1F40000809D0488DBB64C44764864...</td>
<td>%cache% (view folder)</td>
<td>902: Malware Gen</td>
<td>Feb 12th 2018, 22:20</td>
<td></td>
</tr>
<tr>
<td>A18A8427862B1C12C1F86066548C379930690F2676L</td>
<td>%cache% (view folder)</td>
<td>902: Trojan</td>
<td>Feb 12th 2018, 22:18</td>
<td></td>
</tr>
<tr>
<td>198419C0CCB8EF717A2D3FBB95A03644F1A55514L</td>
<td>%cache% (view folder)</td>
<td>902: Keylogger Gen</td>
<td>Feb 12th 2018, 22:13</td>
<td></td>
</tr>
<tr>
<td>E8CC0EF83991707F0F6794A5E08469979B46E36L</td>
<td>%cache% (view folder)</td>
<td>902: Keylogger Gen</td>
<td>Feb 12th 2018, 22:10</td>
<td></td>
</tr>
<tr>
<td>719F9C1A3A5018036342340B80065B88E4305L</td>
<td>%cache% (view folder)</td>
<td>902: Trojan</td>
<td>Feb 12th 2018, 22:09</td>
<td></td>
</tr>
<tr>
<td>898DE2268E8E19DE433149ED515430873535B0L</td>
<td>%cache% (view folder)</td>
<td>902: Trojan</td>
<td>Feb 12th 2018, 21:59</td>
<td></td>
</tr>
</tbody>
</table>

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

![Image of Webroot SecureAnywhere interface showing restored files]

The Restore From Quarantine window displays, with the file name and the MD5 information displayed in the fields.
6. To restore the file, click the **Restore** button.
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.

   ![Management Console with Sites Tab Active]

2. Click the Groups tab.

   The Groups tab displays.

   ![Management Console with Groups Tab Selected]
3. Select a device with the status of Protected that you want to view, and double-click.

![Device Selection Screen]

The Status Panel for the device you selected displays.

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.
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.

   ![Management Console with Sites Tab Active]

2. Click the Groups tab.

   The Groups tab displays.

   ![Management Console with Groups Tab Active]
3. Select a device with the status of **Not Seen Recently** that you want to view, and double-click.

The Status Panel for the device you selected displays.

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**
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.
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.

2. Click the Groups tab.

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

The Status Panel for the device you selected displays.
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.

![Image of the File Information window]

The File Information window displays.
When you're done viewing the information, click the **OK** button.
7. To send a clean command to the device, click the **Cleanup** button.

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

2. Click the Groups tab.

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

![Image of SecureAnywhere interface with a selected device showing Expired status]

The Status Panel for the device you selected displays.

![Image of SecureAnywhere Status Panel]

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**
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.
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.

2. Click the Devices tab.

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

The Status Panel for the device you selected displays.

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.
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.

   ![Management Console Screen](image1.png)

2. Click the Groups tab.

   ![Groups Tab Screen](image2.png)

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

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

The Summary panel displays the following information:

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

- The version number
- Site Information
- Operating System
- Network Information
- Protection
- Properties
- Shields
**Infections Encountered Tab**

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

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

**Blocked URLs Tab**

Contains a list of URLs that have been blocked from that endpoint.
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.*
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.

2. Click the Groups tab.

   The Groups tab displays.
3. In the left column, select the site that contains the device you want to find.

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.

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.
5. To clear the Search field, click the X.

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.

   ![Management Console with Sites Tab Active]

2. Click the Groups tab.

   The Groups tab displays.

   ![Groups Tab Displayed]
3. From the All sites drop-down menu, select the site you'd like to filter on.

The system displays the device you filtered on for.

4. To display all devices again, from the All sites drop-down menu, select All Sites.

The complete list of devices displays.
## Chapter 6: Working With Devices

![Device Management Dashboard](image)

### Device Management

#### Device Summary
- **Name**: [Device Name]
- **Status**: [Status]
- **Products**: [List of Products]
- **Policy**: [Policy Name]
- **Site**: [Site Name]
- **Time**: [Time]
- **Alerts**: [Alert Status]

### Device Details

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Status</th>
<th>Products</th>
<th>Policy</th>
<th>Site</th>
<th>Time</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Device 1]</td>
<td>[Status 1]</td>
<td>[Products 1]</td>
<td>[Policy 1]</td>
<td>[Site 1]</td>
<td>[Time 1]</td>
<td>[Alerts 1]</td>
</tr>
<tr>
<td>[Device 2]</td>
<td>[Status 2]</td>
<td>[Products 2]</td>
<td>[Policy 2]</td>
<td>[Site 2]</td>
<td>[Time 2]</td>
<td>[Alerts 2]</td>
</tr>
</tbody>
</table>
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.

   ![Management Console screenshot with Sites tab active]

2. Click the Groups tab.

   The Groups tab displays.

   ![Groups Tab screenshot]
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.
4. To display all devices again, from the All Statuses drop-down menu, select All Statuses.

The complete list of devices displays.
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.

2. Click the Groups tab.

   The Groups tab displays.
3. In the left column, select the site that contains the group you want to filter.

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.

2. Click the Groups tab.

   The Groups tab displays.
3. In the left column, select the site that contains the group you want to move.

![Image of SecureAnywhere interface showing site selection](image)

4. Select one or more devices from the Devices panel on the right.

![Image of SecureAnywhere interface showing device selection](image)

To select all devices, select the checkbox at the top of the column.
5. Click the **Move** button.

![Move button highlighted in the Webroot SecureAnywhere interface](image)

The Move Group window displays.

![Move Group window](image)

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.

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.
   The management console displays, with the Sites tab active.

2. Click the Groups tab.
   The Groups tab displays.
3. In the left column, select the site that contains the group you want to sort.

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

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.

   ![Management Console](image1.png)

2. Click the **Groups** tab.

   ![Groups Tab](image2.png)

   The Groups tab displays.
3. From the All sites drop-down menu, select the site you'd like to filter on.

The system displays the device you filtered on for.
4. To display all devices again, from the All sites drop-down menu, select **All Sites**.

The complete list of devices displays.

5. Click on a device you want to display a scan history for.

The Summary panel displays with the Summary tab active.
6. Click the **Scan History** tab.

The scan history for that device displays, including the following information:

- Scan Date
- Scan Result
- Scan Type
If any threats are detected, you can click on the file name to view information about the infection encountered.
7. Click the **OK** button after you are done reviewing the information to return to the Scan History tab.

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

2. Click the Groups tab.

   The Groups tab displays.
3. In the left column, select the site that contains the group and device you want to issue an agent command for.
4. In the Devices panel, select the device that you want to issue an agent command for.

To select all devices, select the checkbox at the top of the column.
5. Select a policy from the Agent Commands drop-down menu.

A confirmation window displays similar to the one displayed. Click **Run** or **Cancel**.

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.

   ![Image 1]

   2. Click the Groups tab.

   The Groups tab displays.

   ![Image 2]
3. In the left column, select the site that contains the group and device you want to view an agent command log for.
4. In the Devices panel, select the device that you want to view an agent command log for.

![Webroot SecureAnywhere interface](image)

To select all devices, select the checkbox at the top of the column.
Chapter 6: Working With Devices

![Image of SecureAnywhere interface showing sites and groups]

- All sites
- Apex Technology
- Athlead
- Caffe Giasco
- Down! The Pet Emporium
- East Pennsylvania Seminary
- Hermont Tires
- Prestige Direct Sales Solutions
- Tract Industries
- Vance Refrigeration

- MacOSX10121AEM
- MICHELIN
- PIRELLI
- TOYO
- WIN10X64_AEM
- WINSERVER2012R2
- WINSERVER2016_A
5. From the Agent Commands drop-down menu, select **View Command Log**.

![Image of SecureAnywhere interface with focus on Agent Commands drop-down menu](image)

A Command Log for Selected Devices window displays, and includes the following information:

- Command Sent
- Hostname
- Date Requested
### Status

![Command Log for Selected Devices](image)

<table>
<thead>
<tr>
<th>Command Sent</th>
<th>Hostname</th>
<th>Date Requested</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Scan</td>
<td>APEX-EXCHANGE</td>
<td>Jun 5th 2019, 17:56</td>
<td>Executed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-PROCUREMENT</td>
<td>Jun 5th 2019, 17:56</td>
<td>Executed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-RECEPTION</td>
<td>Jun 5th 2019, 17:56</td>
<td>Elapsed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-CONTROLLER</td>
<td>Jun 5th 2019, 17:56</td>
<td>Elapsed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-DC</td>
<td>Jun 5th 2019, 17:56</td>
<td>Executed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-PROCUREMENT</td>
<td>Jun 5th 2019, 17:55</td>
<td>Executed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-RECEPTION</td>
<td>Jun 5th 2019, 17:55</td>
<td>Elapsed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-CEO-MAC</td>
<td>Jun 5th 2019, 17:55</td>
<td>Elapsed</td>
</tr>
<tr>
<td>Run Scan</td>
<td>APEX-CONTROLLER</td>
<td>Jun 5th 2019, 17:55</td>
<td>Elapsed</td>
</tr>
</tbody>
</table>

6. As needed, you can click the **Export to CSV** button to download a spreadsheet of the Agent Command Log.
7. When you are done, click the **Close** button.
Chapter 7: Working With Policies

To work with policies, see the following topics:

Creating Policies ................................................................. 296
Editing Policies ................................................................. 302
  Basic Configuration Settings .............................................. 311
  Scan Schedule ............................................................... 315
  Scan Settings ............................................................... 317
  Self Protection Settings .................................................... 321
  Heuristics ........................................................................ 322
  Realtime Shield Settings ................................................... 326
  Behavior Shield Settings ................................................. 329
  Core System Shield .......................................................... 330
  Web Threat Shield .......................................................... 332
  Identity Shield ............................................................... 335
  Firewall .......................................................................... 338
  User Interface ................................................................. 340
  System Optimizer ............................................................ 341
  Evasion Shield Settings ..................................................... 350
Renaming Policies .............................................................. 352
Copying Policies ................................................................. 355
Importing Policies Manually ............................................... 359
Deleting Policies ............................................................... 364
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.

2. Click the Policies tab.

   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.
The settings window for that policy displays, with the Recommended Defaults at the top.

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.

<table>
<thead>
<tr>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a splash screen on bootup</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Start Menu</td>
</tr>
<tr>
<td>Show SecureAnywhere in Add/Remove Programs</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Windows Action Center</td>
</tr>
<tr>
<td>Hide the SecureAnywhere keycode and subscription information on-screen</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources</td>
</tr>
</tbody>
</table>

- Settings that apply to PC and Mac are indicated by both the Windows icon and the Mac icon.

<table>
<thead>
<tr>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a splash screen on bootup</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Start Menu</td>
</tr>
<tr>
<td>Show SecureAnywhere in Add/Remove Programs</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Windows Action Center</td>
</tr>
<tr>
<td>Hide the SecureAnywhere keycode and subscription information on-screen</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources</td>
</tr>
</tbody>
</table>

The On/Off column displays how the setting is currently implemented on the endpoints.
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.

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>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.</td>
</tr>
<tr>
<td>Scan Schedule</td>
<td>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.</td>
</tr>
<tr>
<td>Scan Settings</td>
<td>Provides more control over scans, such as performing a more thorough scan.</td>
</tr>
<tr>
<td>Self Protection</td>
<td>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.</td>
</tr>
<tr>
<td>SECTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Heuristics</td>
<td>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.</td>
</tr>
<tr>
<td>Realtime Shield</td>
<td>Blocks known threats listed in Webroot's threat definitions and in Webroot's community database.</td>
</tr>
<tr>
<td>Behavior Shield</td>
<td>Analyzes applications and processes running on the endpoints.</td>
</tr>
<tr>
<td>Core System Shield</td>
<td>Monitors the computer system structures to ensure that malware has not tampered with them.</td>
</tr>
<tr>
<td>Web Threat Shield</td>
<td>Protects endpoints as users surf the Internet and click links in search results.</td>
</tr>
<tr>
<td>Identity Shield</td>
<td>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.</td>
</tr>
<tr>
<td>Firewall</td>
<td>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.</td>
</tr>
</tbody>
</table>
### SECTION

<table>
<thead>
<tr>
<th>User Interface</th>
<th>Provides user access to the SecureAnywhere program on the endpoint.</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Optimizer</td>
<td>Controls System Optimizer behavior, such as an automatic optimization schedule and what types of files and traces to remove from the endpoint.</td>
</tr>
<tr>
<td>Evasion Shield</td>
<td>Detects, blocks, and remediates (quarantines) evasive attacks, whether they are file-based, fileless, obfuscated, or encrypted, and prevents malicious behaviors from executing.</td>
</tr>
</tbody>
</table>

**To edit a policy:**

1. Log in to the management console.

   The management console displays, with the Sites tab active.
2. Click the **Policies** tab.

The Policies tab displays.
3. In the Policies column, click a policy to display its settings.

![Image of SecureAnywhere interface with recommended defaults highlighted]

The policy's settings window displays, with the Basic Configuration setting selected.

![Image of recommended defaults settings window]

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.

<table>
<thead>
<tr>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a splash screen on bootup</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Start Menu</td>
</tr>
<tr>
<td>Show SecureAnywhere in Add/Remove Programs</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Windows Action Center</td>
</tr>
<tr>
<td>Hide the SecureAnywhere keycode and subscription information on-screen</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources</td>
</tr>
</tbody>
</table>

- Settings that apply to PC and Mac are indicated by both the Windows icon and the Mac icon.

<table>
<thead>
<tr>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a splash screen on bootup</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Start Menu</td>
</tr>
<tr>
<td>Show SecureAnywhere in Add/Remove Programs</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Windows Action Center</td>
</tr>
<tr>
<td>Hide the SecureAnywhere keycode and subscription information on-screen</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources</td>
</tr>
</tbody>
</table>

The On/Off column displays how the setting is currently implemented on the endpoints.
4. From the Policy Section drop-down menu, select the category you want to edit.
5. Select either **On** or **Off** for that setting.

For a complete description of each setting, see the following tables in this procedure.

<table>
<thead>
<tr>
<th>Basic Configuration</th>
<th>Core System Shield</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Schedule</td>
<td>Web Threat Shield</td>
</tr>
<tr>
<td>Scan Settings</td>
<td>Identity Shield</td>
</tr>
<tr>
<td>Self Protection</td>
<td>Firewall</td>
</tr>
<tr>
<td>Heuristics</td>
<td>User Interface</td>
</tr>
<tr>
<td>Realtime Shield</td>
<td>System Optimizer</td>
</tr>
<tr>
<td>Behavior Shield</td>
<td>Evasion Shield</td>
</tr>
</tbody>
</table>
6. When you're done making changes for a selection, click the **Save** button.

**Basic Configuration Settings**

The Basic Configuration settings control the behavior of the SecureAnywhere software on sites.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show a SecureAnywhere shortcut on the desktop</strong></td>
<td>Provides quick access to the main interface by placing the shortcut icon on the endpoint desktop. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Show a system tray icon</strong></td>
<td>Provides quick access to SecureAnywhere functions by placing the Webroot icon in the endpoint system tray. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Show a splash screen on bootup</strong></td>
<td>Opens the Webroot splash screen when the endpoint starts. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Show SecureAnywhere in the Start Menu</strong></td>
<td>Lists SecureAnywhere in the Windows Startup menu items. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Show SecureAnywhere in Add/Remove Programs</strong></td>
<td>Lists SecureAnywhere in the Windows Add/Remove Programs panel. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Show SecureAnywhere in Windows Action Center</strong></td>
<td>Lists SecureAnywhere in the Windows Action Center, under Virus Protection information. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>
## Chapter 7: Working With Policies

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide the SecureAnywhere keycode on-screen</td>
<td>Hides the keycode on the endpoint's My Account panel. Asterisks replace the code, except for the first four digits. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
<td>Downloads product updates automatically without alerting the endpoint user. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources</td>
<td>Saves CPU resources by running non-scan related functions in the background. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Favor low disk usage over verbose logging (fewer details stored in logs)</td>
<td>Saves disk resources by saving only the last four log items. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Lower resource usage when intensive applications or games are detected</td>
<td>Suppresses SecureAnywhere functions while the user is gaming, watching videos, or using other intensive applications. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow SecureAnywhere to be shut down manually</td>
<td>Displays a Shutdown command in the endpoint's system tray menu. Deselecting this option removes the Shutdown command from the menu. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Force non-critical notifications into the background</td>
<td>Suppresses information-only messages from displaying in the system tray. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Fade out warning messages automatically</td>
<td>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. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Store Execution History details</td>
<td>Stores data for the Execution History logs, available under Reports. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Poll interval</td>
<td>Specifies how often the endpoint checks for updates. For example: 15 minutes, 30 minutes, 1 hour, or 2 hours. This setting applies to both PC and Mac endpoints.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Scheduled Scans</td>
<td>Allows scheduled scans to run on the endpoint. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Scan Frequency</td>
<td>Determines how often to run the scan. You can set a day of the week or select on bootup. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Time</td>
<td>Specifies the time to run the scan:&lt;br&gt;  • Scan time options for when computer is idle are before 8:00 a.m., before noon, before 5:00 p.m., or before midnight.&lt;br&gt;  • Scan time options for when resources are available are hourly, from 12:00 a.m. to 11:00 p.m. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Scan on bootup if the computer is off at the scheduled time</td>
<td>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. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hide the scan progress window during scheduled scans</td>
<td>Runs scans silently in the background. If this option is disabled, a window opens and displays the scan progress.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Only notify me if an infection is found during a scheduled scan</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Do not perform scheduled scans when on battery power</td>
<td>Helps conserve battery power. If you want SecureAnywhere to launch scheduled scans when the endpoint is on battery power, deselect this option.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Do not perform scheduled scans when a full screen application or game is open</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Randomize the time of scheduled scans up to one hour for distributed</td>
<td>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.</td>
</tr>
<tr>
<td>scanning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Perform a scheduled Quick Scan instead of a Deep Scan</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**Scan Settings**

Scan settings give advanced control over scanning performance.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Realtime Master Boot Record (MBR) Scanning</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable Enhanced Rootkit Detection</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable &quot;right-click&quot; scanning in Windows Explorer</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Update the currently scanned folder immediately as scanned</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Favor low memory usage over fast scanning</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Favor low CPU usage over fast scanning</td>
<td>Reduces CPU usage during scans, but scans will also run a bit slower. Deselect this option to run faster scans.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Save non-executable file details to scan logs</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show the &quot;Authenticating Files&quot; popup when a new file is scanned on-execution</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Scan archived files</td>
<td>Scans compressed files in zip, rar, cab, and 7-zip archives.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatically reboot during cleanup without prompting</td>
<td>Restarts the computer after running a clean-up, which is the process of removing all traces of a malware file. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Never reboot during malware cleanup</td>
<td>Prevents the endpoint from restarting during cleanup, which is the process of removing all traces of a malware file. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Automatically remove threats found during background scans</td>
<td>Removes threats during scans that run in the endpoint's background and sends them to quarantine. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Automatically remove threats found on the learning scan</td>
<td>Removes threats during the first scan on the endpoint and sends them to quarantine. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable Enhanced Support</td>
<td>Allows logs to be sent to Webroot customer support. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Show Infected Scan Results</strong></td>
<td>Displays scan results. If not enabled, the endpoint does not display scan results even if malware is detected.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Detect Possibly Unwanted Applications (PUAs) as malicious</strong></td>
<td>Detects PUAs and blocks them from installing.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Allow Files to be Submitted for Threat Research</strong></td>
<td>Allows you to submit files for threat research.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable self-protection response cloaking</td>
<td>Turns self-protection on and off. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Self-protection level</td>
<td>Sets the detection level to:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Minimum</strong> — Protects the integrity of the SecureAnywhere settings and databases. Recommended if the endpoint has several other security products installed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Medium</strong> — Prevents other programs from disabling protection. Provides maximum possible compatibility with other security software.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Maximum</strong> — Provides the highest protection of the SecureAnywhere processes. We recommend that you use this setting.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**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.
### Advanced Heuristics

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disabled</strong></td>
<td>- Turns off Advanced Heuristics, leaving it vulnerable to new threats; however, it will still be protected against known threats.</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>- Detects programs with a high level of malicious activity. This setting ignores some suspicious behavior and allows most programs to run.</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>- Balances detection versus false alarms by using our tuned heuristics in the centralized community database.</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>- 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.</td>
</tr>
<tr>
<td><strong>Maximum</strong></td>
<td>- 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.</td>
</tr>
</tbody>
</table>

This setting applies only to PC endpoints.
### Age Heuristics

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analyzes</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Disabled</strong> — Turns off Age Heuristics, leaving it vulnerable to new threats; however, it will still be protected against known threats.</td>
<td></td>
</tr>
<tr>
<td><strong>Low</strong> — Detects programs that have been created or modified very recently.</td>
<td></td>
</tr>
<tr>
<td><strong>Medium</strong> — 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.</td>
<td></td>
</tr>
<tr>
<td><strong>High</strong> — 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Maximum</strong> — 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.</td>
<td></td>
</tr>
</tbody>
</table>

This setting applies only to PC endpoints.
## Setting

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Popularity Heuristics</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

## 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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Realtime Shield Enabled</strong></td>
<td>Turns the Realtime shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Enable Predictive Offline Protection from the central SecureAnywhere database</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Remember actions on blocked files</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Automatically quarantine previously blocked files</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Automatically block files when detected on execution</strong></td>
<td>Blocks threats and sends them to quarantine. If this setting is off, the user must respond to alerts about detected threats.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scan files when written or modified</td>
<td>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. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Block threats automatically if no user is logged in</td>
<td>Stops threats from executing even when managed endpoints are logged off. Threats are sent to quarantine without notification. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Show realtime event warnings</td>
<td>Opens an alert when suspicious activity occurs. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show realtime block modal alerts</td>
<td>Displays alerts when Heuristics detects malware, and prompts the user to allow or block the action. 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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show realtime block notifications</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Shield Enabled</td>
<td>Turns the Behavior shield on and off. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Assess the intent of new programs before allowing them to execute</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable advanced behavior interpretation to identify complex threats</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Track the behavior of untrusted programs for advanced threat removal</td>
<td>Watches programs that have not yet been classified as legitimate or as malware. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatically perform the recommended action instead of showing warning messages</td>
<td>Does not prompt the user to allow or block a potential threat. SecureAnywhere determines how to manage the item. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Warn if untrusted programs attempt low-level system modifications when offline</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core System Shield Enabled</strong></td>
<td>Turns the Core System shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Assess system modifications before they are</strong></td>
<td>Intercepts any activity that attempts to make system changes on your managed endpoints, such as a new service installation.</td>
</tr>
<tr>
<td><strong>Detect and repair broken system components</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Prevent untrusted programs from modifying kernel memory</strong></td>
<td>Stops unclassified programs from changing the kernel memory.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td><strong>Prevent untrusted programs from modifying system processes</strong></td>
<td>Stops unclassified programs from changing system processes.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.  
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.  
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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Web Threat Shield</td>
<td>Turns the Web Threat shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>Activate browser extension</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>To completely disable and remove extensions from each supported browser, change the setting to Off.</td>
</tr>
<tr>
<td></td>
<td>This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Block malicious websites</td>
<td>Any URLs and IPs you enter in a browser are checked and a block page displays for known malicious sites.</td>
</tr>
<tr>
<td></td>
<td>This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Enable real-time anti-phishing</strong></td>
<td>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. This setting is turned On by default, which is the setting we recommend. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Show safety ratings when using search engines</strong></td>
<td>Search result are annotated with an icon and tooltip, indicating the likelihood that a site is malicious. This setting is turned On by default, which is the setting we recommend. This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td><strong>Enable web filtering driver</strong></td>
<td>Provides additional protection against malicious connections, and in cases where the browser extensions are disabled. This setting is turned On by default, which is the setting we recommend.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Suppress the user's ability to bypass blocked websites | Prevents users from bypassing the block page presented when a malicious website is detected.  
This setting is turned On by default, which is the setting we recommend.  
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.  
This setting is turned On by default, which is the setting we recommend.  
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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Shield Enabled</td>
<td>Turns the Identity shield on and off.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to both PC and Mac endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: On Mac, this controls the Secure Keyboard Entry Mode setting.</td>
</tr>
<tr>
<td>Look for identity threats online</td>
<td>Analyzes websites as users browse the Internet or open links. If the shield detects malicious content, it blocks the site and opens an alert.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Verify websites for phishing threats</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Verify websites when visited to determine legitimacy</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.  
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.  
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.  
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.  
This setting applies only to PC endpoints.                                                                                                       |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow trusted screen capture programs access to protected screen contents</td>
<td>Allows screen capture programs, no matter what content is displayed on the screen. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable Identity Shield compatibility mode</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Enable keylogging protection in non-Latin systems</td>
<td>Allows endpoints with non-Latin systems, such as Japanese and Chinese, to be protected from keyloggers. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Enabled** | Turns the Firewall on and off.  
This setting applies only to PC endpoints. |
| **Firewall level** |  
- **Default Allow** — Allows all processes to connect to the Internet, unless explicitly blocked.  
- **Warn unknown and infected** — Warns if any new, untrusted processes connect to the Internet, if the endpoint is infected.  
- **Warn unknown** — Warns if a new, untrusted process connects to the Internet.  
- **Default Block** — Warns if any process connects to the Internet, unless explicitly blocked.  
This setting applies only to PC endpoints. |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show firewall management warnings</td>
<td>Controls the alert displayed by SecureAnywhere when the Windows firewall is off:</td>
</tr>
<tr>
<td></td>
<td>• <strong>On</strong> — The user sees an alert when SecureAnywhere detects that the Windows firewall is off.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> — No alert displays when the Windows firewall is off.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Show firewall process warnings</td>
<td>Controls the firewall alerts. If this is setting is Off, no firewall alerts display. This option works in conjunction with the Firewall Level settings.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• If Show Firewall process warnings is set to Off, no alert displays to the endpoint user and the process is allowed.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

**User Interface**

Gives administrative control over the SecureAnywhere interface on the endpoints using this policy.
### 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.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage System Optimizer centrally</td>
<td>Enables the administrator to change System Optimizer settings, as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>On</strong> — System Optimizer settings display in the panel and are available to change.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> — No settings display in this panel.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
</tr>
<tr>
<td>Monday through Sunday</td>
<td>Sets the days of the week, anything from one to seven, to automatically run System Optimizer.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Run at specific time of day - hour</td>
<td>Sets the hour of the day System Optimizer runs on the endpoints.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Run at specific time of day - minute</td>
<td>Sets the time in 15-minute increments that System Optimizer runs on the endpoints.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.  
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:  
This setting applies only to PC endpoints.                             |
| Windows Desktop                                                        |                                                                                                                                              |
| Recycle Bin                                                            | Removes all files from the Recycle Bin in Windows Explorer.  
This setting applies only to PC endpoints.                             |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recent document history</td>
<td>Clears the history of recently opened files, which is accessible from the Windows Start menu. The cleanup does not delete the actual files.  This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Start Menu click history</td>
<td>Clears the history of shortcuts to programs that end users recently opened using the Start menu.                                            This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Run history</td>
<td>Clears the history of commands recently entered into the Run dialog, which is accessible from the Start menu. After the cleanup, the end user may need to restart the computer to completely remove items from the Run dialog.  This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Search history</td>
<td>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.  This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Start Menu order history</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Windows System</td>
<td></td>
</tr>
<tr>
<td>Clipboard contents</td>
<td>Clears the contents from the Clipboard, where Windows stores data used in either the Copy or Cut function from any Windows program.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Windows Temporary folder</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>System Temporary folder</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Windows Update**           | 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.  
This setting applies only to PC endpoints. |
| **Temporary folder**         |                                                                                                                                               |
| **Windows Registry Streams** | Clears the history of recent changes made to the Windows registry. This option does not delete the registry changes themselves.         
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.  
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.  
This setting applies only to PC endpoints. |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **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:  

C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\CD Burning  

or  

C:\Users\[username]\AppData\Local\Microsoft\Windows\Burn\Burn  

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.  

This setting applies only to PC endpoints. |
| **Internet Explorer**       | 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.  

This setting applies only to PC endpoints. |
<p>| <strong>Address bar history</strong>     |             |</p>
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookies</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Temporary Internet Files</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>URL history</td>
<td>Deletes the History list of recently visited websites of the Internet Explorer toolbar.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Setup Log</td>
<td>Deletes log files created during Internet Explorer updates.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Microsoft Download Folder</td>
<td>Deletes the contents in the folder that stores files last downloaded using Internet Explorer.</td>
</tr>
<tr>
<td></td>
<td>This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MediaPlayer Bar History</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Autocomplete form information</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
<tr>
<td>Clean index.dat (cleaned on reboot)</td>
<td>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. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>
## Secure File Removal

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control the level of security to apply when removing files</strong></td>
<td>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. 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. This setting applies only to PC endpoints.</td>
</tr>
</tbody>
</table>

---

### 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.
### Script Protection

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sets the protection level to:</td>
</tr>
<tr>
<td></td>
<td>- Off</td>
</tr>
<tr>
<td></td>
<td>- <strong>Detect and Report</strong> — Threats will be detected, reported to the console and <strong>not</strong> quarantined.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Detect and Remediate</strong> — Threats will be detected, reported to the console and quarantined.</td>
</tr>
</tbody>
</table>

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.

2. Click the Policies tab.

   The Policies tab displays.
3. In the Policies column, select a policy that you want to rename.

**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.

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

2. Click the Policies tab.

   The Policies tab displays.
3. In the Policies column, select a policy that you want to copy.
4. Click the Copy button.

![Copy Policy window](image)

The Copy Policy window displays.

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.
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.

2. Click the Policies tab.

The Policies tab displays.
3. Click the **Import** button.

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.
5. From the Policy drop-down menu, select the policy you want to import.
6. When you're done, click the **Import** button.

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.

   ![Management Console Screenshot]

   The management console displays, with the Sites tab active.

2. Click the Policies tab.

   The Policies tab displays.
Chapter 7: Working With Policies
3. In the Policies column, select the policy you want to delete and click the **Delete** button.

![Dashboard](image)

**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 Standard Policy](image)
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.

5. Click the Confirm Delete button, and be sure to assign any necessary replacement policies.

The system deletes the policy.
Chapter 8: Working With Overrides

To work with overrides, see the following topics:

- Creating Web Overrides ................................................................. 369
- Creating Whitelist Overrides ....................................................... 375
- Creating Blacklist Overrides ....................................................... 383
- Editing Web Overrides ............................................................... 387
- Importing Overrides ................................................................. 393
- Viewing Web Overrides ............................................................ 398
- Deleting Overrides ................................................................. 402
- Deleting Web Overrides ............................................................ 406
- Customizing Block Pages .......................................................... 411
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.

2. Click the [Overrides](#) tab.
   
   The Overrides tab displays, with the File Whitelist tab active.
3. Click the **Web Block / Allow List** tab.

The Web Block / Allow List tab displays.
4. Click the **Add** button.

The Create New Entry window displays.
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.

**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.
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.

2. Click the Overrides tab.

   The Overrides tab displays, with the File Whitelist tab active.
3. Click the **Add** button.
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

Create  Cancel
```

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.

```
<table>
<thead>
<tr>
<th>Name / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a name or description to help identify this entry</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Override Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ MD5 ☐ Folder / File</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a 32 character MD5</td>
</tr>
</tbody>
</table>
```

The system displays the New Whitelist Entry window with the relevant fields.
8. Populate the fields on the window using the information in the following table.
<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 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.  
                              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.                                                                                                       
                              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.            
                              You may not use ‘%temp%’ for example as this refers to a specific users temp directory (‘username/temp/’). Wildcards are not supported. |
<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Sub-folders</td>
<td>Select this checkbox to apply the override to all sub-folders within this folder.</td>
</tr>
<tr>
<td>Detect if Malicious</td>
<td>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. 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.</td>
</tr>
</tbody>
</table>

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

- [ ]

---

**Create**  
**Cancel**
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.

2. Click the Overrides tab.

   The Overrides tab displays, with the File Whitelist tab active.
3. Click the **File Blacklist** tab.

The **File Blacklist** tab displays.
4. Click the **Add** button.

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.

2. Click the Overrides tab.

   The Overrides tab displays, with the File Whitelist tab active.
3. Click the **Web Block / Allow List** tab.

The Web Block / Allow List tab displays.
4. For the override you want to edit, in the Actions column, click the three ellipses, and select **Edit Override**.

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

Edit
Cancel
5. Edit the fields, as needed.

**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.

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.

2. Click the Overrides tab.

   The Overrides tab displays, with the File Whitelist tab active.
3. Click the **Import** button.

The Import Overrides window displays.
4. From the Site to import overrides from drop-down menu, select the site from where you want to import 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.

6. When you’re done, click the **Import** button.
The system imports all overrides from that site into your currently selected site.
Viewing Web Overrides

Follow this procedure to view additional information about 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.

   ![Management Console Screenshot]

2. Click the Overrides tab.

   The Overrides tab displays, with the File Whitelist tab active.

   ![Overrides Tab Screenshot]
3. Click the **Web Block / Allow List** tab.

The Web Block / Allow List tab displays.
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.
# Chapter 8: Working With Overrides

![Image](image-url)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Scope</th>
<th>Associated Policy</th>
<th>Block / Allow</th>
<th>Last Modified</th>
<th>Affiliate</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>Global and Site</td>
<td>All Policies</td>
<td>Block</td>
<td>Jun 25 2019, 18:13</td>
<td></td>
</tr>
<tr>
<td>fast.com</td>
<td>Trusted Indicators</td>
<td>NG2_high-protection</td>
<td>Allow</td>
<td>Mar 21 2016, 22:07</td>
<td></td>
</tr>
<tr>
<td>*facebook.com</td>
<td>Vrij</td>
<td></td>
<td>Block</td>
<td>Mar 18 2019, 15:55</td>
<td></td>
</tr>
<tr>
<td>*facebook.com</td>
<td>Vrij</td>
<td></td>
<td>Allow</td>
<td>Mar 18 2019, 15:57</td>
<td></td>
</tr>
</tbody>
</table>
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.

2. Click the Overrides tab.
   
The Overrides tab displays, with the File Whitelist tab active.
3. On either the Whitelist or the Blacklist tab, highlight the override that you want to delete.

The override you selected is highlighted, and the Delete button becomes active.
4. Click the **Delete** button.

The system displays the Delete Whitelist/Blacklist Entry confirmation window.
5. Click the **Confirm Delete** button.

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.

2. Click the Overrides tab.
   
The Overrides tab displays, with the File Whitelist tab active.
3. Click the **Web Block / Allow List** tab.

The Web Overrides tab displays with the Allow List tab active.
4. For the web override you want to delete, in the Actions column, click the three ellipses and select **Delete**.

The Delete window displays with the URL for the web override that you selected.
5. Click the **Confirm Delete** button.

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.

   The management console displays, with the Sites tab active.

   ![Management Console](image1)

2. Click the **Overrides** tab.

   The Overrides tab displays, with the File Whitelist tab active.

   ![Overrides Tab](image2)
3. Click the **Web Block Page Settings** tab.

The Web Block Page Settings tab displays.
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.

6. When you're done, click the **Submit** button.
7. As needed, click the **Reset to default settings** button.
Chapter 9: Working With Alerts

To work with alerts, see the following topics:

- Creating Alerts ................................................................. 418
- Deleting Alerts ............................................................... 426
- Suspending or Resuming Alerts ....................................... 430
- Creating Distribution Lists ............................................. 435
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.

2. Click the Alerts tab.

   The system displays the Alerts tab, with the Alert List tab active.
3. Click the **Add** button.

The system displays the Create Alert window.
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.

The system displays the Recipients panel.

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.

The system displays the Sites panel.
11. Select one of the following Sites to use this alert radio buttons:
   - All Sites
   - Selected Sites

12. Click the **Next** button.

The system displays the Email Template panel.
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.
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.

2. Click the Alerts tab.
   
The system displays the Alerts tab, with the Alert List tab active.
3. Click the alert you want to delete.

The system displays information about that alert and the Delete button becomes active.
4. Click the **Delete** button.

The Delete Alert Message displays.
5. Click the **Confirm Delete** button.

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.

2. Click the Alerts tab.

   The system displays the Alerts tab, with the Alert List tab 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.
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.
Click the **Resume** button to resume the alert.

The **Status** column reflects whether the alert is active or suspended.
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.

   The management console displays, with the Sites tab active.

   ![Management Console with Sites Tab Active]

   2. Click the Alerts tab.

   The system displays the Alerts tab, with the Alert List tab active.

   ![Management Console with Alert List Tab Active]
3. Click the **Distribution Lists** tab.

The Distribution Lists tab displays.
### Chapter 9: Working With Alerts

![WEBROUT SecureAnywhere Alerts](image)

**Alert List: Distribution Lists**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution List (Used) Renamed</td>
</tr>
<tr>
<td>Distribution List 1</td>
</tr>
<tr>
<td>Distribution List 220180213161717</td>
</tr>
<tr>
<td>Distribution List 320180213162149</td>
</tr>
<tr>
<td>Distribution List 420180213162222</td>
</tr>
<tr>
<td>Distribution List 520180213162326</td>
</tr>
<tr>
<td>Distribution List, not used</td>
</tr>
</tbody>
</table>
4. Click the **Add** button.

The Create Distribution List window displays.
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.
## Chapter 10: Working With Reports

To work with reports, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Site Manager Reports Overview</td>
<td>441</td>
</tr>
<tr>
<td>Creating Reports</td>
<td>442</td>
</tr>
<tr>
<td>Generating Reports</td>
<td>448</td>
</tr>
<tr>
<td>Generating On-Demand Reports</td>
<td>454</td>
</tr>
<tr>
<td>Creating Report Templates</td>
<td>477</td>
</tr>
<tr>
<td>Accessing Report Histories</td>
<td>492</td>
</tr>
<tr>
<td>Downloading Reports</td>
<td>495</td>
</tr>
</tbody>
</table>
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.
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.

2. Click the Reports tab.

The system displays the Reports tab with the On-Demand tab active.
3. Click the **Scheduled Reports** tab.

The Scheduled Reports tab displays.
4. Click the **Add** button.

The Create Report window displays.
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 every 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:

<table>
<thead>
<tr>
<th>German</th>
<th>Turkish</th>
<th>Spanish</th>
</tr>
</thead>
<tbody>
<tr>
<td>French</td>
<td>Italian</td>
<td>Japanese</td>
</tr>
<tr>
<td>Korean</td>
<td>Dutch</td>
<td>Portuguese</td>
</tr>
<tr>
<td>Russian</td>
<td>Chinese (Simplified)</td>
<td>Chinese (Traditional)</td>
</tr>
</tbody>
</table>

12. When you're done, click the **Create** button.
### Chapter 10: Working With Reports

#### Create Report

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Name</td>
<td></td>
</tr>
<tr>
<td>Delivery Schedule</td>
<td>Weekly ▼ Monday ▼ 09:00 ▼ UTC -00:00 ▼</td>
</tr>
<tr>
<td>Creation Method</td>
<td>One report created per site</td>
</tr>
<tr>
<td>Recipients</td>
<td>Email to the report distribution list of each site</td>
</tr>
<tr>
<td>Template</td>
<td>+ 1 template</td>
</tr>
<tr>
<td>Sites</td>
<td>1 of 530 selected</td>
</tr>
<tr>
<td>Languages</td>
<td>1 of 13 selected</td>
</tr>
</tbody>
</table>

[Create] [Cancel]
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.

2. Click the Reports tab.

   The system displays the Reports pane with the On-Demand tab active.
3. Click the **Scheduled Reports** tab.

The Scheduled Reports tab displays.
4. Click the name of the report that you want to run.

The Report Details pane displays.
Chapter 10: Working With Reports

![SecureAnywhere interface showing report details](image)

<table>
<thead>
<tr>
<th>Report Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report Name</strong></td>
</tr>
<tr>
<td><strong>Delivery Schedule</strong></td>
</tr>
<tr>
<td><strong>Creation Method</strong></td>
</tr>
<tr>
<td><strong>Recipients</strong></td>
</tr>
<tr>
<td><strong>Additional Emails</strong></td>
</tr>
<tr>
<td><strong>Template</strong></td>
</tr>
<tr>
<td><strong>Sites</strong></td>
</tr>
<tr>
<td><strong>Languages</strong></td>
</tr>
</tbody>
</table>

© 2019 Webroot Inc.  Privacy Statement  Website Terms of Service  License Agreement
5. Update report details as needed, then click the **Run Report Now** button.

The Run this report now window displays.
6. Do one of the following:
   - To run the report without any changes, click the Run button.
   - 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.
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.

2. Click the Reports tab.

   The system displays the Reports pane with the On-Demand tab active.
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.
<table>
<thead>
<tr>
<th>DATA FIELD</th>
<th>REPORT DESCRIPTION</th>
<th>CHART TYPES</th>
<th>TIME PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Version Spread</td>
<td>Shows which version of the Webroot Secure Anywhere agent each Endpoint device is using.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>All Threats Seen</td>
<td>Locates detected threats. This report lists threats by file name, along with when and where SecureAnywhere detected them.</td>
<td>Spreadsheet</td>
<td>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.</td>
</tr>
<tr>
<td>All Undetermined Software Seen</td>
<td>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.</td>
<td>Spreadsheet</td>
<td>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.</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Attention Required</td>
<td>Provides a list of all Endpoint devices that have been determined as secure, and a list of those that require attention.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Device Activations</td>
<td>Provides a list of all Endpoint devices that have been activated during the time period that you selected.</td>
<td>Area, Area Spline, Bar, Column, Line, Spline</td>
<td>24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days</td>
</tr>
<tr>
<td>Device Type</td>
<td>Provides a list of the number of Endpoint devices that are PCs or Macs.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Devices Needing Attention</td>
<td>Displays a list of devices that have the status of Needs Attention.</td>
<td>List</td>
<td>24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Devices With Threats Seen On Last Scan</td>
<td>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.</td>
<td>Spreadsheet</td>
<td>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.</td>
</tr>
<tr>
<td>Devices With Undetermined Software On Last Scan</td>
<td>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.</td>
<td>Spreadsheet</td>
<td>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.</td>
</tr>
<tr>
<td>Endpoint Status</td>
<td>Shows the number of clean Endpoint devices, and the number of infected Endpoint devices on your sites.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Evasion Shield - Script Detections</td>
<td>Locates detected threats. This report lists threats by name, along with when and where Webroot detected them.</td>
<td>Spreadsheet</td>
<td>24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days</td>
</tr>
<tr>
<td>Evasion Shield - Script Protection Status</td>
<td>Shows which of your Endpoint Devices have the Script Protection option:</td>
<td>Bar with drill-down to sites and endpoints</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Detect and Remediate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Detect and Report</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expired Status</td>
<td>Shows the number of Endpoint devices that are Active, and the number of Endpoint devices that have an Expired state.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Firewall Status</strong></td>
<td>Shows which of your Endpoint Devices have the Firewall option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Identity Shield Status</strong></td>
<td>Shows how many of your Endpoint Devices have the Identity Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Infrared Status</td>
<td>Shows which of your Endpoint devices have the Enable Webroot Infrared option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation Status</td>
<td>Shows which of your Endpoint devices have the Webroot Secure Anywhere product installed and which ones have had the product uninstalled.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Managed by Policy</td>
<td>Shows how many of your Endpoint devices are being managed by a policy you have created and how many are in an unmanaged state.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Offline Shield Status</td>
<td>Shows how many of your Endpoint devices have the Offline Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System Firewall Status</td>
<td>Shows which of your Endpoint devices have an operating system Firewall option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System Language</td>
<td>Shows which Operating system language your Endpoint devices are using.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Operating System Platform</td>
<td>Shows which Operating system platform, from 32 bit, 64 bit, or Unknown, that your Endpoint devices are using.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Phishing Shield Status</td>
<td>Shows how many of your Endpoint devices have the Phishing Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Browser</td>
<td>Shows the Primary Web Browser used by each of your Endpoint devices.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| **Realtime Shield Status** | Shows how many of your Endpoint devices have the Realtime Shield option:  
- Disabled  
- Enabled | Bar, Column, Pie | N/A |
| **Remediation Status** | Shows how many of your Endpoint devices have the Remediation status:  
- Disabled  
- Enabled  
To disable the Remediation status, the **Automatically quarantine previously blocked files** option, must be turned off. | Bar, Column, Pie | N/A |
### Report Summary

<table>
<thead>
<tr>
<th>DATA FIELD</th>
<th>REPORT DESCRIPTION</th>
<th>CHART TYPES</th>
<th>TIME PERIODS</th>
</tr>
</thead>
</table>
| Report Summary | Provides a number of overall counts that effectively summarize site or deployment information:  
- Number of active devices  
- Number of available seats  
Endpoints currently needing attention  
- Endpoints which encountered threats (Last ‘n’ days)  
- Total Threats seen (Last ‘n’ days)  
- Number of Endpoints Seen (Last ‘n’ days)  
- Number of Endpoints Not Seen (Last ‘n’ days)  
- Number of Endpoints Seen | Bar, Column, Pie | N/A |
<table>
<thead>
<tr>
<th>DATA FIELD</th>
<th>REPORT DESCRIPTION</th>
<th>CHART TYPES</th>
<th>TIME PERIOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>(All Time)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rootkit Shield Status</td>
<td>Shows how many of your Endpoint devices have the Rootkit Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Scans Status</td>
<td>Shows how many of your Endpoint devices have a Scheduled Scan:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Silent Mode</td>
<td>Shows how many of your Endpoint devices have the Silent Audit option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Detection History</td>
<td>Shows the history over your selected time period, of all threats that have been detected on your Endpoint devices.</td>
<td>Area, Area Spline, Bar, Column, Line, Spline</td>
<td>24h, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days</td>
</tr>
<tr>
<td>USB Shield Status</td>
<td>Shows how many of your Endpoint devices have the USB Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>Virtual Machine</strong></td>
<td>Shows how many of your Endpoint devices have been classified as Virtual Machines (VMs).</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Web Threat Shield Blocked URL History</strong></td>
<td>Displays a history of the URLs that have been blocked by Webroot’s Web Threat Shield.</td>
<td>Spreadsheet</td>
<td>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.</td>
</tr>
</tbody>
</table>
### DATA FIELD | REPORT DESCRIPTION | CHART TYPES | TIME PERIODS
--- | --- | --- | ---
**Web Threat Shield Blocked URLs** | Displays a list of 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:  
- Disabled  
- 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

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:
7. When you're done, click the **Submit** button.

The system displays the report in the console in a graphic format.
8. To display information about the report, click on any of the segments.
9. In the left panel, click on any site to display additional information about a particular site.

The system displays additional information about that site.
10. Click on any of the names in the Hostname column to display additional and more specific information about that hostname. Use the scrollbar on the right to view all of the information.
11. When you're done, you can click the Left arrow to return to the previous view.
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.

2. Click the Reports tab.

The system displays the Reports pane with the On-Demand tab active.
3. Click the **Scheduled Templates** tab.

The Scheduled Templates tab displays.
Chapter 10: Working With Reports

[Image of the SecureAnywhere interface with the Reports tab selected, showing a list of scheduled templates]
4. Click the **Add** button.

The Create Template window displays.
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.

<table>
<thead>
<tr>
<th>DATA FIELD</th>
<th>REPORT DESCRIPTION</th>
<th>CHART TYPES</th>
<th>TIME PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Version Spread</td>
<td>Shows which version of the Webroot Secure Anywhere agent each Endpoint device is using.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Attention Required</td>
<td>Provides a list of all Endpoint devices that have been determined as secure, and a list of those that require attention.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Device Activations</td>
<td>Provides a list of all Endpoint devices that have been activated during the time period that you selected.</td>
<td>Area, Area Spline, Bar, Column, Line, Spline</td>
<td>24h, 1 day, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Device Type</td>
<td>Provides a list of the number of Endpoint devices that are PCs or Macs.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Endpoint Status</td>
<td>Shows the number of clean Endpoint devices, and the number of infected Endpoint devices on your sites.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Expired Status</td>
<td>Shows the number of Endpoint devices that are Active, and the number of Endpoint devices that have an Expired state.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Firewall Status</td>
<td>Shows which of your Endpoint Devices have the Firewall option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Identity Shield Status</td>
<td>Shows how many of your Endpoint Devices have the Identity Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrared Status</td>
<td>Shows which of your Endpoint devices have the Enable Webroot Infrared option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation Status</td>
<td>Shows which of your Endpoint devices have the Webroot Secure Anywhere product</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>installed and which ones have had the product uninstalled.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Chart Types and Time Periods for Endpoint Management Reports

<table>
<thead>
<tr>
<th>DATA FIELD</th>
<th>REPORT DESCRIPTION</th>
<th>CHART TYPES</th>
<th>TIME PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed by Policy</td>
<td>Shows how many of your Endpoint devices are being managed by a policy you have created and how many are in an unmanaged state.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Offline Shield Status</td>
<td>Shows how many of your Endpoint devices have the Offline Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System Firewall Status</td>
<td>Shows which of your Endpoint devices have an operating system Firewall option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Unsupported</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chapter 10: Working With Reports
<table>
<thead>
<tr>
<th>DATA FIELD</th>
<th>REPORT DESCRIPTION</th>
<th>CHART TYPES</th>
<th>TIME PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System Language</td>
<td>Shows which Operating system language your Endpoint devices are using.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Operating System Platform</td>
<td>Shows which Operating system platform, from 32 bit, 64 bit, or Unknown, that your Endpoint devices are using.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Phishing Shield Status</td>
<td>Shows how many of your Endpoint devices have the Phishing Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Browser</td>
<td>Shows the Primary Web Browser used by each of your Endpoint devices.</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Realtime Shield Status</td>
<td>Shows how many of your Endpoint devices have the Realtime Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation Status</td>
<td>Shows how many of your Endpoint devices have the Remediation status:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To disable the Remediation status, the <strong>Automatically quarantine previously blocked files</strong> option must be turned off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| **Report Summary** | Provides a number of overall counts that effectively summarize site or deployment information:  
  - Number of active devices  
  - Number of available seats  
    Endpoints currently needing attention  
  - Endpoints which encountered threats (Last ‘n’ days)  
  - Total Threats seen (Last ‘n’ days)  
  - Number of Endpoints Seen (Last ‘n’ days)  
  - Number of Endpoints Not Seen (Last ‘n’ days)  
  - Number of Endpoints Seen (All Time) | Bar, Column, Pie | N/A           |
<table>
<thead>
<tr>
<th>DATA FIELD</th>
<th>REPORT DESCRIPTION</th>
<th>CHART TYPES</th>
<th>TIME PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rootkit Shield Status</td>
<td>Shows how many of your Endpoint devices have the Rootkit Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Scans Status</td>
<td>Shows how many of your Endpoint devices have a Scheduled Scan:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Silent Mode</td>
<td>Shows how many of your Endpoint devices have the Silent Audit option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA FIELD</td>
<td>REPORT DESCRIPTION</td>
<td>CHART TYPES</td>
<td>TIME PERIODS</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Threat Detection History</td>
<td>Shows the history over your selected time period, of all threats that have been detected on your Endpoint devices.</td>
<td>Area, Area Spline, Bar, Column, Line, Spline</td>
<td>24h, 1 day, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days</td>
</tr>
<tr>
<td>USB Shield Status</td>
<td>Shows how many of your Endpoint devices have the USB Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unsupported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Shows how many of your Endpoint devices have been classified as Virtual Machines (VMs).</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td>Web Threat Shield Status</td>
<td>Shows how many of your Endpoint devices have the USB Shield option:</td>
<td>Bar, Column, Pie</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
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.

2. Click the **Reports** tab.

   The system displays the Reports tab with the On-Demand tab active.
3. Click the Scheduled History tab.

The History pane displays with the following information:

- Report Name
- Creation Type
- Recipients
- Sites
- Date Requested
- Status
- Download PDF
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.
2. Click the **Reports** tab.

The system displays the Reports pane with the On-Demand tab active.
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 report displays in a spreadsheet format.
5. Click the Export to CSV button.

![Export to CSV button]

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:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings Overview</td>
<td>501</td>
</tr>
<tr>
<td>Viewing Account Information</td>
<td>503</td>
</tr>
<tr>
<td>Accessing Usage Data</td>
<td>507</td>
</tr>
<tr>
<td>Downloading Usage Data Reports</td>
<td>515</td>
</tr>
<tr>
<td>Setting GSM-Level Data Filters</td>
<td>521</td>
</tr>
<tr>
<td>Creating API Client Credentials</td>
<td>528</td>
</tr>
<tr>
<td>Accessing the My Billing portal</td>
<td>536</td>
</tr>
<tr>
<td>Adding an account on the My Billing portal</td>
<td>538</td>
</tr>
<tr>
<td>Using the My Billing Portal to Pay a Bill</td>
<td>543</td>
</tr>
<tr>
<td>Setting Up Auto Pay</td>
<td>553</td>
</tr>
<tr>
<td>Updating Saved Credit Card Information in the My Billing Portal</td>
<td>556</td>
</tr>
</tbody>
</table>
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.

   ![Management Console with Sites Tab Active](image)

2. Click the Settings tab.

   The system displays the Settings tab, with the Subscriptions tab active.

![Management Console with Settings Tab Active](image)
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.

2. Click the Settings tab.

   The system displays the Settings tab, with the Subscriptions tab active.
Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multilayered 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.
3. Click the **Account Information** tab.

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*. 
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.

2. Click the Settings tab.

   The Settings tab displays with the Subscriptions tab active.
GSM Admin Guide

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.

Subscription Active
(551 days remaining)
Upgrade / Renew

Subscription Active
(551 days remaining)
Upgrade / Renew

Subscription Active
(551 days remaining)
Upgrade / Renew
3. Click the **Account Information** tab.

![Account Information Tab](image)

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.
4. Click the **Usage Console** button.

The My Usage console displays.
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.

![Date Picker](image)

**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 Spreadsheet](image)

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.

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.
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.

2. Click the **Settings** tab.

   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.

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.
3. Click the **Account Information** tab.

![Account Information Tab](image)

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.
4. Click the **Usage Console** button.

The My Usage console displays.
5. After you have used the Date Picker to select the date range, click the **Download CSV Usage as of** link.

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
   - DSNP Enabled
   - DSNP License Type
   - Total DSNP Devices Actual
   - DSNP EST Network Derived Endpoints
   - Total DSNP 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.

2. Click the Settings tab.

   The Settings tab displays, with the Subscription tab active.
## Endpoint Protection
Webroot SecureAnywhere Business Endpoint Protection provides a multi-vector 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)

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 Wi-Fi, roaming users, and groups.

**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.

**Subscription Active**
(551 days remaining)

Upgrade / Renew
3. Click the **Data Filter** tab.

The system displays the Data Filter tab.
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
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.

The system displays a note indicating that your changes have been saved.
6. Click the **OK** button.

![Save Successful dialog box](image)

**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](image)
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.

2. Click the Settings tab.

   The Settings tab displays with the Subscriptions tab active.
3. Click the **API Access** tab.

The API access tab displays.
4. Click the **New** button.

![Image of the Create New Client Credential window](image1.png)

The Create New Client Credential window displays.

![Image of the Create New Client Credential form](image2.png)

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.

![Image of Create New Client Credential window]

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.
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.
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.
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.

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.
3. In the top bar, click **My Billing** and in the dropdown, click **+ Add account**.

![Image of My Usage dashboard](image)

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.

[VERIFY]

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.
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.
4. Review the information presented and click **Continue** to proceed.

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.

6. Once the payment has been processed successfully, the system will display the payment successful screen:
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.
3. Click **Pay** in the bottom section of the My Billing portal next to an individual invoice.
4. Click **Continue** on the Payment Review screen.

![Payment Review Screen]

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.
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

Return
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.
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.
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.
3. The My Billing portal will display billing information, assuming an account has been added. Under Account Information, click Update card.
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:

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Protection Overview</td>
<td>559</td>
</tr>
<tr>
<td>Starting DNS Protection Trials</td>
<td>560</td>
</tr>
<tr>
<td>Step 1 — Activate a Trial</td>
<td>560</td>
</tr>
<tr>
<td>Step 2 — Trial Confirmation and Begin Guided Setup</td>
<td>561</td>
</tr>
<tr>
<td>About the DNS Protection Guided Setup</td>
<td>563</td>
</tr>
<tr>
<td>Step 1 — Select DNS Group Policy</td>
<td>563</td>
</tr>
<tr>
<td>Step 2 — Select Endpoints</td>
<td>564</td>
</tr>
<tr>
<td>Step 3 — Review and Confirm</td>
<td>565</td>
</tr>
</tbody>
</table>
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.

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 with 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 setup 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.
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.
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.
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 ................................................................. 568
- Starting Security Awareness Training Trials .......................................................... 569
  - Activate a Trial .................................................................................................. 569
  - Trial Confirmation and Begin Guided Setup ....................................................... 570
- Guided Setup - Overview ...................................................................................... 570
- About the Security Awareness Training Guided Setup ......................................... 572
  - Step 1 — Verify Domain .................................................................................... 572
  - Step 2 — Import Targets ................................................................................... 573
  - Step 3 — Review Campaigns ............................................................................. 573
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.

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 with 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
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.

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.

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.
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:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Console Overview</td>
<td>576</td>
</tr>
<tr>
<td>Setting Up Your Business Console</td>
<td>579</td>
</tr>
<tr>
<td>About the Business Dashboard Tab</td>
<td>583</td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td>583</td>
</tr>
<tr>
<td>DNS Protection</td>
<td>584</td>
</tr>
<tr>
<td>Security Awareness Training</td>
<td>585</td>
</tr>
<tr>
<td>Dashboard Charts</td>
<td>586</td>
</tr>
<tr>
<td>Viewing and Editing Company Information</td>
<td>588</td>
</tr>
<tr>
<td>Viewing and Editing Advanced Settings</td>
<td>590</td>
</tr>
<tr>
<td>Purchasing Additional Site Seats</td>
<td>594</td>
</tr>
<tr>
<td>DNS Protection Trial</td>
<td>598</td>
</tr>
<tr>
<td>Security Awareness Training Trial</td>
<td>603</td>
</tr>
<tr>
<td>About the Business Console Spotlight Tour</td>
<td>608</td>
</tr>
<tr>
<td>Going to the Endpoint Console</td>
<td>610</td>
</tr>
</tbody>
</table>
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.
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.

The Business information page displays.
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.

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.

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.

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.

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

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 information 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.

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.
3. Click the **Advanced Settings** tab.

The Advanced Settings tab displays.

4. To hide data for endpoints which have not been seen, click the **Edit** button. This information updates daily.
5. To change your console to a multi-site or Managed Service Provider, click the **Convert** button.

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 Console** button.

**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.
3. Click the **Subscriptions** tab.

The Subscriptions tab displays.
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.
Webroot SecureAnywhere

Dashboard | Admins | Groups

Endpoint Protection

Protected

- 0 Installed
- 0 Active (Last 7 days)
- 0 Infected

Dashboard Protection Console

DNS Protection

Secure your DNS connections against cyberattacks, get total visibility into web usage, and enforce acceptable web usage policies to reduce risk.

Start Free Trial

Learn More

Security Awareness Training

Cybercriminals target end users. Ongoing cybersecurity education and training for end users is a must for businesses to stay secure.

Start Free Trial

Learn More
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](image)

   **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.

   CANCEL  CONFIRM

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.
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:
GSM Admin Guide

1. From the Dashboard tab, in the Security Awareness Training area, slick the **Start Free Trial** button.
Chapter 14: Working With the Business Console

![Webroot SecureAnywhere Console](image)

**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.

- [Start Free Trial](#)
- [Learn More](#)

**Security Awareness Training**

Cybercriminals target end users. Ongoing cybersecurity education and training for end users is a must for businesses to stay secure.

- [Start Free Trial](#)
- [Learn More](#)
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

CANCEL  CONFIRM

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
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.

   ![Spotlight Tour button](image)

   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.

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.
3. Scroll down and click the **Go To Endpoint Protection Console** button.
Chapter 15: Global Site Manager Support

For information about support, see the following topic:

| Accessing Technical Support | 614 |

- 613 -
Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Look for the answer in our knowledgebase.
- Look for the answer in our online documentation.
- Enter a help ticket.
- Connect to the Webroot Online Business Forum.
Index

A

about
   business console 19
   Business Console Spotlight Tour 608
   business dashboard tab 583
   DNS Protection 559
   Managed Service Provider Console 16
   Security Awareness Training 568
   Security Awareness Training Guided Setup 572
   spotlight tour 22
accessing
   endpoint protection 36
   report histories 492
   technical support 614
   usage data 507
account information, viewing 503
adding
   admins 154
   admins to sites 154
   groups 188
   sites 73
   web overrides to devices 219
additional site information, viewing 92
admins
   adding 154
   deleting 175
   working with 160
advanced settings, editing 590
advanced settings, viewing 590
agent commands, issuing 283
agent commands, viewing 288
alerts
   creating 418
   deleting 426
   resuming 430
   suspending 430
API client credentials, creating 528

B

blacklist overrides, creating 383
block pages, customizing 411
business console, about 19
business console, setting up 579
Business console, spotlight tour 608
business dashboard tab, about 583
business forum, online 614

C
changing consoles 28
communicating through firewalls 24
company information
  editing 588
  viewing 588
console, selecting 13
consoles
  changing 28
  renaming 32
  switching between 28
copying policies 355
creating
  alerts 418
  API client credentials 528
  blacklist overrides 383
dashboard charts 44
GSM distribution lists 435
policies 296
report templates 477
reports 442
web overrides 369
Webroot accounts 2
whitelist overrides 375
CSV files, downloading 88
customizing block pages 411

D
dashboard charts
  creating 44
  deleting 65
drilling down 58
  editing 51
deactivating site protection 111
deleting
  admins 175
  alerts 426
dashboard charts 65
groups 204
overrides 402
policies 364
web overrides 406
device management overview 209
device summaries
viewing 252
devices
adding web overrides to 219
filtering by site names 261
viewing expired 248
devices between groups
moving 270
devices that have expired, viewing 245
devices that need attention, viewing 239
devices within groups
filtering 267
sorting 275
devices, searching for 258
displaying scan histories 277
DNS Protection
guided setup 563
DNS Protection trial 598
starting 560
DNS Protection, about 559
documentation, online 614
downloading
CSV files 88
reports 495
usage data reports 515
Webroot 149
drilling down dashboard charts 58

E
editing
advanced settings 590
company information 588
dashboard charts 51
groups 198
policies 302
policies applied to devices 214
site details 114
site settings 136
sites 73
web overrides 387
endpoint console, going to 610
endpoint protection, accessing 36
enhanced display, mobile devices 26
entering help tickets 614

F

files
restoring from quarantine 228
files on devices, whitelisting 224
filtering
devices within groups 267
sites 81
filtering devices
site names 261
site status 264
firewalls, communicating through 24

G

generating on-demand reports 454
generating reports 448
Global Site Mangager reports overview 441
going to endpoint console 610
groups
adding 188
deleting 204
editing 198
GSM
distribution lists, creating 435
reports overview 441
sites overview 69
GSM-level data filters, setting 521
guided setup for DNS Protection 563

H

help ticket, entering 614

I

importing
overrides 393
policies manually 359
issuing, agent commands 283
K

knowledgebase 614

M

Managed Service Provider Console, about 16
manually importing policies 359
mobile devices, enhanced display 26
moving
devices between groups 270
multi-site summaries, viewing 96

N

not seen recently
viewing devices 236

O

on-demand reports, generating 454
online business forum 614
online documentation 614
overrides
blacklist, creating 383
deleting 402
importing 393
whitelist, creating 375
overview
device management 209
Global Site Manager reports 441
GSM reports 441
GSM sites 69
settings 501

P

policies
copying 355
creating 296
deleting 364
ingting 302
importing manually 359
renaming 352
policies applied to devices
ingting 214
protected devices, viewing 233
purchasing site seats 594

Q

quarantined files
  restoring 228

R

renaming
  consoles 32
  policies 352
report
  histories, accessing 492
  templates, creating 477
report histories, accessing 492
report templates, creating 477
reports
  creating 442
  downloading 495
  generating 448
requirements, systems 42
restoring files from quarantine 228
resuming
  alerts 430
  site protection 108

S

SAT trial 603
scan histories, displaying 277
searching
  for devices 258
  for sites 86
Security Awareness Training
  guided setup 572
  starting 569
  trial 603
Security Awareness Training, about 568
selecting consoles 13
setting
  GSM-level data filters 521
  site-level data filters 142
setting up, business console 579
settings
  overview 501
site-level data filters, setting 142
site admin permissions, updating 132
site details, editing 114
site names
  filtering by devices 261
site protection, deactivating 111
site protection
  resuming 108
  suspending 108
site seats, purchasing 594
site settings, editing 136
site statuses
  filtering by 264
site summaries, viewing 92
sites
  adding 73
  editing 73
  filtering 81
  searching for 86
  sorting 90
  tagging 122
sorting
  devices within groups 275
  sites 90
spotlight tour, about 22
starting
  DNS Protection Trial 560
  Security Awareness Training Trials 569
suspending
  alerts 430
  site protection 108
switching between consoles 28
system requirements 42

T

tagging sites 122
technical support, accessing 614
trial
  DNS Protection 598
  SAT 603
  Security Awareness Training 603
U

updating site admin permissions 132
usage data reports, downloading 515
usage data, accessing 507

V

viewing
account information 503
additional site information 92
advanced settings 590
company information 588
devices not seen recently 236
devices summaries 252
devices that have expired 245
devices that need attention 239
devices that need attention and are expired 248
multi-site summaries 96
protected devices 233
site summaries 92
web overrides 398
viewing, agent commands 288

W

web overrides
adding to devices 219
creating 369
ingesting 387
viewing 398
web overrides, deleting 406
Webroot accounts, creating 2
Webroot, downloading 149
whitelist overrides, creating 375
whitelisting files on devices 224
working with admins 160