Notices

Webroot Business Products Administration Guide revision Wednesday, September 7, 2022

Information in this document is for the following products:

- Webroot Endpoint Protection
- Webroot DNS Protection
- Webroot Security Awareness Training

One or more patents may cover these products. For more information, please visit https://www.opentext.com/patents.

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.

© 2004-2022 Webroot. All rights reserved.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>3</td>
</tr>
<tr>
<td>Overview</td>
<td>6</td>
</tr>
<tr>
<td>Basic terms</td>
<td>7</td>
</tr>
<tr>
<td>Requirements</td>
<td>9</td>
</tr>
<tr>
<td>Getting started with Endpoint Protection</td>
<td>10</td>
</tr>
<tr>
<td>Step 1: Register/Purchase</td>
<td>10</td>
</tr>
<tr>
<td>Step 2: Setup</td>
<td>11</td>
</tr>
<tr>
<td>Step 3: Deploy</td>
<td>17</td>
</tr>
<tr>
<td>Navigating your Webroot product</td>
<td>21</td>
</tr>
<tr>
<td>Sites (MSPs only)</td>
<td>26</td>
</tr>
<tr>
<td>Entities</td>
<td>33</td>
</tr>
<tr>
<td>Policies</td>
<td>43</td>
</tr>
</tbody>
</table>

## Overview

- Basic terms
- Requirements

## Getting started with Endpoint Protection

- Step 1: Register/Purchase
- Step 2: Setup
  - Creating and activating your account
  - Selecting your Management Console view
  - Setting up two-factor authentication (2FA)
  - Creating a site (MSPs only)
- Step 3: Deploy
  - Creating a custom workstation policy
  - Deploying agents to devices
  - Finding your keycode
- Starting to use Endpoint Protection
- Spotlight tours
- Learn more

## Navigating your Webroot product

- Navigation
- Commonly used functions
- Dashboard

## Sites (MSPs only)

- Viewing all sites (MSPs only)
- Viewing a specific site

## Entities

- Viewing available entities
- Viewing a specific entity
- Managing groups

## Policies

- Endpoint Protection policy best practices
- Viewing available policies
- Adding a new policy
- Copying an existing policy
- Renaming a policy
- Importing an existing policy from another site
- Editing a policy
- Deleting a policy
- Endpoint Protection policy settings
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan policies</td>
<td>53</td>
</tr>
<tr>
<td>Self protection</td>
<td>55</td>
</tr>
<tr>
<td>Heuristics</td>
<td>56</td>
</tr>
<tr>
<td>Realtime shield</td>
<td>57</td>
</tr>
<tr>
<td>Behavior shield</td>
<td>59</td>
</tr>
<tr>
<td>Core system shield</td>
<td>60</td>
</tr>
<tr>
<td>Web threat shield</td>
<td>61</td>
</tr>
<tr>
<td>Identity shield</td>
<td>62</td>
</tr>
<tr>
<td>Firewall</td>
<td>64</td>
</tr>
<tr>
<td>User interface</td>
<td>65</td>
</tr>
<tr>
<td>System optimizer</td>
<td>66</td>
</tr>
<tr>
<td>DNS Protection policy settings</td>
<td>69</td>
</tr>
<tr>
<td>Evasion shield</td>
<td>70</td>
</tr>
<tr>
<td>USB shield</td>
<td>71</td>
</tr>
<tr>
<td><strong>Overrides for Endpoint Protection</strong></td>
<td>72</td>
</tr>
<tr>
<td>Allowing and blocking files</td>
<td>72</td>
</tr>
<tr>
<td>Allowing and blocking websites</td>
<td>74</td>
</tr>
<tr>
<td><strong>Reports</strong></td>
<td>75</td>
</tr>
<tr>
<td>Report types</td>
<td>75</td>
</tr>
<tr>
<td>Device reports</td>
<td>75</td>
</tr>
<tr>
<td>File threat reports</td>
<td>75</td>
</tr>
<tr>
<td>Shield reports</td>
<td>76</td>
</tr>
<tr>
<td>Creating and running a report</td>
<td>76</td>
</tr>
<tr>
<td>Scheduled reports</td>
<td>78</td>
</tr>
<tr>
<td>Creating a scheduled report template</td>
<td>78</td>
</tr>
<tr>
<td>Scheduling a report</td>
<td>79</td>
</tr>
<tr>
<td>Viewing scheduled report history</td>
<td>80</td>
</tr>
<tr>
<td><strong>Deploying agents</strong></td>
<td>81</td>
</tr>
<tr>
<td>Installing on Windows or macOS using the installation wizard</td>
<td>81</td>
</tr>
<tr>
<td>Installing on Windows or macOS from the command line</td>
<td>82</td>
</tr>
<tr>
<td>Installing on Windows using Msiexec</td>
<td>84</td>
</tr>
<tr>
<td>Installing on Windows using group policy</td>
<td>85</td>
</tr>
<tr>
<td>Installing the agent using scripts</td>
<td>85</td>
</tr>
<tr>
<td><strong>Alerts and alert distribution lists</strong></td>
<td>86</td>
</tr>
<tr>
<td>Managing alerts and alert distribution lists</td>
<td>86</td>
</tr>
<tr>
<td>Adding an alert</td>
<td>86</td>
</tr>
<tr>
<td>Adding an alert distribution list</td>
<td>87</td>
</tr>
<tr>
<td><strong>Administration tasks</strong></td>
<td>88</td>
</tr>
<tr>
<td>Viewing available administrators</td>
<td>88</td>
</tr>
<tr>
<td>Adding an administrator</td>
<td>88</td>
</tr>
<tr>
<td>Editing an administrator</td>
<td>89</td>
</tr>
<tr>
<td>Deleting an administrator</td>
<td>90</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>91</td>
</tr>
<tr>
<td>Business view settings</td>
<td>91</td>
</tr>
<tr>
<td>Service provider view settings</td>
<td>94</td>
</tr>
</tbody>
</table>
## DNS Protection

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting started with DNS Protection</td>
<td>97</td>
</tr>
<tr>
<td>Enabling and configuring DNS Protection</td>
<td>97</td>
</tr>
<tr>
<td>Installing network certificates and licenses</td>
<td>100</td>
</tr>
<tr>
<td>Managing DNS Protection policies</td>
<td>101</td>
</tr>
<tr>
<td>Providing DNS Protection by deploying an agent</td>
<td>107</td>
</tr>
<tr>
<td>Using policies to deploy the DNS Protection agent</td>
<td>108</td>
</tr>
<tr>
<td>Providing DNS Protection over a network</td>
<td>108</td>
</tr>
<tr>
<td>Configuring the network</td>
<td>109</td>
</tr>
<tr>
<td>Overrides for DNS Protection</td>
<td>110</td>
</tr>
<tr>
<td>Allowing and blocking websites for DNS Protection</td>
<td>111</td>
</tr>
<tr>
<td>DNS Protection reports</td>
<td>111</td>
</tr>
</tbody>
</table>

## Security Awareness Training

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting started with Security Awareness Training</td>
<td>112</td>
</tr>
<tr>
<td>Enabling Security Awareness Training</td>
<td>112</td>
</tr>
<tr>
<td>Targeting users for training</td>
<td>113</td>
</tr>
<tr>
<td>Managing users</td>
<td>115</td>
</tr>
<tr>
<td>Creating and managing distribution lists</td>
<td>115</td>
</tr>
<tr>
<td>Creating a new campaign</td>
<td>116</td>
</tr>
<tr>
<td>Linking an image from custom templates</td>
<td>120</td>
</tr>
<tr>
<td>Enabling Autopilot</td>
<td>120</td>
</tr>
<tr>
<td>Viewing and managing available campaigns</td>
<td>120</td>
</tr>
<tr>
<td>Viewing available training courses</td>
<td>121</td>
</tr>
<tr>
<td>Viewing a campaign summary report</td>
<td>121</td>
</tr>
<tr>
<td>Interpreting campaign events</td>
<td>123</td>
</tr>
<tr>
<td>Security Awareness Training reports</td>
<td>123</td>
</tr>
</tbody>
</table>
Overview

This Administration Guide details how to use Webroot Endpoint Protection. Users of Webroot DNS Protection and Webroot Security Awareness Training products should also reference this guide as these products work in conjunction with Webroot Endpoint Protection.

Webroot Endpoint Protection is for both individual administrators running a small business, as well as managed service providers (MSPs) who manage the security of their clientele. Large enterprises with offices spread across various locations may want to use this guide as well.

- **Webroot Endpoint Protection** is designed to help keep businesses and their customers safe from viruses, ransomware, phishing, malware, and other cyberattacks. You must install and configure Endpoint Protection before you can use either DNS Protection or Security Awareness Training.

- **Webroot DNS Protection** is a domain filtering service that uses DNS to provide internet usage restrictions both independently and across a network. This product works in conjunction with Webroot Endpoint Protection and is purchased separately. See DNS Protection on page 97.

- **Security Awareness Training** is a hosted program designed to increase understanding and practical implementation of security best practices. The program includes a phishing simulator, training courses, and other tools. This product works in conjunction with Webroot Endpoint Protection and is purchased separately. See Security Awareness Training on page 112.

All business products are accessed from an online portal called the Management Console. The Management Console is a centralized website where you can log in and manage your Webroot business products.

This guide first walks you through installing and configuring Webroot Endpoint Protection, which is a prerequisite for all Webroot products. Specific information for DNS Protection and Security Awareness Training is included in separate chapters at the end.
Basic terms

To get started, here are some basic terms relating specifically to Webroot Endpoint Protection and the cybersecurity industry in general.

Webroot Endpoint Protection terms:

- **Entities** are devices and groups that you work with in Endpoint Protection.
  - **Devices** are the endpoints.
  - **Groups** are organizational units that allow you to manage devices together, for example to apply a specific policy to a group of devices.

- A **site** can represent a department, corporate region, or office location. For managed service providers (MSPs) or larger businesses, sites are a way to summarize sets of endpoints and work with them as groups.

- **Policies** configure the behavior of the agent and include settings for how the scan is performed, the frequency of the scan, how the scan manages threats, and other instructions. Default policies for Endpoint Protection and DNS Protection can be modified to fit your specific needs. An Endpoint Protection unmanaged policy allows you to select and manage your own settings.

- An **Agent** is a small piece of software that runs on your endpoint devices. The agent has a unique identity to the computer it is installed on and performs background security actions on behalf of the administrator.

Industry terms:

- **Malware** is short for malicious software, and refers to dangerous programs or code. Malware attacks are typically launched by clicking an infected attachment in an email and can include any of the following techniques:
  - A **virus** is a program that may replicate itself. It typically infects computer programs by inserting its own code.
  - **Spyware** are programs that spy on computer activity.
  - **Ransomware** are programs that block access to data or threaten to publish data unless a ransom is paid.

- **Social engineering** is a collective name for tricking users into revealing sensitive information. It may include attempts to get users to download a malicious attachment, phishing, baiting, email hacking, and other tactics.
  - **Phishing** is the practice of sending a fraudulent email that appears to be valid with the purpose of getting the recipient to make a purchase or reveal sensitive information. **Spear phishing** is a targeted version of phishing.
  - **Baiting** is the practice of using a false promise to attract a target’s greed or curiosity. Typical strategies are to leave malware-infected flash drives in a conspicuous area, enticing online ads or promises that lead to malicious web sites, or other tactics to encourage someone to download a malware infected file.
  - **Email hacking** is the unauthorized manipulation of an email account or message.

- **Security** best practices for general protection of endpoints include:
• **Password security** is a critical practice to ensure passwords are complex enough to survive hackers’ brute force logins. Passwords should be updated regularly and after any potential security breach. Two factor authentication adds an extra layer of security. Webroot strongly recommends that our users adopt as many of these best practices as possible.

• **Endpoint/device security** are practices that ensure all endpoints are patched and up to date. Webroot strongly recommends that our users keep up-to-date with patches, in accordance with their own security standards.

• **WiFi security** ensures that wireless connectivity is limited to secure networks. Webroot strongly recommends that our users maintain as much WiFi security as possible.

• **Mobile device security** includes the practice of limiting the possibility of loss or theft of mobile devices and ensuring they are only used for company business on secure networks. Webroot strongly recommends that our users protect their mobile devices as much as possible.

• **Physical security** includes increased awareness of portable devices (laptops, tables, phones), as well as the importance of the physical office and its security. Webroot strongly recommends that our users follow physical security best practices as much as possible.

• **Travel security** includes all the security measures mentioned above when outside the office. Webroot strongly recommends that our users follow these best practices as much as possible.
Requirements

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

The system requirements for desktops, servers, VM platforms, and browsers are listed in the Endpoint Protection product page.

System requirements for ports and firewalls are listed in the Knowledge Base.

**DNS Protection** – The DNS Protection agent uses port 443 for most communication and the DNS Protection resolvers support DNS (port 53) and DoH (port 443) for DNS resolution.

For specific firewall configuration settings, see the Knowledge Base.

**Security Awareness Training** requirements include:

- To receive the phishing simulation emails, users must have a valid email in the targeted domain.
- To view the training courses, most modern web browsers are supported.
- Your email server must not block 167.89.85.54 for the phishing simulation and 149.72.237.117 for training emails.
- If you are using Microsoft or Google, you may want to take additional recommended steps to allow emails through by email header as well:
  - [How to allow Webroot Security Awareness Training email in Microsoft Exchange and Office 365](#)
  - [How to allow Webroot Security Awareness Training email in G Suite Gmail](#)
  - [How to allow Webroot Security Awareness Training email in Proofpoint Essentials](#)

These links are to the United States English language site. Country and language options can be changed at the top of the website by clicking a flag to select a country.
Getting started with Endpoint Protection

This section provides the basic steps to start working with Endpoint Protection, DNS Protection, and Security Awareness Training. When configuring your product, your unique network topology and security requirements should always be taken into consideration.

Webroot Endpoint Protection is the foundation for both Webroot DNS Protection and Webroot Security Awareness Training. Getting started with any of these products requires an initial setup of Endpoint Protection.

**Endpoint Protection:**

- **Step 1** – **Register** a trial or **purchase** your Webroot business product. You should have completed this step before receiving this guide.
  - See *Purchasing or registering for a trial* on page 11.
- **Step 2** – Configure Endpoint Protection by creating and activating your Webroot account, setting up two-factor authentication (if desired), and selecting your Management Console view.
  - See *Creating and activating your account* on page 11.
  - See *Setting up two-factor authentication (2FA)* on page 13.
  - See *Selecting your Management Console view* on page 12.
  - See *Creating a site (MSPs only)* on page 13.
- **Step 3** - Deploy the Endpoint Protection agents to devices. Install an agent on each computer you want protected; the agent then registers and reports endpoint activity through the Management Console. Managed service providers also need to set up at least one site.
  - See *Deploying agents to devices* on page 18.

**DNS Protection:**

- Complete Steps 1 – 3 above to register, configure, and deploy Endpoint Protection.
- Enable and install DNS Protection.
  - See *Enabling and configuring DNS Protection* on page 97.
  - See *Installing network certificates and licenses* on page 100.

**Security Awareness Training:**

- Complete Steps 1 – 2 above to register and configure Endpoint Protection.
- Enable Security Awareness Training and target users.
  - See *Enabling Security Awareness Training* on page 112
  - See *Targeting users for training* on page 113.

After you have completed these steps, use the Management Console to work with all your Webroot products.

**Step 1: Register/Purchase**

You can skip this step if you have already purchased the product or registered for a trial.
Purchasing or registering for a trial

2. Under the For Business menu, find the Products section and click Endpoint Protection.
3. Click How to Buy.
   - To purchase the product, click Buy Now and follow the on-screen steps to purchase product. To purchase large subscriptions, contact Sales.
   - To register for a trial, click Start Trial. On the next page, complete the required information and click Get My Free Trial.

Email addresses on ISP or public domains (for example gmail.com) are restricted and cannot be used. Email addresses must be valid company or organization addresses.

Step 2: Setup

This configuration step walks you through the following tasks so that you can start using the Management Console for business:

- Create and activate your account
- Select your Management Console view
- Set up two-factor authentication
- Create a site (MSPs only)

Creating and activating your account

After you have purchased your product or registered for a trial, you will receive a welcome email.

1. Open the email.
2. Click the registration link.
3. Use the temporary password from the email on the registration page.
4. Complete the remainder of the form.
   - Password requirements:
     - Must be at least 9 characters and not more than 30 characters
     - Must contain at least 3 numerics and 6 other characters
     - Cannot be null or empty string
     - Cannot contain special characters < or >
     - Cannot match the Security code
   - Security code requirements:
     - A word or number to be used as an extra security step after you enter your password
     - You are asked to enter two random characters from this code so something easy to remember is recommended
• Case sensitive
• Minimum of six characters
• Cannot be sequential (i.e., 1 2 3 4 5 6)
• Cannot be a common word

Selecting your Management Console view

The Management Console has two configuration options:

• The business view is designed for organizations managing their own security on a single site.
• The service provider (or MSP) view is designed by organizations managing security for multiple companies, businesses, or other organizational units. Each customer is managed using its own site.

The Management Console view is established the first time you access it.

To select your Management Console view:

1. Log in to your Management Console at my.webrootanywhere.com.
2. If this is your first time accessing the console, you are prompted to select a view.
   • Selecting Business sets up a Management Console as a single site, which focuses only on one company’s security.
     • All devices and billing use a single keycode.
     • You can use groups to organize your devices.
     • This view can be changed to the managed service provider view later.
   • Selecting Managed Service Provider sets up a Management Console where you can manage multiple sites for the companies that pay you to provide their cybersecurity.
     • Sites can represent businesses, departments, regions, office locations, or other organizational units under your management.
     • Separate billing and keycodes are available for each site.
     • This view cannot be changed to business view.
3. Click Select for your preferred view.
4. If you selected Business, fill out your company information.
   • Site / Company Name is a unique name for the site or company.
   • Number of Devices is the number of devices to be managed.
   • Company Industry is the industry that the company works within.
   • Company Size is the range of numbers that represents the size of the company.
5. When done, click Select.

Note that if you selected business view, you can change it to service provider view at a later time. If you selected service provider view, you cannot change it to business view.

To change your console view from business view to service provider view:
1. In the navigation pane, go to **Settings**.
2. Click the **Advanced Settings** tab.
3. Under **Convert to Managed Service Provider Console**, click **Convert**.

**Setting up two-factor authentication (2FA)**

Once your account is active, you have the option to set up two-factor authentication (2FA) to help prevent unauthorized access.

Setting up 2FA is optional but highly recommended.

**To set up two-factor authentication (2FA):**

1. On any Android or iOS mobile device or tablet, open or install any authenticator app, such as Google Authenticator, Microsoft Authenticator, LastPass Authenticator, Authy 2-Factor Authentication.
2. Log in to your Management Console at [https://my.webrootanywhere.com](https://my.webrootanywhere.com).
3. Click **Setup 2FA**.
   - If you want to set up 2FA later, click **Skip for now**.
   - To set up 2FA later, go to the **Admins** section in your console. Click your name in the list of admins. In the **Login Settings** box, click **Enable 2FA**.
4. Answer the security questions and click **Continue**.
   - Security codes are case-sensitive.
5. On your mobile device or tablet, open your authenticator app and scan the QR code presented in the Management Console.
   - If you are unable to scan the code, click **Can't scan the QR code** and enter the code from your authenticator app.
   - The code is case-sensitive.
6. A verification code is displayed after you enter the code. Enter the code and click **Verify Code**.
7. Confirm successful verification.
   - If verification fails, enter a new code from your authenticator app. Codes are valid for 30 seconds.
8. Once successful, click **Go to Console** and log in again.

With two-factor authentication, use the code from the authenticator app each time you log in, rather than your personal security code.

If you are setting up a **business** console, go to **Step 3: Deploy** on page 17.

If you are a **managed service provider**, go to **Creating a site (MSPs only)** on page 13 next.

**Creating a site (MSPs only)**

If you are an MSP and have selected the service provider view in the Management Console, you need to create a site to complete your initial configuration.
To create a site:

1. Click Sites List and then click Add Site. The Add Site wizard opens.
2. Complete the site Details.
   - Site / Company Name is a unique name for the site or company.
   - Site Type
     - External Company is an external company that purchases services from you.
     - Internal Site is a site within your own company, such as a location or office.
   - Company Size (external companies only) is the range of numbers that represents the size of the company.
   - Company Industry (external companies only) is the industry that the company works within.
   - Billing Cycle (external companies only) is the billing cycle you define and use as needed for this site (as opposed to the billing cycle associated with Webroot).
   - Billing Date (external companies only) is the month and date for billing, designed and used as needed for this site (as opposed to the billing date associated with Webroot).
   - Distribution List is a comma-separated list of up to ten email addresses that receive scheduled reports. When scheduling a new report, select Send to distribution list of each site so all associated email addresses receive it.
   - Include Global Policies
     - When enabled, all global policies are available for this site.
     - If a global policy is in use and changes, each device using the policy gets the change.
     - Once enabled, this option cannot be changed.
     - When disabled, global policies are not available, and site level policies are used.
   - Include Global Overrides
     - When enabled, global policy overrides are applied to this site. For example, if a site has blocked a particular file and configured it to be a global override, all sites with this option enabled use that override and block that file.
     - When this option is disabled, global overrides from other sites are not applied to this site, and all overrides for this site must be manually configured.
     - Once enabled, this option cannot be changed.
   - Comments (optional) are comments describing the site or company.
   - Tags (optional) are useful labels for filtering your searches.
3. Click Next to continue.
4. In the Admin Permissions step, select the permissions to grant to this site. By default, the account that created the site is given full administrator permissions and is not shown in the list. All other accounts are listed and default to No Access.
- **Admin** allows full access to the site.
- **View Only** allows the ability to only view the site.
- **No Access** denies access to the site.

5. Click **Next** to continue.

6. In the third step of the **Add Site** wizard, configure Endpoint Protection.

- **Keycode Type**
  - Full if you purchased the product.
  - Trial if you registered for a free 30-day trial.

- **Site Seats** are the number of endpoints for the site you are configuring. This setting is not used for billing.

- **Default Endpoint Policy** is used for all new devices installed for this site unless the policy is assigned using inheritance from the group, site, or company. You can modify the policy the device uses after installation. Webroot recommends that you create a copy of this default endpoint policy and modify it according to policy best practices and your specific needs. See **Endpoint Protection policy best practices** on page 43.

  - **Recommended Defaults** is intended for desktops and laptops. User interface and possibly unwanted applications (PUAs) are disabled. The setting to install DNS Protection is disabled in this policy.
  
  - **Recommended DNS Enabled** is the same as **Recommended Defaults**, except the setting to install DNS Protection is enabled.
  
  - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
  
  - **Silent Audit** is based on the **Recommended Defaults** policy, except the remediation function is disabled to minimize production impact. It catches known threats, but not undetermined threats.
    - Use the undetermined threats reports to identify items to add to your block and allow overrides.
    
    - Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.
    
    - Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.

- **Unmanaged**
  - Intended for technical support, troubleshooting, and when no policy management is needed.
  
  - Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
  
  - Should not be used in production.
• **Default Endpoint Policy** is used for all new devices installed for this site unless the policy is assigned using inheritance from the group, site, or company. You can modify the policy the device uses after installation. Webroot recommends that you create a copy of this default endpoint policy and modify it according to policy best practices and your specific needs. See *Endpoint Protection policy best practices* on page 43.

  • **Recommended Defaults** is intended for desktops and laptops. User interface and possibly unwanted applications (PUAs) are disabled. The setting to install DNS Protection is disabled in this policy.

  • **Recommended DNS Enabled** is the same as **Recommended Defaults**, except the setting to install DNS Protection is enabled.

  • **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.

  • **Silent Audit** is based on the **Recommended Defaults** policy, except the remediation function is disabled to minimize production impact. It catches known threats, but not undetermined threats.
    
    1. Use the undetermined threats reports to identify items to add to your block and allow overrides.
    2. Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.
    3. Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.

  • **Unmanaged**
    
    1. Intended for technical support, troubleshooting, and when no policy management is needed.
    2. Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
    3. Should not be used in production.

• **Data Filter**

  • Use data filters to show or hide data displayed in the console.
  
  • For example, if you select **2 Months**, all devices that have not connected for two months are excluded from the data shown for this site.
  
  • Data filtering may improve page loading performance but limits what you see.
  
  • When applying or clearing filters, data may take a few minutes to update depending on the deployment size and the amount of data to display.

  • **Inherit Parent Setting** causes the filter set at the console level to be inherited. This is found under **Settings > Data Filter > Data Filter** drop-down.

7. Click **Next** to continue.

8. If desired, enable **DNS Protection**. See *DNS Protection* on page 97.
9. Click Next to continue.

10. If desired, enable Security Awareness Training. See Security Awareness Training on page 112.

11. Click Save to complete the site configuration and to assign a keycode to the site.

Step 3: Deploy

To complete your initial configuration of Webroot Endpoint Protection, you need to deploy agents to endpoints so they can monitor and provide feedback about potential problems on the devices. We recommend creating a custom workstation policy first so you can apply it easily to all devices going forward.

- Create a custom workstation policy
- Deploy agents to devices
- Learn how to find your keycode

Creating a custom workstation policy

Webroot recommends creating a custom workstation policy using best practices for securing your endpoints. By creating the policy now, it can be easily applied to all endpoints in the future.

The steps below are for an example custom Endpoint Protection policy. Your specific requirements should always take precedence.

To create a custom workstation policy:

1. Make a copy of the Recommended Defaults policy:
   a. In the navigation pane, under Manage, click Policies.
   b. Find the row for Recommended Defaults.
   c. Under Actions, click Copy.

2. Create a custom policy to apply best practices and configure specific requirements:
   - Name is the name of the workstations.
   - Description should be the policy for workstations.
   - For each policy setting below, expand the section and make the recommended changes.
     - Basic Configuration
       - Change Poll interval to 1 Hour (strongly recommended). This reduces the length of time that the agent checks for setting changes or commands. Changing this setting gets you up and running much faster.
     - Scan Settings
       - Set Automatically remove threats found on the learning scan to ON to eliminate threats and improve performance.
       - Set Detect Possibly Unwanted Applications (PUAs) as malicious to ON to identify more malicious code with a small chance of a false positive.
• Behavior Shield
  • Set **Automatically perform the recommended action instead of showing warning messages** to **ON** to have Webroot immediately address an issue rather than delaying for a manual action.

• Core System Shield
  • Set **Prevent any program from modifying the HOSTS file** to **ON** to limit malware’s ability to tamper with the network configuration file.

• User Interface
  • Set **GUI** to **Show** to have the user interface easily available for straightforward troubleshooting.
  • There are no security issues with exposing the user interface.

• Evasion Shield
  • Set **Script Protection** to **Detect and Remediate** to allow immediate action when a threat is identified.

### Deploying agents to devices

Webroot Endpoint Protection protects PCs and Macs by installing a small piece of software, called an agent, that runs on each device. The Webroot agent has a unique identity on each installed computer and performs security actions outside of the user’s control on behalf of the administrator.

If you are an MSP, once you have a site configured, you can deploy the Webroot Endpoint Protection agent to devices and begin protecting them.

- **Endpoint Protection** is cloud-based, so once you install the agent, you do not need to install or update any definition files. Any newly identified threats are updated in the cloud for immediate protection.

- **DNS Protection** filters DNS requests when the devices are on and off the network. It uses a different agent than Endpoint Protection, but the Endpoint Protection agent must be present for the DNS Protection agent to function properly.

See the Knowledge Base for more details.

Make sure the firewall allows traffic to the Webroot cloud. For a list of URLs that need to be allowed, see the Knowledge Base.

### To download and install the agent:

1. Locate the agent installation download links in the Management Console.
   - If you are using **business view**:
     a. Go to **Settings > Downloads** to see the installation file download links.
     b. Click the **Download** link under the operating system used by the target device.
   - If you are using **service provider view**:
a. Click **Sites List**.
b. Find your site in the list and click the name.
c. Open the **Endpoint Protection** tab.
d. Click the **Download Windows .exe**, **Download Windows (.msi)**, or **Download Mac** link to download the appropriate file for the target device.

2. Copy the **Keycode** for your company or for the site for future reference.

3. Move the installation file to the device you are installing the agent on.

4. Install the agent.

After installation is finished, the agent scans for threats. Once the initial scan is complete, the agent checks in with the Management Console and the **Devices** column on the **Entities** page populates. This process typically takes 15 – 30 minutes but can take up to 24 hours.

If DNS Protection is enabled, filtering begins immediately.

### Finding your keycode

You can find your keycode in either of the following ways.

**For business view users:**

1. Click **Settings** from the navigation pane.
2. Select the **Downloads** tab.

**For MSP users:**

1. Click the **Sites List** tab.
2. Click the **Key** button next to the site name.

### Starting to use Endpoint Protection

Congratulations! You have finished setting up Endpoint Protection.

- The agents typically complete their first scans for threats within 15 – 30 minutes and can take up to 24 hours to report into the Management Console. If a device is not seen after 24 hours, contact Customer Support.
- Webroot uses cloud-based threat detection, so you won’t have to download and install any definition files for Windows endpoints. Any new threats that are identified are updated in the cloud for immediate protection.
- Mac agents use specific version files. The version number is appended to the end of the Agent version.
- You can run Endpoint Protection alongside other security products without conflicts.

As the endpoint agents check into the console, the number of devices increases in the **Devices** column. If any threats are detected, the Status changes to **Needs Attention**.
Spotlight tours

To help you get oriented, the Spotlight Tour launches when you first visit the console. The tour includes a brief description about the following:

- Dashboard
- Additional security layers, such as DNS Protection and Security Awareness Training
- Managing Admins
- Groups and Policies
- Overrides, Reports, Alerts, and Settings

To view the Spotlight Tour again in the future:

1. Click the Resources button in the global navigation bar.
2. Select Spotlight Tour from the drop-down menu.

Learn more

Online help is available within every product by clicking the Help button in the global navigation bar.

You can also see more information online:

- The Webroot Support Knowledge Base at answers.webroot.com
- Business Endpoint Protection at The Webroot Community
Navigating your Webroot product

All business products are accessed from an online portal called the Management Console. The Management Console is where you can log in and manage your Webroot business products.

The Management Console URL is https://my.webrootanywhere.com/.

The Management Console has two views, one of which is selected the first time Webroot Endpoint Protection is opened:

- The **business view** enables you to use the Management Console as a single site, focusing only on one company’s cybersecurity.
  - All devices and billing use a single keycode.
  - You can use Groups to organize your devices.
  - This view can be changed to the managed service provider view later.
- The **service provider view** enables you to manage multiple sites for companies that pay you to provide their cybersecurity.
  - Sites can represent businesses, departments, regions, office locations, or other organizational units under your management.
  - Separate billing and keycodes are available for each site.

The Management Console contains a navigation pane and an interactive page, where you see your information and manage your settings. Several icons are at the top of the console that provide links to helpful information.

Navigation

The Management Console **navigation pane** enables you to access the various console pages using navigation links. Collapse and expand the navigation links using < or > at the bottom of the navigation pane.

- The **console switcher** enables you to move between consoles. If you only have one console assigned to you, your console name will be statically displayed. If you work with multiple consoles, a selectable list of console names can be seen in a drop-down list. You can also rename a using the console switcher; any name change is seen by anyone who uses that console.
- The **Sites List (service provider view only)** shows all the sites you can access. View and manage individual sites from this page. See **Sites (MSPs only)** on page 26.
- The **Dashboard** tab provides high-level views of your protection. Because the **business view** is geared towards only a single organization and the **service provider view** is for organizations managing multiple sites, the **Dashboard** view is different for each console view. See **Dashboard** on page 23.
- The **Manage** tab contains three sub-tabs:
  - The **Entities** page is where you can view, organize, and manage all your devices and groups. See **Entities** on page 33.
• **Devices** are the endpoints.
• **Groups** are organizational units that allow you to manage devices together, for example to apply a specific policy to a group of devices.

• The **Policies** page is where you can create and manage your policies. See *Policies* on page 43.
  • A policy configures the behavior of the agent and includes setting for how the scan is performed, the frequency of the scan, and other instructions.
  • Default policies for **Endpoint Protection** and **DNS Protection** can be modified to fit your specific needs.
  • An **Endpoint Protection** unmanaged policy allows you to select and manage your own settings.
• **Overrides** allow you to identify files and URLs that should be allowed or blocked regardless of a policy setting or how Webroot might define the file or URL. See *Overrides for Endpoint Protection* on page 72.

• **DNS Protection (business view only)** shows whether you have **DNS Protection** enabled, and, if so, how it is configured. See *DNS Protection* on page 97.
  • In **service provider view**, **DNS Protection** is configured per site. See *Sites (MSPs only)* on page 26.

• **Security Awareness Training** shows your campaigns, content, users, and settings (business view only) for **Security Awareness Training**. See *Security Awareness Training* on page 112.
  • In **service provider view**, Security Awareness Training settings are available on the Site page.

• **Reports** provide in-depth information about **Endpoint Protection**, **DNS Protection**, and **Security Awareness Training**. You can create reports on demand or schedule them at recurring intervals. See *Reports* on page 75.

• **Alerts** are email notifications that notify you when a threat is detected or when the Webroot agent is installed on a device. An alert distribution list is a list of one or more email addresses that alerts are sent to. See *Alerts and alert distribution lists* on page 86.

• **Admins** shows the administrators, or accounts, that exist in your console. See *Administration tasks* on page 88.

• **Settings** contains configuration sections that vary depending on which view you are using. See *Settings* on page 91.

### Commonly used functions

There are several icons at the top of the screen that provide access to commonly used functions.

• The **Resources** button provides links to announcements, the Spotlight Tours, service status, partner training, documentation, legal, and other product information.

• The **Help** button provides links to help documentation and customer support, where you can open a new support ticket.

• Click your **Login Name** to log out of the console.
Dashboard

The dashboard gives you high-level views of your protection. The dashboard is different for each Management Console view.

- Migrated keycodes when a device is moved from one site to another may cause discrepancies in device counts.

The business view version of the dashboard displays an assortment of statistical tiles and status charts:

Three tiles provide high-level statistics for Endpoint Protection, DNS Protection, and Security Awareness Training. These statistics help you analyze each component briefly.

- **Endpoint Protection** shows high-level statistics for the devices being scanned. Click View Infected to view infected devices.

- **DNS Protection** shows the status of the agents and networks covered by DNS Protection. If it is not enabled, click **Enable SecureAnywhere DNS** to enable **DNS Protection**.

- **Security Awareness Training** shows information about your target users and campaigns.

Buttons and hyperlinks within the tiles allow you to move to specific pages of the console or to enable products that you are not using.

Next to the component tiles, various charts detail activity. You can drill down within chart components by clicking on chart data or machine names.

- Drill down within chart components by clicking on chart data.

- In some cases, you can drill down a second level within the displayed details.
• Click the **Edit** button to modify the chart.
• Click the **Remove** button to delete the chart.

The **service provider view** version of the dashboard displays site summaries and status charts.

The **Dashboard Summary** shows high-level statistics for your sites, seats, and devices.
  • Hover over **Sites** to see a breakdown of the number.
  • Click **Need attention** or **Expiring sites** to go to the **Sites List** page and view details on individual sites.

Below the Dashboard Summary, various charts detail activity.
  • Drill down within chart components by clicking on chart data.
  • In some cases, you can drill down a second level within the displayed details.
  • Click the **Edit** button to modify the chart.
  • Click the **Remove** button to delete the chart.

From this dashboard you can also perform the following actions:
  • Click **Add Chart** to create another chart. Select the options you require. Once the chart is defined, click **Add Chart**.
  • Click **Site Filter** to set or clear the filter that determines which sites are reported in the charts.
    • Choose **All** to display all sites in the charts.
    • Choose **Select sites** to pick which sites should be displayed in the charts.
  • Click **Reset Dashboard** to reset the chart layout, display, and filter back to the default.
• The **Layout** buttons change the chart display to anywhere from one to four charts per row. You can also drag and drop charts to sort them in your desired view.
Sites (MSPs only)

A site can represent a department, corporate region, or office location. For managed service providers (MSPs) or larger businesses, sites are a way to summarize sets of endpoints and work with them as groups.

From the Management Console, you can view available sites, add sites, and manage sites.

To add a site, see Creating a site (MSPs only) on page 13.

Viewing all sites (MSPs only)

Click Sites List to view high-level information about the sites you have access to.

The top of the Sites List page provides the following controls:

- The Sites List table displays all products by default. Click the View drop-down menu to select a list of Products or your Custom view, which you can define by clicking the Customize Columns button.

- Enter text in the Search box to find only those rows that contain the search text.
  - The search checks the entire table, not just the visible rows.
  - Any applied filters will limit the search to only those rows displayed by the filter.
  - The search terms, filters, and sorting preferences that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.

- Add Site creates a new site. See Creating a site (MSPs only) on page 13.

- Export downloads the list of sites as a comma-separated file (.csv), based on the currently applied search and filters.

- Refresh updates the list of sites. Any search and filters you have specified continue to be applied.

- Filters opens the filter panel.
  - A green circle with a number on the Filters button indicates the number of filters currently being applied.
  - Within the filter panel, expand each section to see available filters.
  - Clicking the exclude link next to a filter excludes that filter and selects the rest of the filters in that group.
  - The filters that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.
  - Click Reset to manually clear any selections for a single filter group.
  - Click Reset Filters at the bottom of the panel to clear all filters.

To customize the Sites List table view:
1. Click the **Customize Columns** button.

2. In the **Customize Columns** panel that opens, select the check box next to each data point to include or exclude it in the **Sites List** table.

3. Drag the double lines icon next to each data point to rearrange the order of columns as they appear on the table.

4. Click **Apply** to save your changes.

The Custom view will persist even after you go to another page or log out of the console. To reset the table view back to the default view, in the **Customize Columns** panel, click **Reset to default**.

The **Sites List** table enables you to view and manage your sites as follows:

- **Product subscription status** can be viewed by expanding the blue line. Click the blue arrow at the top of the line to expand and collapse the information.
  - **Active paid** subscriptions are denoted by a blue-filled circle with a white letter.
  - **Active trial** subscriptions are denoted by a white-filled circle with a blue letter.
  - **Expired trial** subscriptions are denoted by a white-filled circle with a blue letter and a blue slash.
  - **Expired paid** subscriptions are denoted by a red-filled circle with a white letter and a white slash.
  - **Inactive** subscriptions are denoted by a gray-filled circle with a black letter.
  - **Suspended** subscriptions are denoted by a black-filled circle with a white letter.

- Click the **Site Name** link to open that site. Whether you can manage or view the site depends on your permissions.

- Click the **Key** button to see the keycode assigned to the site. Click **Copy** to save the code to the clipboard.

- Click the **Actions** button to choose ways to manage the subscription:
  - The **Configure** button enables you to change the settings for the subscription.
  - **Start trial** appears as an option if the site has never had a subscription enabled. Click to start a fully functional, free, 30-day trial.
  - **Upgrade** appears as an option if the subscription is a trial. Click to upgrade to a paid subscription.
  - **Buy** appears if the subscription has expired. Click to renew your subscription.
  - **Re-enable** appears if the subscription has been disabled. Click to re-enable the subscription.
  - The **Legacy Console** button appears for **Endpoint Protection** or **Security Awareness Training** subscriptions that can access the legacy Endpoint Protection console. Click to open the legacy console. Once in the legacy console, click **Back To Sites** to return to the modern interface.

- To **Sort** a column, click its column heading.
• **Rows and paging** controls enable you to view more or less on a page and move between pages.

**Viewing a specific site**

1. Open the Sites List page.
2. Click the Site Name link. The tabbed site page opens.

- Once a site is open, you can use the site switcher at the top to move between sites.
- The **Summary** tab provides a high-level overview of the devices, status, and administrators associated with this site.
  - In the **Devices Requiring Attention** tile, the View Devices link is visible if you have at least one device that needs attention. Click the link to open the Entities page. See Entities on page 33.
  - In the **Admins** tile, click Edit to modify the administrators for the site. See Administration tasks on page 88.
  - In the **Suspend Protection** tile, click Suspend to suspend all protection for the site.
    - This action leaves the agent installed but will not resolve any infections.
    - If you are using DNS Protection, the service will be disabled on the devices, all DNS settings will revert back to the original settings, and filtering will be disabled.
    - DNS traffic will be allowed regardless of policy settings.
    - Suspended sites will continue to be billed like active sites. If you want to stop billing, deactivate the site.
  - In the **Suspend Protection** tile, click Resume to resume suspended protections.
    - Infections will begin resolving
    - If you are using DNS Protection, the service will be enabled and DNS traffic handled according to policy settings.
  - In the **Deactivate Site** tile, click Deactivate Site to deactivate the site keycode.

Sites (MSPs only) 28
• This is a permanent action that cannot be reversed.
• This action sends an uninstall command to all devices using that keycode.
• Deactivated sites will not be billed.
• In the Deactivate Site tile, click Delete Site to delete a deactivated site from the console.
  • This is a permanent action that cannot be reversed.
  • You will no longer be able to view any data for this site.
• The Details tab shows the details of the site as provided when you created the site. Modify any of the settings as needed.
  • Site / Company Name is a unique name for the site or company.
• Site Type
  • External Company is an external company that purchases services from you.
  • Internal Site is a site within your own company, such as a location or office.
• Company Size (external companies only) is the range of numbers that represents the size of the company.
• Company Industry (external companies only) is the industry that the company works within.
• Billing Cycle (external companies only) is the billing cycle you define and use as needed for this site (as opposed to the billing cycle associated with Webroot).
• Billing Date (external companies only) is the month and date for billing, designed and used as needed for this site (as opposed to the billing date associated with Webroot).
• Distribution List is a comma-separated list of up to ten email addresses that receive scheduled reports. When scheduling a new report, select Send to distribution list of each site so all associated email addresses receive it.
• Include Global Policies
  • When enabled, all global policies are available for this site.
  • If a global policy is in use and changes, each device using the policy gets the change.
  • Once enabled, this option cannot be changed.
  • When disabled, global policies are not available, and site level policies are used.
• Include Global Overrides
  • When enabled, global policy overrides are applied to this site. For example, if a site has blocked a particular file and configured it to be a global override, all sites with this option enabled use that override and block that file.
• When this option is disabled, global overrides from other sites are not applied to this site, and all overrides for this site must be manually configured.

• Once enabled, this option cannot be changed.

• Comments (optional) are comments describing the site or company.

• Tags (optional) are useful labels for filtering your searches.

• The Admin Permissions tab identifies who has access to the site.
  • The list of administrators shows who has been granted **Admin, View only, or No Access** to the site.
  • Modify the permissions for each administrator as needed.

• The Endpoint Protection tab shows the subscription status and the default site settings. It also contains download links for the agent installation files.

• Site Seats are the number of endpoints for the site you are configuring. This setting is not used for billing.

**Default Endpoint Policy** is used for all new devices installed for this site unless the policy is assigned using inheritance from the group, site, or company. You can modify the policy the device uses after installation. Webroot recommends that you create a copy of this default endpoint policy and modify it according to policy best practices and your specific needs. See **Endpoint Protection policy best practices** on page 43.

• **Recommended Defaults** is intended for desktops and laptops. User interface and possibly unwanted applications (PUAs) are disabled. The setting to install DNS Protection is disabled in this policy.

• **Recommended DNS Enabled** is the same as **Recommended Defaults**, except the setting to install DNS Protection is enabled.

• **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimizes impact on the server.

• **Silent Audit** is based on the **Recommended Defaults** policy, except the remediation function is disabled to minimize production impact. It catches known threats, but not undetermined threats.
  • Use the undetermined threats reports to identify items to add to your block and allow overrides.
  • Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.
  • Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.

• **Unmanaged**
  • Intended for technical support, troubleshooting, and when no policy management is needed.
• Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
• Should not be used in production.

• **Data Filter**
  • Use data filters to show or hide data displayed in the console.
  • For example, if you select 2 Months, all devices that have not connected for two months are excluded from the data shown for this site.
  • Data filtering may improve page loading performance but limits what you see.
  • When applying or clearing filters, data may take a few minutes to update depending on the deployment size and the amount of data to display.
  • **Inherit Parent Setting** causes the filter set at the console level to be inherited. This is found under Settings > Data Filter > Data Filter drop-down.
  • **Site Seats** are the number of endpoints for the site you are configuring. This setting is not used for billing.
  • **Default Endpoint Policy** is used for all new devices installed for this site unless the policy is assigned using inheritance from the group, site, or company. You can modify the policy the device uses after installation. Webroot recommends that you create a copy of this default endpoint policy and modify it according to policy best practices and your specific needs. See *Endpoint Protection policy best practices* on page 43.

• **Recommended Defaults** is intended for desktops and laptops. User interface and possibly unwanted applications (PUAs) are disabled. The setting to install DNS Protection is disabled in this policy.

• **Recommended DNS Enabled** is the same as **Recommended Defaults**, except the setting to install DNS Protection is enabled.

• **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.

• **Silent Audit** is based on the **Recommended Defaults** policy, except the remediation function is disabled to minimize production impact. It catches known threats, but not undetermined threats.
  • Use the undetermined threats reports to identify items to add to your block and allow overrides.
  • Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.
  • Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.

• **Unmanaged**
• Intended for technical support, troubleshooting, and when no policy management is needed.
• Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
• Should not be used in production.

• **Data Filter**
  • Use data filters to show or hide data displayed in the console.
  • For example, if you select 2 Months, all devices that have not connected for two months are excluded from the data shown for this site.
  • Data filtering may improve page loading performance but limits what you see.
  • When applying or clearing filters, data may take a few minutes to update depending on the deployment size and the amount of data to display.
  • **Inherit Parent Setting** causes the filter set at the console level to be inherited. This is found under Settings > Data Filter > Data Filter drop-down.

• Go to **Endpoint Protection Console** opens the Endpoint Protection legacy console. Once in the legacy console, click **Back To Sites** to return to the modern interface.
• The **Download Software** section contains links to the agent installation files. These links and files are specific to the site and keycode. See **Deploying agents** on page 81.

• The **DNS Protection** tab is where you enable or disable DNS Protection.
  • Once enabled, you can configure DNS Protection configuration for the site. See **DNS Protection** on page 97.

• The **Security Awareness Training** tab is where you enable or disable Security Awareness Training.
  • Once enabled, you can target the users you want to include in training by identifying a domain that contains the email addresses you want to include.
  • You can use Azure Active Directory integration or a manual process to identify the domain. See **Security Awareness Training** on page 112.
Entities

Entities are devices and groups that you work with in Endpoint Protection.

- **Devices** are the endpoints.
- **Groups** are organizational units that allow you to manage devices together, for example to apply a specific policy to a group of devices.

Viewing available entities

The **Entities** tab is where you view, organize, and manage your devices and groups.

To view your available entities, go to **Manage > Entities**.

- In **business view** the entities table contains a list of groups and devices within each group.
- In **service provider view** the entities table contains a list of sites. You can expand a site and see the groups and devices.

When you select a site or group, you can see high-level information for each device.

- You can quickly see if the device is protected.
- A device that has not checked in within the last seven days will be identified as not recently seen.
- Deactivated devices appear in a separate **Deactivated Devices** group.
  - To reactivate a device and restore it to its former group, select the check box next to the device name, then click **Reactivate**.
- When looking at devices within a group, the icon next to the device **Name** identifies the type of device as follows:
  - **Windows** icon ENUM denotes a Windows desktop.
  - **Server** icon 11 denotes a Windows server.
  - **Apple** icon ♦ denotes a macOS desktop.
  - **Location** icon ♦ denotes an IP address.
- The icon next to the policy name identifies the **Policy** assigned to the device. Hovering over this icon displays the full policy name and assignment method.
  - **Monitor** icon ⓔ signifies the policy is assigned directly to the device.
  - **Building** icon  Affero signifies the policy is assigned to the device using a site policy.
  - **Connected boxes** icon ʝ signifies the policy is assigned to the device using a group policy.
  - **Circle with letter l** icon ● signifies there is more than one policy assigned to the device.
- When you hover over a device name, a pencil icon нстру appears.
  - By default, Endpoint Protection displays the hostname of a device. Click **Edit** нстру to change the assigned device name to one that is more intuitive or user-friendly.
• This changes the device name on the **Entities** page and all other locations that it appears within the console.

The following actions are available from the top of the **Entities** page:

• In **service provider view**, enter text in the **Search** box to find only those rows that contain the search text.
  
  • The search checks the entire table, not just the visible rows.
  
  • The search terms, filters, and sorting preferences that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.

• Click **Agent Commands** to perform specific functions on the selected device(s). Agent commands are executed based on the polling interval defined in the policy assigned to the device.
  
  • Windows and Apple icons denote which commands apply to which operating systems.
  
  • The **Most Popular** commands appear at the top of the list.
    
    • **Scan** starts a scan of the selected devices when the command is received.
    
    • **Clean Up** starts a scan of the device when the command is received and quarantines any malicious files. After the scan is complete, you can see the results in the **Scan History**.
    
    • **Uninstall** removes the agent from the selected devices. If the device is using an Endpoint Protection policy configured to install DNS Protection, DNS Protection will be installed the next time the device checks in.
    
    • **Deactivate Device** uninstalls the agent from the selected devices. This option also moves the devices from the assigned group to the deactivated group.
    
    • **Change Keycode** changes the keycode on the selected devices to the keycode entered.
    
    • **Reverify All Files and Processes** verifies all files and processes on the selected devices when the next scan runs. This option is useful when creating manual overrides and enforcing those changes to the selected devices.
    
    • **Restore File** restores a file that has been quarantined, for example, a false positive for a file that you want to allow.
    
    • **Run Customer Support Script** runs scripts provided by customer support to update devices or remove infections.
    
    • **System Optimizer** starts the System Optimizer process when the command is received.
    
    • **Reset** is a tool used by technical support in specific situations. Do not run this command without assistance.
    
    • **Restart Device** sends a reboot command to the selected devices. Once the device receives the command, the reboot happens immediately, without notification to the user.
• Click **View All Commands** to see all possible commands. Use the **Search** box to find specific commands.
  
  • **Allow Application** allows an application to run on the selected devices.
  
  • **Allow ProcessesBlocked by Firewall** allows communication for all processes that are blocked by the Firewall policy setting. See **Firewall** on page 64.
  
  • **Change Scan Time** changes the time of day that the agent runs a daily scan on the selected devices.
  
  • **Clear Log Files** erases current log files to free up space on the selected devices.
  
  • **Consider All Items as Good / Allow All Denied Applications** tags all detected files on the selected devices as safe and resets all applications that were previously blocked so that they can run.
  
  • **Customer Support Diagnostics** runs a utility to gather information about an infected device and sends the results to the Webroot support team.
  
  • **Deny Application** blocks an application from running on the selected devices.
  
  • **Disable Proxy Settings** disables any proxy settings that were enabled on the selected devices. The device will no longer be able to communicate with the internet if its only internet access is through the proxy server.
  
  • **Lock Endpoint** locks the selected devices by activating the login screen. The user must enter a user name and password to log back in.
  
  • **Log Off** ends the session and logs the user out of the current account.
  
  • **Protect an Application** adds an extra layer of security to a specified application running on the selected devices.
  
  • **Remove Password Protection** removes an uninstall password for Webroot if one was configured during installation.
  
  • **Reset Desktop Wallpaper** resets the desktop wallpaper to its default settings. You must restart the device to apply these changes. This option is useful if the device was recently infected with malware that changed the desktop wallpaper settings.
  
  • **Reset Screen Saver** resets the screen saver to its default settings. You must restart the device to apply these changes. This option is useful if the device was recently infected with malware that changed the screen saver settings.
  
  • **Reset System Policies** resets system policies in the registry that might prevent the use of administrative Windows functions, such as opening the Task Manager. This option is useful if the device was recently infected with malware that changed these settings.
  
  • **Restart in Safe Mode with Networking** restarts the selected devices in Safe Mode with Networking.
  
  • **Scan a Folder** scans a specified folder on the selected devices.
  
  • **Shutdown** shuts down the selected devices when they next report in.
• **Stop Untrusted Processes** stops and terminates any processes that are not allowed. This option is useful if a regular scan did not completely remove all traces of suspected malware.

• **Unprotect an Application** removes the extra security from a previously protected application.
  
  • The **Command Log** displays the history of the agent commands that have been run. You can export the command log to a CSV (comma-separated) file.

• **Move** moves selected devices to another group.
  
  • If you are using the **service provider view**, the groups must be within the same site.
  
  • Specify if the devices are going to update to the policy assigned to the group they are moving to or keep the policy they are currently using.

• **Change Policy** changes the policy assigned to the selected devices.

• **Filters** opens the filter panel.
  
  • A green circle with a number on the **Filters** button indicates the number of filters currently being applied.
  
  • Within the filter panel, expand each section to see available filters.
  
  • Clicking the **exclude** link to the right of a filter excludes that filter and selects the rest of the filters in that group.
  
  • The filters that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.

  • Click **Reset** to manually clear any selections for a single filter group.

  • Click **Reset Filters** at the bottom of the panel to clear all filters.

**To customize the Entities table view:**

1. Click the **Customize Columns** button.

2. In the **Customize Columns** panel that opens, select the check box next to each data point to include or exclude it in the **Entities** table.

3. Drag the double lines icon next to each data point to rearrange the order of columns as they appear on the table.

4. Click **Apply** to save your changes.

The Custom view will persist even after you go to another page or log out of the console. To reset the table view back to the default view, in the **Customize Columns** panel, click **Reset to default**.

The following actions are available from the top of the list of **Sites & Groups** (in **service provider view**) or **Groups** (in **business view**):

• Click the **Create Group** button to create a new group for the selected site. In **service provider view**, you must select a site to create a new group.
• Click the **Delete Group** button to delete the selected group. You must specify a new group to move any devices that exist in the group you are deleting.

• Click the **Edit Group** button to modify the name of the group or the policy assigned to the group.

• Click the **Install Devices into this Group** button to deploy a new device directly into the selected group. Follow the on-screen prompts to download and run the installer. The devices will automatically inherit the policies assigned to the selected group.
Viewing a specific entity

1. Go to Manage > Entities.
   - In service provider view, select the site that contains the device you want to manage.
   - In business view, select the group that contains the device you want to manage.

2. Find the device in the list and click the device Name link. A tabbed page opens.

   The top of the page has general commands:

   - By default, Endpoint Protection displays the hostname of a device. Click Edit next to the device name to change the assigned device name to one that is more intuitive or user-friendly.
     - This changes the device name on the Entities page and all other locations that it appears within the console.
     - To change the device name back to its original name, click Revert to original host name.
   - Click Agent Commands are executed based on the polling interval defined in the policy assigned to the device.
     - Windows and Apple icons denote which commands apply to specific operating systems.
     - The Most Popular commands appear at the top of the list.
       - Scan starts a scan of the selected devices when the command is received.
       - Clean Up starts a scan of the device when the command is received and quarantines any malicious files. After the scan is complete, you can see the results in the Scan History.
       - Uninstall removes the agent from the selected devices. If the device is using an Endpoint Protection policy configured to install DNS Protection, DNS Protection will be installed the next time the device checks in.
       - Deactivate Device uninstalls the agent from the selected devices. This option also moves the devices from the assigned group to the deactivated group.
       - Change Keycode changes the keycode on the selected devices to the keycode entered.
       - Reverify All Files and Processes verifies all files and processes on the selected devices when the next scan runs. This option is useful when creating manual overrides and enforcing those changes to the selected devices.
       - Restore File restores a file that has been quarantined, for example, a false positive for a file that you want to allow.
       - Run Customer Support Script runs scripts provided by customer support to update devices or remove infections.
- **System Optimizer** starts the System Optimizer process when the command is received.
- **Reset** is a tool used by technical support in specific situations. Do not run this command without assistance.
- **Restart Device** sends a reboot command to the selected devices. Once the device receives the command, the reboot happens immediately, without notification to the user.
- Click **View All Commands** to see all possible commands. Use the search box to find specific commands.
  - **Allow Application** allows an application to run on the selected devices.
  - **Allow Processes Blocked by Firewall** allows communication for all processes that are blocked by the Firewall policy setting. See Firewall.
  - **Change Scan Time** changes the time of day that the agent runs a daily scan on the selected devices.
  - **Clear Log Files** erases current log files to free up space on the selected devices.
  - **Consider All Items as Good / Allow All Denied Applications** tags all detected files on the selected devices as safe and resets all applications that were previously blocked so that they can run.
  - **Customer Support Diagnostics** runs a utility to gather information about an infected device and sends the results to the Webroot support team.
  - **Deny Application** blocks an application from running on the selected devices.
  - **Disable Proxy Settings** disables any proxy settings that were enabled on the selected devices. The device will no longer be able to communicate with the internet if its only internet access is through the proxy server.
  - **Lock Endpoint** locks the selected devices by activating the login screen. The user must enter a user name and password to log back in.
  - **Log Off** ends the session and logs the user out of the current account.
  - **Protect an Application** adds an extra layer of security to a specified application running on the selected devices.
  - **Remove Password Protection** removes an uninstall password for Webroot if one was configured during installation.
  - **Reset Desktop Wallpaper** resets the desktop wallpaper to its default settings. You must restart the device to apply these changes. This option is useful if the device was recently infected with malware that changed the desktop wallpaper settings.
  - **Reset Screen Saver** resets the screen saver to its default settings. You must restart the device to apply these changes. This option is useful if the device was recently infected with malware that changed the screen saver.
settings.

- **Reset System Policies** resets system policies in the registry that might prevent the use of administrative Windows functions, such as opening the Task Manager. This option is useful if the device was recently infected with malware that changed these settings.

- **Restart in Safe Mode with Networking** restarts the selected devices in Safe Mode with Networking.

- **Scan a Folder** scans a specified folder on the selected devices.

- **Shutdown** shuts down the selected devices when they next report in.

- **Stop Untrusted Processes** stops and terminates any processes that are not allowed. This option is useful if a regular scan did not completely remove all traces of suspected malware.

- **Unprotect an Application** removes the extra security from a previously protected application.

- The **Command Log** displays the history of the agent commands that have been run. You can export the command log to a CSV (comma-separated) file.

- **Change Policy** changes the policy assigned to the selected devices.

The tabs at the top of the screen provide information about the device.

- The **Summary** tab provides high-level information for the device.

- The **Threats Detected** tab contains two tables that identify infections.
  
  - **File Threat Detections** shows any infected files. Click a file name to see details on the file and the malware detected.
  
  - **Evasion Shield Script Detections** shows any infected scripts. Click a script name to see details of the infected script.

- Click **Actions** to modify specific files as follows:
  
  - **Add File to Allow List** enables you to create a new allow list entry for the selected file.
  
  - **Restore from Quarantine** removes the file from quarantine and restores it to its original location.

- The **Executable Detection Note** is displayed if threats have been detected and remediated according to policy settings.
  
  - The status is automatically updated to Protected after the next scheduled scan.
  
  - To scan the device immediately, click **Clean up** to quarantine any malicious files.
  
  - After the scan is complete, view the results in the **Scan History**.
- **Web Threat Shield Blocks** displays the URLs that have been blocked by Web Threat Shield.
  - Click **Actions** and select **Add URL to Allow List** to create a new entry in the Web Overrides list.
- **DNS Protection** (if DNS Protection is enabled) displays information about blocked domains, users, and reasons for blocking.
  - Click **Actions** and select **Add URL to Allow List** to create a new entry in the Web Overrides list.
- **Scan History** displays the history of scans for the device. If a threat was detected during a scan, expand the table row to see details.
  - Click the **File name** to see details on the file and the malware detected.
  - Click **Actions** to modify specific files as follows:
    - **Add File to Allow List** specifies this file as an allowed file.
    - **Restore from Quarantine** removes the file from quarantine and restores it to its original location.

### Managing groups

Groups are organizational units that allow you to manage devices together, for example to apply a specific policy to a group of devices.

When the Endpoint Protection agent is deployed, all devices are automatically assigned to a default group. You can make customized groups to manage separate devices in different ways.

The following actions are available from the top of the list of **Sites & Groups** (in service provider view) or **Groups** (in business view):

* Click the **Create Group** button to create a new group for the selected site. In service provider view, you must select a site to create a new group.

* Click the **Delete Group** button to delete the selected group. You must specify a new group to move any devices that exist in the group you are deleting.

* Click the **Edit Group** button to modify the name of the group or the policy assigned to the group.

* Click the **Install Devices into this Group** button to deploy a new device directly into the selected group. Follow the on-screen prompts to download and run the installer. The devices will automatically inherit the policies assigned to the selected group.

**To move a device into a new group:**

1. Click **Entities** in the navigation pane.
2. On the **Entities** page, select one or more devices to move to a new group.
3. Click **Move**.
• If you are using the service provider view, the groups must be within the same site.
• Specify if the devices are going to update to the policy assigned to the group they are moving to or keep the policy they are currently using.
Policies

**Policies** configure the behavior of the agent and include settings for how the scan is performed, the frequency of the scan, how the scan manages threats, and other instructions. Default policies for Endpoint Protection and DNS Protection can be modified to fit your specific needs. An Endpoint Protection unmanaged policy allows you to select and manage your own settings.

**Global** policies can be edited, copied, or deleted. The **Can Edit** icon 🌐 beside the policy **Name** indicates that a policy can be edited.

**System** policies can be viewed or copied.

We recommend reviewing our suggested best practices when setting up policies. See *Endpoint Protection policy best practices* on page 43.

**Endpoint Protection policy best practices**

Default Endpoint Protection policies should be considered generic baseline policies that need to be modified to meet the specific needs of the groups the policy will be assigned to. Your specific requirements should always prevail.

Consider the following when determining which policies you need to create:

- **Naming.** Make sure your policy names can be easily understood. When you have multiple policies, use a descriptive name that quickly identifies the type of settings that are enabled in the policy. You might want to also specify any applications or web sites that are blocked.

- **Logical groups and special circumstances.** What are your main logical groups? Do some need to be broken down into smaller groups? What functions require different policy settings? Do you need to have different policies for machines you want to allow to be shut down versus those that cannot be shut down? Do you need to block applications or websites for some of your logical groups?

- **People and computers.** You may need different policies for executives and non-executives, workstations and servers, different departments, or even different roles within a department.

The following are best practice suggestions for different types of entities. Again, your specific requirements should always prevail.

- **Workstations.** When creating a policy for workstations, make a copy of the **Recommended Defaults** policy and then modify each of the following settings:
  
  - **Basic Configuration**
    
    - Change **Poll interval** to **1 Hour** (strongly recommended). This reduces the length of time that the agent checks for setting changes or commands.
  
  - **Scan Settings**
    
    - Turning **Automatically remove threats found on the learning scan** to **On** removes found threats during the learning scan and creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.
• Turn the Detect Possibly Unwanted Applications (PUAs) as malicious option On to start detecting attacks that come through adware, browser add-ons, and other utilities. This setting may create more false positives, but it also identifies more malicious code.

• Behavior Shield

• Turn Automatically perform the recommended action instead of showing warning messages to On to immediately take action to address an issue rather than delaying until someone manually takes action after reviewing a warning.

• Core System Shield

• Turn Prevent any program from modifying the HOSTS file to On to limit the ability to tamper with this file.

• User Interface

• Change GUI to Show. There are no security issues with exposing the user interface and having it available allows for easier troubleshooting.

• Evasion Shield

• At a minimum, set Script Protection to Detect and Report so threats are identified and then reported upon. Because it is easier to remove a block at the time of detection, rather than to fix a threat that has gotten through, this option should ideally be set to Detect and RemEDIATE so immediate action is taken when a threat is identified.

• Servers. When creating a policy for servers that will not be directly accessed, make a copy of the Recommended Server Defaults policy and then modify each of the following settings:

• Basic Configuration

• Turn Allow SecureAnywhere to be shut down manually to Off. Disabling this option provides more protection due to inadvertent shutdowns. This is especially important if multiple people have access to the server.

• Change Poll interval to 1 Hour (strongly recommended). This reduces the length of time that the agent checks for setting changes or commands.

• Scan Settings

• Turning Automatically remove threats found on the learning scan to On removes found threats during the learning scan and creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.

• Turn the Detect Possibly Unwanted Applications (PUAs) as malicious option On to start detecting attacks that come through adware, browser add-ons, and other utilities. This setting may create more false positives, but it also identifies more malicious code.

• Realtime Shield

• Turn the Scan files when written or modified option to On. This option prevents the injection of threats, especially back door threats, such as a malicious macro
embedded in what appears to be a safe document file.

- **Behavior Shield**
  - Turn **Automatically perform the recommended action instead of showing warning messages** to **On** to immediately take action to address an issue rather than delaying until someone manually takes action after reviewing a warning.

- **Evasion Shield**
  - At a minimum, set **Script Protection** to **Detect and Report** so threats are identified and then reported upon. Because it is easier to remove a block at the time of detection, rather than to fix a threat that has gotten through, this option should ideally be set to **Detect and Remediate** so immediate action is taken when a threat is identified.

- **RDS/Terminal Servers.** When creating a policy for servers that will be directly accessed, make a copy of the **Recommended Server Defaults** policy and modify each of the following settings:
  - **Basic Configuration**
    - Turn **Show a system tray icon** to **Off**. Disabling this option provides more protection due to Endpoint Protection being accessed from the system tray. This is especially important if multiple people have access to the server.
    - Turn **Show SecureAnywhere in the Start Menu** to **Off**. Disabling this option provides more protection from Endpoint Protection being accessed from the **Start** menu. This is especially important if multiple people have access to the server.
    - Turn **Show SecureAnywhere in Add/Remove Programs** to **Off**. Disabling this option provides more protection from Endpoint Protection being uninstalled. This is especially important if multiple people have access to the server.
    - Turn **Allow SecureAnywhere to be shut down manually** to **Off**. Disabling this option provides more protection from Endpoint Protection being inadvertently shut down. This is especially important if multiple people have access to the server.
    - Change **Poll interval** to **1 Hour** (strongly recommended). This reduces the length of time that the agent checks for setting changes or commands.
  - **Scan Settings**
    - Turn **Scan archived files** to **On**. This provides more thorough protection of the server.
    - Turning **Automatically remove threats found on the learning scan** to **On** removes found threats during the learning scan and creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.
    - Turn the **Detect Possibly Unwanted Applications (PUAs) as malicious** option **On** to start detecting attacks that come through adware, browser add-ons, and other utilities. This setting may create more false positives, but it also identifies more malicious code.

- **Realtime Shield**
• Turn the Scan files when written or modified option to On. This option prevents
  the injection of threats, especially back door threats, such as a malicious macro
  embedded in what appears to be a safe document file.

• Behavior Shield

  • Turn Automatically perform the recommended action instead of showing
    warning messages to On to immediately take action to address an issue rather
    than delaying until someone manually takes action after reviewing a warning.

• Evasion Shield

  • At a minimum, set Script Protection to Detect and Report so threats are
    identified and then reported upon. Because it is easier to remove a block at the
    time of detection, rather than to fix a threat that has gotten through, this option
    should ideally be set to Detect and RemEDIATE so immediate action is taken when
    a threat is identified.

**Viewing available policies**

Open Manage > Policies to work with Endpoint Protection and DNS Protection policies.

If you are an MSP working in the service provider view, policies you create are global and can be
used across all your sites.

Global policies can be edited, copied, or deleted. The Can Edit icon 🗝 beside the policy Name
indicates that a policy can be edited.

System policies can be viewed or copied.

The following action buttons are available from the top of the Policies page on both the Endpoint
Protection and DNS Protection tabs:

  • Click Add Policy to create a new policy. See Adding a new policy on page 47.
  • Click Import Policy to import an existing policy from another site or console. See Importing an
    existing policy from another site on page 48.

The tabs at the top of the screen are categorized by type of policy.

  • The Endpoint Protection tab displays the default Endpoint Protection system policies and
    any global policies that have been created:

    • Recommended Defaults is intended for desktops and laptops. User interface and
      possibly unwanted applications (PUAs) are disabled. The setting to install DNS
      Protection is disabled in this policy.
    
    • Recommended DNS Enabled is the same as Recommended Defaults, except the
      setting to install DNS Protection is enabled.
    
    • Recommended Server Defaults is intended for server environments. It focuses on
      resource utilization and minimal impact on the server.
    
    • Silent Audit is based on the Recommended Defaults policy, except the remediation
      function is disabled to minimize production impact. It catches known threats, but not
      undetermined threats.
• All visible aspects of Webroot (user interface, system tray icon, add/remove programs entry) are hidden.

• Use the undetermined threats reports to identify items to add to your block and allow overrides.

• Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.

• Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.

• The Unmanaged policy does not have any specific settings (except whether to show the user interface) and the settings of previous policies.

  • Intended for technical support, troubleshooting, and when no policy management is needed.
  • Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
  • Should not be used in production.

• The DNS Protection tab displays a switch to turn on DNS Protection, if it hasn’t been enabled already. If DNS Protection has been enabled, it displays the default DNS Protection policies and any global policies that have been created:

  • DNS High Protection blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
  • DNS Medium Protection blocks all security categories as well as Human Resource Protections and Questionable/Legal content.

  • See Managing DNS Protection policies on page 101.

The following functions are available from within the Policies page on both the Endpoint Protection and DNS Protection tabs:

• Click the policy Name link to view or edit it. Only user-created policies are editable.

• In the Actions column, you can manage the policy as follows:

  • View enables you to review the policy settings assigned to a default policy.
  • Copy copies an existing policy. See Copying an existing policy on page 48.
  • Edit enables you to edit the policy settings assigned to a policy you created, copied, or imported. See Editing a policy on page 49.
  • Delete deletes a user-created policy. See Deleting a policy on page 49.

• Policy Usage metrics are displayed at the bottom of the page.

### Adding a new policy

1. Open Manage > Policies.

2. From either the Endpoint Protection or DNS Protection tab, click Add Policy.
• Provide a unique **Name** and a **Description**. Each field is limited to 50 alphanumeric characters.
• Click the caret to expand and contract the settings in each section.
• Modify any of the default policy settings as desired.

3. When done, click **Save**.

**Copying an existing policy**

1. Open **Manage > Policies**.
2. From either the **Endpoint Protection** or **DNS Protection** tab, select the policy you want to copy.
3. Under **Actions**, click **Copy**.
   • Provide a unique **Name** and a **Description**. Each field is limited to 50 alphanumeric characters.
   • Click the caret to expand and contract the settings in each section.
   • The new policy is based on the settings of the policy you copied.
   • Modify the policy settings as desired.
4. When done, click **Save**.

**Renaming a policy**

1. Open **Manage > Policies**.
2. From either the **Endpoint Protection** or **DNS Protection** tab, open the policy you want to copy.
3. In the **Name** field, enter the new name.
   • The new name must be unique.
4. When done, click **Save**.

**Importing an existing policy from another site**

You can import an existing policy from another site or from another console.

1. Open **Manage > Policies**.
2. Click **Import Policy**.
   • In the **Import** dialog, specify the site or console that contains the policy you want to import.
   • Select the Policy you want to import. Only the policies on the selected site will be listed.
   • You cannot import a policy if the name of the policy you are importing already exists.
3. Click **Import Policy**.

Once the policy has been imported, you can edit it as needed.
Editing a policy
You can edit policies that you created, copied, or imported. Default policies cannot be edited.

1. Open Manage > Policies.
2. From either the Endpoint Protection or DNS Protection tab, click on a policy Name link.
3. Modify the Name, Description, or any of the Policy Settings.
   - Click the caret to expand and contract the settings in each section.
   - Save each section as you go.
4. When each section is complete, click Save.

Deleting a policy
You can delete any policy that you have created, copied, or imported. You cannot delete a default policy. Any devices using the policy you want to delete must be reassigned to another policy.

1. Open Manage > Policies.
2. From either the Endpoint Protection or DNS Protection tab, select the policy that you want to delete.
3. Under Actions, click Delete.
4. When prompted, select the Replacement Policy. Any devices using the policy that you are deleting will be assigned to the Replacement Policy.
5. Click Delete Policy.

Endpoint Protection policy settings
Review Endpoint Protection policy best practices on page 43 when determining how best to set up your policies.

To review or modify Endpoint Protection Policies:

1. Open Manage > Policies.
2. From the Endpoint Protection tab, select the policy you want to view or modify.
   - When viewing a policy, the Policy Usage is displayed at the bottom of the page.
   - All policies can be used when working with Windows devices. Policies marked with an asterisk (*) apply to Apple devices as well.
**Basic configuration**

Basic configuration policies control the behavior of the agent.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a SecureAnywhere shortcut on the desktop</td>
<td>An Endpoint Protection desktop shortcut is available on the desktop.</td>
<td>The Endpoint Protection shortcut is not available on the desktop.</td>
</tr>
<tr>
<td>Show a system tray icon</td>
<td>An Endpoint Protection icon is available in the system tray.</td>
<td>The Endpoint Protection icon is not in the system tray.</td>
</tr>
<tr>
<td>Show a splash screen on bootup</td>
<td>An Endpoint Protection screen displays during system boot.</td>
<td>The Endpoint Protection screen is not displayed during system boot.</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Start Menu</td>
<td>Endpoint Protection is available in the <strong>Start</strong> menu.</td>
<td>Endpoint Protection is not available in the <strong>Start</strong> menu.</td>
</tr>
<tr>
<td>Show SecureAnywhere in Add/Remove Programs</td>
<td>Endpoint Protection is listed in <strong>Add/Remove Programs</strong> or <strong>Programs and Features</strong>, depending on your Windows version.</td>
<td>Endpoint Protection is not listed in <strong>Add/Remove Programs</strong> or <strong>Programs and Features</strong>.</td>
</tr>
<tr>
<td>Show SecureAnywhere in Windows Action Center</td>
<td>Endpoint Protection is listed in the <strong>Action Center</strong>, under Virus &amp; threat protection.</td>
<td>Endpoint Protection is not listed in the <strong>Action Center</strong>.</td>
</tr>
<tr>
<td>Automatically download and apply updates*</td>
<td>The agent automatically downloads and applies updates without notifying the end-user.</td>
<td>The agent does not automatically download or apply updates.</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources*</td>
<td>Non-scan functionality is run in the background to save CPU resources.</td>
<td>All Endpoint Protection functionality is run in the foreground.</td>
</tr>
<tr>
<td>Favor low disk usage over verbose logging</td>
<td>The Endpoint Protection log only maintains the last four log items.</td>
<td>The Endpoint Protection log maintains all log items.</td>
</tr>
<tr>
<td>Lower resource usage when intensive applications or games are detected*</td>
<td>Endpoint Protection functions are postponed while the end-user is gaming, watching videos, or using other intensive applications.</td>
<td>Endpoint Protection functions are not postponed.</td>
</tr>
<tr>
<td>Allow SecureAnywhere to be shut down manually*</td>
<td>Endpoint Protection can be shut down from the system tray icon.</td>
<td>The option to shut down Endpoint Protection from the system tray is not available.</td>
</tr>
<tr>
<td>Policy Setting</td>
<td>When the policy setting is enabled</td>
<td>When the policy setting is disabled</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Force non-critical notifications into the background</td>
<td>Endpoint Protection only displays critical messages in the system tray. Information messages are hidden.</td>
<td>Both critical and information messages are displayed in the system tray.</td>
</tr>
<tr>
<td>Fade out warning messages automatically*</td>
<td>Endpoint Protection messages in the system tray automatically disappear after a few seconds.</td>
<td>The end-user must close Endpoint Protection messages in the system tray.</td>
</tr>
<tr>
<td>Store Execution History details</td>
<td>Data is stored in the <strong>Execution History</strong> log.</td>
<td>No data is stored in the <strong>Execution History</strong> log.</td>
</tr>
<tr>
<td>Poll interval*</td>
<td>This specifies how often the agent will check for updates. The default setting is 24 hours. The recommended setting is 15 minutes.</td>
<td></td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
Scan schedule

Scan schedule policies control when scans occur.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Scheduled Scans*</td>
<td>Scans are performed using the defined schedule.</td>
<td>Scans run once a day at the approximate time you installed the software. That is, the scan runs at install time and then roughly 24 hours thereafter.</td>
</tr>
<tr>
<td>Scan Frequency*</td>
<td>This option specifies how often the device is scanned.</td>
<td></td>
</tr>
<tr>
<td>Time*</td>
<td>This option specifies when the device is scanned. You can select a time range or a specific time.</td>
<td></td>
</tr>
<tr>
<td>Scan on bootup if the computer is off at the</td>
<td>Missed scans occur within an hour after bootup.</td>
<td>Missed scans are skipped.</td>
</tr>
<tr>
<td>scheduled time*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hide the scan progress window during scheduled</td>
<td>Scans run silently in the background.</td>
<td>Scan progress is displayed in a window.</td>
</tr>
<tr>
<td>scans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Only notify me if an infection is found during a</td>
<td>An alert is shown only if a threat is found.</td>
<td>A status window displays when the scan completes, even if there are no threats found.</td>
</tr>
<tr>
<td>scheduled scan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do not perform scheduled scans when on battery</td>
<td>Scans are skipped when using only battery power.</td>
<td>Scans occur using any power source.</td>
</tr>
<tr>
<td>power*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do not perform scheduled scans when a full screen</td>
<td>Scans are skipped when a full screen application, such as a movie or game, is being used.</td>
<td>Scans occur when full screen applications are being used.</td>
</tr>
<tr>
<td>application or game is open*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Randomize the time of scheduled scans up to one</td>
<td>Scans run within an hour of the scheduled time.</td>
<td>Scans run at the scheduled time. If you need to schedule scans for an exact time, turn this setting off.</td>
</tr>
<tr>
<td>hour for distributed scanning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform a scheduled Quick Scan instead of a Deep</td>
<td>Only quick scans of memory are performed.</td>
<td>Scans check the entire machine.</td>
</tr>
<tr>
<td>Scan</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
Scan policies

Scan policies control what is scanned and how the scans occur.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Realtime Master Boot Record (MBR) Scanning</td>
<td>The master boot record, which loads before the operating system, is scanned.</td>
<td>The master boot record is not scanned.</td>
</tr>
<tr>
<td>Enable Enhanced Rootkit Detection</td>
<td>Endpoint Protection scans for rootkits and other malicious software hidden on disk or in protected system areas. These are created by spyware developers to avoid detection and removal.</td>
<td>Endpoint Protection does not scan for rootkits and other malicious software.</td>
</tr>
<tr>
<td>Enable &quot;right-click&quot; scanning in Windows Explorer</td>
<td>A right-click menu is available in Windows Explorer to immediately scan a file.</td>
<td>The right-click menu is not available.</td>
</tr>
<tr>
<td>Update the currently scanned folder immediately as scanned</td>
<td>The Endpoint Protection display updates each time a file is scanned.</td>
<td>The Endpoint Protection display is updated periodically, showing all files scanned since the last update.</td>
</tr>
<tr>
<td>Favor low memory usage over fast scanning</td>
<td>Less memory is used to run a scan, but the scan might run slower.</td>
<td>More memory is used to run a scan, so the scan runs faster.</td>
</tr>
<tr>
<td>Favor low CPU usage over fast scanning</td>
<td>Less processor usage is used to run a scan, but the scan might run slower.</td>
<td>More processor usage is used to run a scan, so the scan runs faster.</td>
</tr>
<tr>
<td>Show the &quot;Authenticating Files&quot; popup when a new file is scanned on execution</td>
<td>A dialog box showing the scan appears when an end-user executes a file for the first time.</td>
<td>Nothing appears when an end-user executes a file for the first time, however, the file will still be scanned.</td>
</tr>
<tr>
<td>Save non-executable file details to scan logs</td>
<td>All file data is saved to the scan log, resulting in a larger log file.</td>
<td>Only executable file data is saved to the scan log, resulting in a smaller log file.</td>
</tr>
<tr>
<td>Policy Setting</td>
<td>When the policy setting is enabled</td>
<td>When the policy setting is disabled</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scan archived files*</td>
<td>The file types .zip, .rar, .cab, and 7-zip are scanned.</td>
<td>The file types .zip, .rar, .cab, and 7-zip are not scanned.</td>
</tr>
<tr>
<td>Automatically reboot during cleanup without prompting</td>
<td>A reboot automatically occurs after a cleanup to remove malware.</td>
<td>The user is prompted to reboot after a cleanup to remove malware.</td>
</tr>
<tr>
<td>Never reboot during malware cleanup</td>
<td>The machine does not reboot during a cleanup to remove malware.</td>
<td>A reboot is not prevented during a cleanup to remove malware. The cleanup may be incomplete.</td>
</tr>
<tr>
<td>Automatically remove threats found during background scans</td>
<td>Threats found during background scans are automatically sent to quarantine.</td>
<td>Threats are sent to quarantine during scheduled scans.</td>
</tr>
<tr>
<td>Automatically remove threats found on the learning scan</td>
<td>Threats found during the first scan of the device are automatically sent to quarantine.</td>
<td>Threats are sent to quarantine during scheduled scans.</td>
</tr>
<tr>
<td>Enable Enhanced Support</td>
<td>Logs are sent to Webroot customer support.</td>
<td>No logs are sent to Webroot.</td>
</tr>
<tr>
<td>Show Infected Scan Results</td>
<td>Logs are sent to Webroot customer support.</td>
<td>No logs are sent to Webroot.</td>
</tr>
<tr>
<td>Detect Possibly Unwanted Applications (PUAs) as malicious</td>
<td>Possibly unwanted applications (programs that may not be malicious but could be unwanted or create security concerns, such as adware or toolbars) are blocked from installation or removed, if possible, from the machine. The recommended setting is <strong>On</strong>.</td>
<td>These applications are not blocked or removed.</td>
</tr>
<tr>
<td>Allow files to be submitted for threat research</td>
<td>Files are sent to Webroot for threat research.</td>
<td>No files are sent to Webroot.</td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
## Self protection

Self protection policies control how the agent protects itself.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable self-protection response cloaking</td>
<td>If another product is attempting to interfere with Endpoint Protection, Endpoint Protection attempts to protect itself by launching a protective scan.</td>
<td>Endpoint Protection does not attempt to protect itself.</td>
</tr>
</tbody>
</table>

### Self-protection Level

This option specifies the self-protection detection level.

- **Minimum** protects the Endpoint Protection settings. Use this level if you have other cybersecurity products installed.
- **Medium** prevents other programs from disabling Endpoint Protection. Use this level for maximum compatibility with other cybersecurity products.
- **Maximum** protects the Endpoint Protection processes. This is the recommended level if you have no other cybersecurity products.
Heuristics

The collection of heuristics policies control behavior for the local drive, internet, network, CD/DVD drives, and when the machine is offline. You should not modify any of the default settings without guidance from technical support.
# Realtime shield

Realtime shield policies control blocking and alerting behaviors around suspicious or known threats.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realtime Shield Enabled*</td>
<td>Suspicious or known threats are immediately blocked.</td>
<td>Threats are not blocked, and the user is not notified. Protection is diminished when this setting is disabled.</td>
</tr>
<tr>
<td>Enable Predictive Offline Protection</td>
<td>A threat definition file is downloaded to the device and used for protection when the device is offline.</td>
<td>The threat definition file is not downloaded and the device is not protected when it is offline.</td>
</tr>
<tr>
<td>Remember actions on blocked files</td>
<td>Endpoint Protection remembers how an end-user responded to an alert (allow or block) and does not prompt the user again about the same file.</td>
<td>Endpoint Protection alerts every time for the same file.</td>
</tr>
<tr>
<td>Automatically quarantine previously blocked files*</td>
<td>Files that have been previously quarantined are quarantined automatically, for example if the file was downloaded a second time.</td>
<td>Files that have been previously quarantined are not quarantined during the next scheduled scan.</td>
</tr>
<tr>
<td>Automatically block files when detected on execution*</td>
<td>Suspicious or known threats are automatically blocked when executed.</td>
<td>Suspicious or known threats alert for the end-user to allow or block.</td>
</tr>
<tr>
<td>Scan files when written or modified*</td>
<td>New or modified files are scanned when they are saved or installed.</td>
<td>New or modified files are not scanned when they are saved or installed.</td>
</tr>
<tr>
<td>Block threats automatically if no user is logged in*</td>
<td>Suspicious or known threats are automatically blocked from execution when no user is logged in.</td>
<td>Files are not blocked from execution when no user is logged in.</td>
</tr>
<tr>
<td>Show realtime event warnings</td>
<td>An alert is displayed as soon as suspicious activity is detected.</td>
<td>No alerts are displayed.</td>
</tr>
<tr>
<td>Show realtime block modal alerts</td>
<td>An alert is displayed as soon as malware is detected. Enable this option if any of your heuristics options are set to <strong>Warn when new programs execute that are not known good.</strong></td>
<td>No alerts are displayed.</td>
</tr>
<tr>
<td>Show realtime block notifications</td>
<td>A tray notification alert is displayed as soon as malware is detected.</td>
<td>No tray notification alerts are displayed.</td>
</tr>
</tbody>
</table>

---

Policies 57
* applies to Apple devices as well.
**Behavior shield**

Behavior shield policies control the analysis of applications and processes running on devices.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Shield Enabled</td>
<td>The end-user is prompted for suspicious threats, and known threats are immediately blocked and quarantined.</td>
<td>Threats are not alerted or blocked.</td>
</tr>
<tr>
<td>Assess the intent of new programs before allowing them to execute</td>
<td>Endpoint Protection examines a program’s activity before allowing it to run. If it appears safe, Endpoint Protection allows it to launch and continues to monitor its activity.</td>
<td>Programs are not examined.</td>
</tr>
<tr>
<td>Enable advanced behavior interpretation to identify complex threats</td>
<td>Endpoint Protection examines a program to determine its intent. For example, malware may modify a registry entry and then send an email.</td>
<td>Programs are not examined.</td>
</tr>
<tr>
<td>Track the behavior of untrusted programs for advanced threat removal</td>
<td>Endpoint Protection examines only those programs that have not been classified as safe or a threat.</td>
<td>Programs are not examined.</td>
</tr>
<tr>
<td>Automatically perform the recommended action instead of showing warning messages</td>
<td>Endpoint Protection determines if a threat should be allowed or blocked.</td>
<td>The end-user is prompted to determine if a threat should be allowed or blocked.</td>
</tr>
<tr>
<td>Warn if untrusted programs attempt low-level system modifications when offline</td>
<td>Programs that are not classified alert if the program tries to make changes to a device when the device is offline.</td>
<td>Programs are not alerted if they try to make changes to a device when the device is offline.</td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
# Core system shield

Core system shield policies monitor and protect the computer system structures.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core System Shield Enabled</td>
<td>The end-user is prompted for suspicious threats, and known threats are immediately blocked and quarantined.</td>
<td>Threats are not alerted or blocked.</td>
</tr>
<tr>
<td>Assess system modifications before they are allowed to take place</td>
<td>Endpoint Protection intercepts any attempt to make system changes, for example a new service installation.</td>
<td>Endpoint Protection does not intercept any attempt to make system changes.</td>
</tr>
<tr>
<td>Detect and repair broken system components</td>
<td>Endpoint Protection detects and restores corrupted components or files.</td>
<td>Endpoint Protection does not detect or restore corrupted components or files.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying kernel memory</td>
<td>Programs that are not classified are blocked from changing kernel memory.</td>
<td>Programs that are not classified are not blocked from changing kernel memory.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying system processes</td>
<td>Programs that are not classified are blocked from changing system processes.</td>
<td>Programs that are not classified are not blocked from changing system processes.</td>
</tr>
<tr>
<td>Verify the integrity of the LSP chain and other system structures</td>
<td>Endpoint Protection monitors the Layered Service Provider (LSP) chain and other system structures for corruption.</td>
<td>Endpoint Protection does not monitor the Layered Service Provider (LSP) chain and other system structures for corruption.</td>
</tr>
<tr>
<td>Prevent any program from modifying the HOSTS file*</td>
<td>Endpoint Protection alerts when an attempt is made to modify the hosts file.</td>
<td>Endpoint Protection does not alert when an attempt is made to modify the hosts file.</td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
# Web threat shield

Web threat shield policies control browsing and search engine behavior.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Web Shield*</td>
<td>Endpoint Protection monitors internet browsing and alerts on suspicious sites. It also analyzes search engine result links.</td>
<td>There is no internet browsing monitoring or search engine analysis.</td>
</tr>
<tr>
<td>Activate browser extension</td>
<td>Users see icons when viewing web search results. They can hover over an icon to get a review of the site's reputation.</td>
<td>Users do not see reputation icons when viewing web search results.</td>
</tr>
<tr>
<td>Block malicious websites*</td>
<td>Endpoint Protection blocks known malicious websites.</td>
<td>No websites are blocked.</td>
</tr>
<tr>
<td>Enable real time antiphishing*</td>
<td>Endpoint Protection alerts on zero-day phishing sites, which are sites that have never been seen before and are not classified.</td>
<td>Zero-day phishing sites are not alerted.</td>
</tr>
<tr>
<td>Show safety ratings when using search engines*</td>
<td>Search engine result links are identified as trusted sites (green checkmark) or suspicious sites (red X).</td>
<td>Search engine results are not identified.</td>
</tr>
<tr>
<td>Enable web filtering driver</td>
<td>Additional protections against malicious connections, including when browser extensions are disabled, are used.</td>
<td>Additional protections against malicious connections are not used.</td>
</tr>
<tr>
<td>Suppress the user's ability to bypass blocked websites*</td>
<td>End-users are not able to bypass the block page presented when a known malicious website is detected.</td>
<td>A user can bypass the block page.</td>
</tr>
<tr>
<td>Suppress the user's ability to request website reviews*</td>
<td>End-users are not able to submit a website review request from the block page presented when a known malicious website is detected.</td>
<td>A user can request a website review from a block page.</td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
# Identity shield

Identity shield policies control how data is protected during online transactions.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Shield Enabled*</td>
<td>Endpoint Protection monitors online transactions. On macOS, this option controls the <strong>Secure Keyboard Entry Mode</strong> setting.</td>
<td>Online transactions are not monitored.</td>
</tr>
<tr>
<td>Look for identity threats online</td>
<td>Endpoint Protection analyzes and alerts when it detects malicious content.</td>
<td>Content is not analyzed.</td>
</tr>
<tr>
<td>Verify websites when visited to determine legitimacy</td>
<td>Endpoint Protection analyzes and alerts when a website's IP address has been redirected or has been identified as a threat.</td>
<td>Website IP addresses are not analyzed.</td>
</tr>
<tr>
<td>Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks</td>
<td>Endpoint Protection analyzes and alerts when a website is redirected, such as a man-in-the-middle attack.</td>
<td>Website redirects are not analyzed.</td>
</tr>
<tr>
<td>Block websites from creating high risk tracking information</td>
<td>Endpoint Protection blocks third-party cookies if they originate from a malicious site.</td>
<td>Third-party cookies are not blocked.</td>
</tr>
<tr>
<td>Prevent programs from accessing protected credentials</td>
<td>Endpoint Protection blocks programs from accessing credentials, for example, when you enter your user name and password or choose to save credentials for a website.</td>
<td>Programs are not blocked from accessing credentials.</td>
</tr>
<tr>
<td>Warn before blocking untrusted programs from accessing protected data</td>
<td>Endpoint Protection alerts when programs attempt to access data.</td>
<td>Programs accessing data are not alerted.</td>
</tr>
<tr>
<td>Policy Setting</td>
<td>When the policy setting is enabled</td>
<td>When the policy setting is disabled</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow trusted screen capture programs access to</td>
<td>Trusted screen capture programs function, regardless of the content displayed on screen.</td>
<td>Screen capture programs are not able to access protected screen contents.</td>
</tr>
<tr>
<td>protected screen contents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Identity Shield compatibility mode</td>
<td>Certain applications that Identity Shield might normally block are allowed to run. For example, you may need to enable this option if devices have issues running applications. Even when enabled, the Identity Shield core functionality still protects the device.</td>
<td>Identity Shield continues to block all applications that it identifies as malicious.</td>
</tr>
<tr>
<td>Enable keylogging protection in non-Latin systems</td>
<td>Endpoint Protection protects devices using non-Latin languages, such as Japanese and Chinese, from keyloggers.</td>
<td>There is no protection from keyloggers.</td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
# Firewall

The firewall policies control the Endpoint Protection firewall.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>The Endpoint Protection firewall monitors outgoing traffic and the Windows firewall monitors incoming traffic. The Endpoint Protection firewall looks for untrusted processes trying to connect to the internet and steal personal information. If the firewall detects suspicious traffic, the end-user is alerted.</td>
<td>Outgoing traffic is not monitored.</td>
</tr>
</tbody>
</table>

Firewall level

This option specifies the level of firewall protection.

- **Default Allow** allows all processes to connect to the internet, unless explicitly blocked by the agent.
- **Warn unknown and infected** looks for any new, untrusted processes connecting to the internet or if the device is infected.
- **Warn unknown** looks for any new, untrusted process connecting to the internet.
- **Default Block** looks for any process connecting to the internet, unless explicitly blocked by the agent.

<table>
<thead>
<tr>
<th>Show firewall management warnings</th>
<th>A warning is displayed when Windows firewall is off.</th>
<th>No warnings are displayed when Windows firewall is off.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show firewall process warnings</td>
<td>Firewall level warnings are displayed.</td>
<td>No warnings are displayed and the process is allowed.</td>
</tr>
</tbody>
</table>

* applies to Apple devices as well.
User interface

The user interface policy controls whether Endpoint Protection is available on end-user Windows or Apple devices.

- When set to **Show**, users can see and access Endpoint Protection on their device. They can perform a scan, but they cannot manage the agent or modify any settings.
- When set to **Hide**, users are prompted to contact their administrator if they attempt to access Endpoint Protection. On macOS, this option hides the system tray icon as well.
System optimizer policies control general Windows cleanup tasks, such as removing unnecessary files and data.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage System Optimizer centrally</td>
<td>Displays the System Optimizer controls.</td>
<td>System Optimizer controls are not displayed.</td>
</tr>
<tr>
<td>Days of week</td>
<td>System Optimizer runs on the selected day of the week.</td>
<td>System Optimizer does not run on the selected day of the week.</td>
</tr>
<tr>
<td>Run at specific time of day - hour</td>
<td>This option specifies the hour of the day when you want the System Optimizer to run.</td>
<td></td>
</tr>
<tr>
<td>Run at specific time of day - minute</td>
<td>This option specifies the minute of the selected hour when you want the System Optimizer to run.</td>
<td></td>
</tr>
<tr>
<td>Run on bootup if the system was off at the scheduled time</td>
<td>System Optimizer runs at bootup if the machine was off at the scheduled run time.</td>
<td>System Optimizer only runs at the scheduled run time.</td>
</tr>
<tr>
<td>Enable Windows Explorer right click secure file erasing</td>
<td>Windows Explorer has a right-click menu option allowing a user to erase a file, without the file being sent to the Recycle Bin.</td>
<td>This option is not displayed in Windows Explorer.</td>
</tr>
<tr>
<td>Recycle Bin</td>
<td>All files in the Recycle Bin are deleted when System Optimizer runs.</td>
<td>Nothing is deleted from the Recycle Bin.</td>
</tr>
<tr>
<td>Recent document history</td>
<td>The history of recently opened files is deleted from the Start menu. Note that only the history is deleted, not the actual files.</td>
<td>Nothing is deleted from the Start menu.</td>
</tr>
<tr>
<td>Start Menu click history</td>
<td>The history of shortcuts to recently opened programs is deleted from the Start menu. Note that only the history is deleted, not the actual shortcuts.</td>
<td>No history is deleted.</td>
</tr>
<tr>
<td>Run history</td>
<td>The history of commands is deleted from the Run dialog box. A reboot may be needed to clear all commands.</td>
<td>No history is deleted.</td>
</tr>
<tr>
<td>Search history</td>
<td>The computer search history is deleted. Note that only the history is deleted, not any files or programs that were found during a search.</td>
<td>No history is deleted.</td>
</tr>
<tr>
<td>Start Menu order history</td>
<td>When a reboot occurs, any changes to the Start menu order is reverted, and the menu will be in the default alphabetical order.</td>
<td>The Start menu order is not reverted.</td>
</tr>
<tr>
<td>Policy Setting</td>
<td>When the policy setting is enabled</td>
<td>When the policy setting is disabled</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Clipboard contents</td>
<td>Content on the Clipboard is cleared.</td>
<td>No clipboard content is cleared.</td>
</tr>
<tr>
<td>Windows Temporary folder</td>
<td>All data in the Windows temporary folder, usually <code>C:\Windows\Temp\</code>, is deleted, unless the file is in use.</td>
<td>No data is deleted.</td>
</tr>
<tr>
<td>System Temporary folder</td>
<td>All data in the system temporary folder is deleted unless the file is in use. The location of this folder varies depending on the Windows version.</td>
<td>No data is deleted.</td>
</tr>
<tr>
<td>Windows Update Temporary folder</td>
<td>All data in the Windows Update temporary folder is deleted, unless the file is in use.</td>
<td>No data is deleted.</td>
</tr>
<tr>
<td>Windows Registry Streams</td>
<td>The Windows registry change history is deleted. Note that only the history is deleted, not any registry changes or keys.</td>
<td>No history is deleted.</td>
</tr>
<tr>
<td>Default logon user history</td>
<td>The registry key that stores the last user logged into the computer is deleted. Users have to enter their user name each time the computer is booted. This setting does not apply to computers using the default Welcome screen.</td>
<td>The registry key is not deleted.</td>
</tr>
<tr>
<td>Memory dump files</td>
<td>All memory dump files, which are automatically created for certain Windows errors, are deleted.</td>
<td>No dump files are deleted.</td>
</tr>
<tr>
<td>CD burning storage folder</td>
<td>All Windows project files, created when the Windows built-in function is used to copy files to a CD, are deleted unless the file is in use. The location of this folder varies depending on the Windows version.</td>
<td>No project files are deleted.</td>
</tr>
<tr>
<td>Flash Cookies</td>
<td>Adobe Flash data are deleted. Note that these are not actual cookies controlled by browser cookie privacy controls.</td>
<td>No data is deleted.</td>
</tr>
<tr>
<td>Address bar history</td>
<td>The history of visited websites is deleted from Internet Explorer.</td>
<td>No history is deleted.</td>
</tr>
<tr>
<td>Cookies</td>
<td>All cookies are deleted. Users must re-enter passwords, shopping cart items, and other entries stored in cookies.</td>
<td>No cookies are deleted.</td>
</tr>
<tr>
<td>Policy Setting</td>
<td>When the policy setting is enabled</td>
<td>When the policy setting is disabled</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Temporary internet Files</td>
<td>All temporary browser files are deleted.</td>
<td>No files are deleted.</td>
</tr>
<tr>
<td>URL history</td>
<td>The history pane in Internet Explorer is cleared.</td>
<td>No entries in the history pane are deleted.</td>
</tr>
<tr>
<td>Setup Log</td>
<td>Internet Explorer update log files are deleted.</td>
<td>No files are deleted.</td>
</tr>
<tr>
<td>Microsoft Download Folder</td>
<td>Files in the Internet Explorer download folder are deleted.</td>
<td>No files are deleted.</td>
</tr>
<tr>
<td>MediaPlayer Bar History</td>
<td>The list of audio and video files recently opened with the media player in Internet Explorer is deleted. Note that the files themselves are not deleted, just the list of recently opened files.</td>
<td>The list of recently opened files is not deleted.</td>
</tr>
<tr>
<td>Autocomplete form information</td>
<td>Internet Explorer AutoComplete data are deleted. Users must re-enter data on forms.</td>
<td>No data is deleted.</td>
</tr>
<tr>
<td>Clean index.dat</td>
<td>When a reboot occurs, the index.dat file that stores Windows information, such as web addresses, search queries, and recently opened files, is deleted.</td>
<td>The index.dat file is not deleted.</td>
</tr>
<tr>
<td>Control the level of security to apply when removing files</td>
<td>This option specifies how you want to handle deleted files.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Normal</strong>—Files are deleted, bypassing the Recycle Bin. A recovery utility may be able to restore these files. This option is the fastest cleanup process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong>—Files are deleted, bypassing the Recycle Bin, and the location where the data was stored will be overwritten three times. A recovery utility has a harder time restoring these files. This cleanup process takes longer than a normal cleanup process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum</strong>—Files are deleted, bypassing the Recycle Bin, and the location where the data was stored will be overwritten seven times, including space around the data location. These files are the most difficult for a recovery utility to restore. This is the slowest cleanup process.</td>
<td></td>
</tr>
</tbody>
</table>
**DNS Protection policy settings**

The DNS Protection policy controls whether DNS Protection is installed with the agent.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install DNS Protection</td>
<td>DNS Protection is installed with the Endpoint Protection agent.</td>
<td>DNS Protection is not installed.</td>
</tr>
</tbody>
</table>
Evasion shield

Evasion shield policies detect and block evasive attacks, including file-based, fileless, obfuscated, or encrypted attacks. It requires agents running version 9.0.29.00 or later.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
</table>
| Script Protection | This setting specifies the level of script protection.  
  • Off disables script protection.  
  • Detect and Report detects and alerts when script threats are discovered.  
  • Detect and Remediate detects, alerts, and quarantines script threats when discovered. | |
USB shield

These settings control detection and access on USB storage devices. It requires agents running version 9.0.31.84 or later.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable USB Shield</td>
<td>Suspicious or known threats on a USB attached storage device are immediately blocked if executed.</td>
<td>Threats are not blocked in real-time. USB drives can still be scanned using the context menu option Scan with Webroot.</td>
</tr>
<tr>
<td>Block USB Storage Devices</td>
<td>USB attached storage devices are blocked for all read, write, and execute access. End users receive a message when a USB storage device is inserted.</td>
<td>USB attached storage devices are fully accessible.</td>
</tr>
</tbody>
</table>
Overrides for Endpoint Protection

Overrides allow you to identify files and URLs that should be allowed or blocked regardless of a policy setting or how Webroot might define the file or URL.

In service provider view, Global file overrides are applied to all sites that have Include Global Overrides enabled in the site details.

Specific site rules always override global rules.

Policy settings take precedence over group settings.

Changes in overrides are applied to devices at their next polling interval, as configured in the Endpoint Protection policy that the device is using. To manually push changes out before that interval, use the Re-Verify Data agent command.

To access overrides, go to Manage > Overrides.

Allowing and blocking files

File overrides allow admins to define what files can execute and what files are blocked when using Endpoint Protection. File and folder overrides are only supported on Webroot Agent version 9.0.1 or later.

Go to Manage > Overrides and click the File Overrides tab to view and manage allowed and blocked files. Click the Overrides drop-down menu to select the scope of results shown in the Overrides table as follows:

- **Global** overrides apply to all sites that you have access to.
- Under the Sites list, select a specific site to view overrides that are associated with it.

To further narrow table results, use the Search box or click Filters. The search terms, filters, and sorting preferences that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.

To add a file override:

1. Click Add Override.
2. On the Add File Override page, select either Allow or Block as the file override type.
   - **Allow** - File overrides allow a file to execute, regardless of Webroot's cloud classification.
   - **Block** - File overrides block a file from executing, regardless of Webroot's cloud classification.
3. Select an override Type to specify whether the file should be identified by its folder/file location or by its MD5 hash value.
   - **Folder/File**
     - You cannot block based on folders/files; folders/files can only be allowed.
     - In the Folder field, enter an absolute file path or a file path using a system variable (such as %SystemDrive%) to be specified. Enter % to see a list of supported variables.
• In the **File** field, enter a specific file name or a wildcard. If left blank, all files in the specified folder will be allowed.

• Select **Include Sub-Folders** to include subfolders of the specified path.

• Select **Detect if Malicious** to detect and remediate the file according to the assigned policy. Monitoring and journaling are disabled. When this option is disabled, the detect and remediate policy settings do not apply to the file.

• Enter a **Name** for the override.

• Select **Scope** to specify if the rule should apply to all sites that are configured to include **Global** settings or just the selected **Site**.

• If you selected **Site** as the **Scope** of the override, you can associate it with a policy, which can be applied to individual sites, groups, or devices.

• **MD5** hash
  
  • Files based on MD5 hash values can be allowed or blocked.

  • If selected, specify the 32-character hash value.

4. When you are finished, click **Save**.

**To import defined overrides from another console or site:**

1. Click **ImportOverrides**.

2. Use the **Console / Site Source** drop-down menu to select the console/site containing the overrides you want to import from.

3. Use the **Console / Site Destination** drop-down menu to select the console/site you want to import the overrides to.

4. Select the check box next to any of the following options:

   • **Remove Redundant Overrides** removes redundant entries from the override import list, keeping the override that you already have in place. If not selected, redundant entries are not removed.

   • **Overwrite Existing Overrides** allows redundant entries that are not removed to overwrite existing entries. If not selected, redundant entries persist after the import.

   • **Include Policy Based Overrides** imports overrides assigned to the policy used by the site that you are importing from. These overrides will be converted to **Global** overrides. If not selected, the policy overrides from the site are not imported.

5. When you are finished, click **Import**.

**To edit an override:**

1. Find the override in the table and under the Actions column, click **Edit**.

2. Change any override specifications. Note that you will receive a **Redundant Override** alert if the Webroot Cloud determination already matches the selected Allow/Block value.

3. Click **Save**.

**To delete an override:**
1. In the **Overrides** table, select the check box next to the name of the override that you want to delete.

2. Click **Delete**.

### Allowing and blocking websites

If you are not using DNS Protection, the allowed/blocked domains specified in the Web Overrides tab are related to the Web Threat Shield policy settings.

If you are using DNS Protection, the Web overrides specified in this tab are your DNS Protection overrides.

**To specify a URL that should be allowed or blocked:**

1. Click **Add** to specify a URL that should be allowed or blocked.
   - In the **Domain(s)** box, enter a comma-separated list of domains you want to create a rule for. The protocol (such as https or www) is not needed. For example, you can specify domain.com. Wildcards are supported (*.domain.com).
   - Select **Scope** (**service provider view** only) to specify if the rule should apply to all sites that are configured to include global settings or just the selected site.
   - Select **Policy** (**service provider view** only) to associate this rule with a policy and specify the policy. If you do not specify a policy, the override will be associated with the site.
   - Select **Block/Allow** to specify if the domain should be blocked or allowed.
   - When **Block Malicious URLs** is selected, malicious URLs (such as domains with known malware) are blocked regardless of a rule.

2. Click **Refresh** to update the table.

**Filters** can be viewed by using the up and down arrow on the Filters row. You can narrow the list displayed to only those rows containing the domain, by scope, by policy, or whether the URL is blocked or allowed.

**To Sort**, click a column heading to sort the table by that column.

Under the **Action** column, you can **Edit Override** or **Delete Override**.
Reports

Reports provide in-depth information for Endpoint Protection, DNS Protection, and Security Awareness Training. You can create reports on demand or schedule them at recurring intervals.

Click Reports in the navigation pane to see all reporting options.

In service provider view, open the API Reporting tab to get information on the standalone Universal Reporter tool, which can be used to create customized reports for your customers.

Report types

The following reports are available for on-demand and scheduled reporting:

- DNS Protection reports are only available if you have DNS Protection enabled. See DNS Protection reports on page 111.
- Security Awareness Training reports are only available if you have Security Awareness Training enabled. See Security Awareness Training reports on page 123.

Device reports

- Agent Version Spread shows installed agent versions.
- Device Activations shows activations within the time period you can specify in a drop-down menu.
- Device Type shows Windows or macOS devices.
- Endpoint Status shows clean and infected devices.
- Expired Status shows active and expired devices.
- Installation Status shows active and uninstalled devices.
- Managed by Policy shows policy-managed and unmanaged devices.
- Operating System Firewall Status shows enabled, disabled, and unsupported operating system firewalls.
- Operating System Language shows operating system languages.
- Operating System Platform shows 32-bit, 64-bit, or unknown operating system architectures.
- Primary Browser shows default browsers.
- Remediation Status shows enabled and disabled remediation status.
- Scheduled Scans Status shows enabled and disabled scheduled scans.
- Silent Mode shows enabled, disabled, and unsupported silent scans.
- Virtual Machine shows devices classified as virtual machines.

File threat reports

- All Threats Seen shows identified threats by file name.
- All Undetermined Software Seen shows undetermined threats by file name.
• **Attention Required** shows sites that require attention.
• **Devices Needing Attention** shows devices that require attention.
• **Devices with Threats Seen on Last Scan** shows identified threats by device.
• **Devices with Undetermined Software on Last Scan** shows undetermined threats by device.
• **Threat Detection History** shows identified threats by count.

**Shield reports**

• **Evasion Shield - Script Protection Status** shows the status of all detect and report, detect and remediate, disabled, and unsupported Evasion Shield protection.
• **Evasion Shield - Script Detections** shows detected threats.
• **Firewall Status** shows enabled, disabled, and unsupported Endpoint Protection firewalls.
• **Identity Shield Status** shows enabled and disabled Identity Shield protection.
• **Infrared Status** shows enabled, disabled, and unsupported infrared setting.
• **Offline Shield Status** shows enabled, disabled, and unsupported Offline Shield protection.
• **Phishing Shield Status** shows enabled and disabled Phishing Shield protection.
• **Realtime Shield Status** shows enabled and disabled Realtime Shield protection.
• **Rootkit Shield Status** shows enabled, disabled, and unsupported Rootkit Shield protection.
• **USB Shield Status** shows enabled, disabled, and unsupported USB Shield protection.
• **Web Threat Shield Blocked URL History** shows blocked URLs by date.
• **Web Threat Shield Blocked URLs** shows blocked URLs.
• **Web Threat Shield Status** shows enabled and disabled Web Threat Shield protection.

**Creating and running a report**

You can create and run new reports on demand. You can also run existing, scheduled reports outside of their scheduled times.

1. Click **Reports** and open the **On-Demand** tab.
2. Specify the **Site** to run the report against. You can also run reports against all sites.
3. Specify the **Report** you want to generate.
4. When applicable, specify a time **Period** for the report data.
5. Click **Submit** to generate and display the report. Depending on the report type, you may have one or more of the following tasks and controls available for the report:
   • Click on chart data to show details for that subset of data. Some charts provide further levels to show more information.
   • In a table layout, click on a row to see details for that table row entry.
   • Click on file names to see more details.
• Click **Export to CSV** to download the report data to a comma-separated file (.csv). Export to CSV is only available for the following reports:
  • All Threats Seen
  • All Undetermined Software Seen
  • Devices with Threats Seen on Last Scan
  • Devices with Undetermined Software on Last Scan
  • DNS: Active Hosts
  • Evasion Shield
  • Web Threat Shield Blocked URL History
  • Web Threat Shield Blocked URLs

• Click **Actions** to access some of the following functions:
  • **Add this File to Allow list** specifies the file as an allowed file for the following reports:
    • All Threats Seen
    • All Undetermined Software Seen
    • Devices with Undetermined Software on Last Scan
    • Evasion Shield – Script Detections
    • Devices with Threats Seen on Last Scan
    • Threat Detection History reports
  • **Add this File to Block list** specifies the file as a blocked file for the following reports:
    • All Undetermined Software Seen
    • Devices with Undetermined Software on Last Scan
  • **Restore this File from Quarantine** removes the file from quarantine and restores it to its original location.
  • **Initiate Cleanup on this Device** starts a scan immediately and quarantines any malicious files.
  • **Create Override** creates an override for the URL.

• In the **Domain(s)** box, enter a comma-separated list of domains you want to create a rule for. The protocol (such as https or www) is not needed. For example, you can specify domain.com. Wildcards are supported (*.domain.com). This applies to the following reports:
  • Web Threat Shield Blocked URLs
  • Web Threat Shield Blocked URL History
• Select **Scope** (service provider view only) to specify if the rule should apply to all sites that are configured to include global settings or just the selected site. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History

• Select **Policy** (service provider view only) to associate this rule with a policy and specify the policy. If you do not specify a policy, the override will be associated with the site. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History

• Select **Block/Allow** to specify if the domain should be blocked or allowed. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History

• When **Block Malicious URLs** is selected, malicious URLs (such as domains with known malware) are blocked regardless of a rule. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History

### Scheduled reports

Scheduled reports allow you to get in-depth information on your sites at recurring intervals. Links to scheduled reports provided in emails are only valid for 48 hours. If you need to see a report past that time frame, see the scheduled reports history.

All scheduled reports must be created from an existing report template.

### Creating a scheduled report template

Two report templates are available by default. You can create your own templates as needed.

To view your available scheduled report templates, click **Reports** and select the **Scheduled Templates** tab.

The following buttons are available on the top of the **Scheduled Templates** tab:

• Click **Add** to add a new scheduled report template.

• Click **Copy** to make a copy of an existing scheduled report template. Select the new template to make modifications.

• Click **Delete** to delete a scheduled report template. If you delete a template, you need to assign a replacement template.

**To create a scheduled report template:**

1. Click **Reports** and select the **Scheduled Templates** tab.

2. Click **Add**. The **Create Template** dialog is displayed.
• **Name** is a unique name for the template.
• **Title Page Text** is used for the title of the report generated by this template.
• **File Format** provides options between PDF or CSV.

3. Construct your report template by choosing and placing the types of data you want to be included.
   - Click **Add Page** to add report types to the template. Use the drop-down menu to select specific report types for each page.
   - **Data Field** shows the type of data that is displayed.
   - From the **Chart Type** drop-down, if applicable, select what type of chart to use for the data.
   - From the **Time Period** drop-down, if applicable, select the time frame for the data.
   - Click **Delete Page** to remove the selected row from the template.
   - Use the **up/down** arrows to reorder the rows.

4. When done, click **Create**.

**Scheduling a report**

You must have an existing scheduled report template before you can create a new report to be scheduled. See *Creating a scheduled report template* on page 78.

**To view your existing scheduled reports:**

1. Click **Reports** and select the **Scheduled Reports** tab. The following buttons are available on the top of the reports table:
   - Click **Add** to create a new scheduled report.
   - Click **Copy** to make a copy of an existing scheduled report. Select the new report to make modifications.
   - Click **Delete** to delete a scheduled report.
   - Click **Suspend** to suspend a report. The report will not be generated or emailed until it is resumed.
   - Click **Resume** to resume a suspended report. The report is generated and emailed at the interval specified in the scheduled report settings.

2. Click **Run Report Now** to immediately generate and send a scheduled report. You can change the **Creation Method** and **Recipients** for an immediate run; changes are not applied to the scheduled report.

**To schedule a report:**

1. Click **Reports** and select the **Scheduled Reports** tab.
2. Click **Add**. The **Create Report** dialog box opens.
• **Report Name** is a unique name for the report.

• Select **Delivery Schedule** to specify when you want the report to be generated. Specify the time zone in UTC.

• Select from the **Creation Method** drop-down to specify whether to create one report per site, or one report for all sites.

• The **Recipients** options vary depending on your creation method.
  
  • If you have selected one single report creating data for all selected sites, enter a comma-separated list of up to 25 email addresses.

  • If you have selected one report per site, select from the following:
    
    • Select **Send to distribution list of each site** to use the report distribution list associated with each site.
      
      • In **business view**, this report distribution list is specified on the **Settings** tab.

      • In **service provider view**, go to the **Sites List** tab, click the site **Name** link, and then go to the **Details** tab.

    • Select **Send to email addresses provided below** to enter a comma-separated list of up to 25 email addresses.

    • Select **Send to both** to use both options above.

  • Select **Template** to specify what template to use for the report.

  • Select the **Sites** you want to generate the report for.

  • Select **Languages** to specify the default text of the report to be generated in. One report per selected language will be created.

3. Once the report is configured, click **Create**.

### Viewing scheduled report history

To view scheduled reports that were generated within the last 90 days, click **Reports** and select the **Scheduled History** tab.

Each report generated within the last 90 days will be listed in the table.

In the **Sites** column, hover over the question mark in the blue circle to see the sites included in the report.

Click **Download** to download a copy of the report to your local machine. If you selected one report per site and selected multiple sites, you need to specify which site’s report to download.

If needed, click **Refresh History** to update the table.
Deploying agents

An agent is software that runs on each device. The Webroot agent has a unique identity on each installed computer and performs security actions outside of the user's control on behalf of the administrator.

Webroot business products use two kinds of agents:

- **Webroot Endpoint Protection**
  - Cloud-based.
  - Once you install the agent you do not need to install or update any definition files.
  - When a new Endpoint Protection threat is identified, the agent is updated in the cloud for immediate protection of Endpoint Protection devices.

- **DNS Protection**
  - Only available when DNS Protection has been purchased.
  - Enabling DNS for a site in site settings does not install the DNS agent.
  - Only installs using a policy applied to the device. See *Using policies to deploy the DNS Protection agent* on page 108
  - Only runs on Windows endpoints.
  - Mac endpoints can have DNS Protection when connected (either using a VPN or on-site) in a DNS protected network.
  - The DNS agent will resolve requests when the devices are both on and off the network.
  - See *Providing DNS Protection by deploying an agent* on page 107.

There are multiple ways to deploy agents to devices, from manual installations on a local machine to remote deployments using RMM solutions or GPO to third-party tools like SCOM, PDQ Deploy, or AutoMox.

Regardless of your method, you should initially work with a small subset of devices until you are confident your deployment strategy is working. Once you are sure, you can implement the strategy for larger numbers of devices.

The following sections include instructions for a few of the most commonly used deployment methods.

**Installing on Windows or macOS using the installation wizard**

To install an agent on Windows or macOS using the installation wizard:

1. Locate the agent installation download links in the Management Console.
   - If you are using **Business view**:
     a. Go to *Settings > Downloads* to see the installation file download links.
     b. Click the *Download* link under the operating system used by the target device.
   - If you are using **service provider view**: 

---

Deploying agents
a. Click **Sites List**.

b. Find your site in the list and click the name.

c. Open the **Endpoint Protection** tab.

d. Click the **Download Windows .exe, Download Windows (.msi), or Download Mac** link to download the appropriate file for the target device.

2. Copy the **Keycode** for your company or for the site for future reference.

3. Move the installation file to the device you are installing the agent on.

4. Install the agent.

After installation is finished, the agent scans for threats. Once the initial scan is complete, the agent checks in with the Management Console and the **Devices** column populates on the **Entities** page. This process typically takes 15 – 30 minutes but can take up to 24 hours.

If DNS Protection is enabled, filtering begins immediately.

**Installing on Windows or macOS from the command line**

To install an agent on Windows or macOS from the command line:

1. Locate the agent installation download links in the Management Console.
   - If you are using **Business view**:
     - Go to **Settings > Downloads** to see the installation file download links.
     - Click the **Download** link under the operating system used by the target device.
   - If you are using **service provider view**:
     - Click **Sites List**.
     - Find your site in the list and click the name.
     - Open the **Endpoint Protection** tab.

2. Select the Windows download link to download the file.

3. Install the agent using any of the command options that correspond to your device. Unless otherwise noted, these options are for Windows machines.
   - `/key=keycode` or `-keycode = (mac)` installs the agent software using the specified keycode, with or without hyphens.
   - `/silent` or `-silent` (mac) installs the agent in the background with no on-screen interaction.
   - `/nostart` installs the agent, but does not start it.
   - `/lockautouninstall=password` installs the agent without adding it to the Windows Control Panel programs list. You can silently uninstall later using the specified password. When you use `/lockautouninstall`, Endpoint Protection is not included in the **Add/Remove Programs** list in the Control Panel. Use the `/exeshowaddremove` command to include Endpoint Protection in **Add/Remove Programs**.
• /autouninstall=password uninstalls the agent using the password specified with
 锁定/autouninstall。默认情况下，Endpoint Protection 不显示在
Add/Remove Programs 列表中，这将阻止用户从
删除软件在未管理模式下。

• -clone enables you to assign a unique ID to the machine when the agent is installed on
a device that does not have a unique host name due to cloning. The unique ID will be
included in the host name to better identify this machine.

• -uniquedevice enables you to assign a unique ID to the machine when the agent is
installed on a device that does not have a unique machine ID, but does have a unique
host name. The host name will be used to identify this machine.

• /exeshowaddremove includes the agent software in the Windows Control Panel
programs list. End-users will be able to uninstall the agent software when it is in
unmanaged mode.

• /group=groupcode assigns the device to the specified group during the agent
installation. The group must already exist in the Management Console and the machine
must not have had the agent software previously installed.

• /proxyhost=IPaddress or -proxy_host= (mac) causes the specified proxy
server to be used during the agent installation.

Endpoint Protection automatically detects proxy settings, so the command line options are
available for preferred usage over automatic detection.

If you specify the proxy server, use all proxy settings and pass a null value for any option you do
not want to specify.

• /proxyport=portnumber or -proxy_port= (mac) causes the specified port
number to be used for the proxy server.

• /proxyuser=name or -proxy_user= (mac) causes the specified user name to be
used for the proxy server.

• /proxypass=password or -proxy_pass= (mac) causes the specified password to
be used for the proxy server.

• /proxyauth=authtype or -proxy_auth= (mac) causes one of the following
authentication types to be used for the proxy server:
  • 0—Search through all authentication types. This option may take longer and may
cause unnecessary errors on the proxy server.
  • 1—Use basic authentication.
  • 2—Use digest authentication.
  • 3—Use negotiate authentication.
  • 4—Use NTLM authentication.

• /lang=languagecode or -language= (mac) installs the agent using one of the
following language codes.
  • de—German
  • en—English
After installation is finished, the agent scans for threats. Once the initial scan is complete, the agent checks in with the Management Console and the Devices column populates in the Entities page. This process typically takes 15 – 30 minutes but can take up to 24 hours.

If DNS Protection is enabled, filtering begins immediately.

### Installing on Windows using Msiexec

Msiexec is a Windows command-line based program that interprets and installs software installation packages. You can use Msiexec to install Endpoint Protection. Typically, use this method of installation when you are pushing the software using a remote deployment tool.

**To install an agent on Windows using Msiexec:**

1. Locate the agent installation download links in the Management Console.
   - If you are using Business view:
     a. Go to Settings > Downloads to see the installation file download links.
     b. Click the Download link under the operating system used by the target device.
   - If you are using service provider view:
     a. Click Sites List.
     b. Find your site in the list and click the name.
     c. Open the Endpoint Protection tab.

2. Download the .msi file.

3. Use the following syntax to use Msiexec with Endpoint Protection. Substitute your keycode, with or without hyphens, for keycode in GUILIC.

   ```
   msiexec /i wsasme.msi GUILIC=keycode CMDLINE=SME,quiet /qn /l*v install.log
   ```

   You can also specify ARPNOREMOVE in your command to prevent end-users from uninstalling Endpoint Protection.
After installation is finished, the agent scans for threats. Once the initial scan is complete, the agent checks in with the Management Console and the Devices column populates on the Entities page. This process typically takes 15 – 30 minutes but can take up to 24 hours.

If DNS Protection is enabled, filtering begins immediately.

**Installing on Windows using group policy**

Group policy can be used as a software deployment tool with the .msi installer. You should be familiar with Microsoft Active Directory and the GPO editor to use this method.

**To install an agent on Windows using a group policy:**

1. Locate the installation file download links in the Management Console.
   - If you are using Business view:
     a. Go to Settings > Downloads to see the installation file download links.
     b. Click the Download link under the operating system used by the target device.
   - If you are using service provider view:
     a. Click Sites List.
     b. Find your site in the list and click the name.
     c. Open the Endpoint Protection tab.
2. Download the .msi file.
3. On the domain controller, use the GPO editor to create a policy for deployment group.
4. Assign Endpoint Protection to all devices that belong to the Organizational Unit where the Group Policy is created. Endpoint Protection is installed on the devices in the group when they restart.

After installation is finished, the agent scans for threats. Once the initial scan is complete, the agent checks in with the Management Console and the Devices column populates on the Entities page. This process typically takes 15 – 30 minutes but can take up to 24 hours.

If DNS Protection is enabled, filtering begins immediately.

**Installing the agent using scripts**

Scripts used to install the agent should be thoroughly tested before use. Webroot does not troubleshoot or support scripts and will not answer script-related questions.

See How to use a script to install the Webroot agent on macOS in the Knowledge Base to see a sample script for installing on Macs.
Alerts and alert distribution lists

An alert is an email notification that notifies you when a threat is detected or when the Webroot agent is installed on a device. You can also generate alerts that are summaries of threats and installations. An alert distribution list is a list of one or more email addresses that alerts will be sent to.

Managing alerts and alert distribution lists

To view your available alerts, click Alerts. The page is divided into two tabs for the alerts and alert distribution lists. Each list shows high-level information about the alert or alert distribution list.

- Click Add on either tab to add an alert or an alert distribution list.
- Click Delete on either tab to delete the selected alert or the alert distribution list.
- Click Suspend to suspend the selected alert. No emails are sent to the alert distribution list when the alert criteria is met.
- Click Resume to resume the selected alert. Emails are sent to the alert distribution list when the alert criteria is met.

Click on a table row to see and edit details for that table row entry.

Adding an alert

To add an alert:

1. Click Alerts and open the Alert List tab.
2. Click Add.
3. In the first step of the Create Alert wizard, configure the basic settings of the alert.
   - Click Name to specify a unique name for the alert.
   - Click Alert type to select the type of alert you want to create.
4. Click Next to continue.
5. In the second step of the Create Alert wizard, identify who will receive the alert.
   - Click Use Existing List to select an existing distribution list from the drop-down.
   - Select Create New List to create a new alert distribution list.
     - Distribution List Name should be a unique name for the new alert distribution list.
     - In the Email Addresses box, specify a comma-separated list of up to 25 addresses to receive the alert notification email.
6. Click Next to continue.
7. In the third step of the Create Alert wizard, select the sites that should use this alert.
   - All sites configures all sites for this alert.
   - Selected sites enables you to select specific sites for this alert.
8. Click Next to continue.
9. In the fourth step of the Create Alert wizard, configure the email that will be sent when the alert is generated.
   
   - **Email Title** is the title of the email message that will be sent.
   - **Email Message Body** is the text of the email message to be sent.
   - **Data Inputs** are the variables that will be populated with specific data when an alert is generated. When you are working in either the title or body fields, the data input buttons are blue (enabled). Click an enabled variable to add it to the title or body.
     
     - If you select the Threat List data input, you will need to select additional data inputs from a list to identify which threats you want to include.
     
     - The Workgroup and Active Directory data inputs are not applicable to macOS.

10. Click **Finish** to create the alert.

**Adding an alert distribution list**

To add an alert distribution list:

1. Click **Alerts** and open the Distribution Lists tab.

2. Click **Add**.

3. Configure the alert distribution list.
   
   - Click Name to specify a unique name for the alert.
   
   - In the Email Addresses box, specify a comma-separated list of up to 25 addresses to receive the alert notification email.

4. Click **Create** to create the alert distribution list.
Administration tasks

Each user account is assigned one of three types of permissions:

- **Super Admin** accounts have full visibility and permission to do all tasks on the Management Console.
- **Limited Admin** accounts are allowed to see only specific areas of the Management Console.
- **No Access** accounts are prohibited from using the Management Console.

If you are an MSP using **service provider view**, you can also use user accounts to control access to sites.

- **Admin** has full access to the site.
- **View Only** has view-only access to the site.
- **No Access** denies access to the site. The user cannot see the site listed on the **Sites List** page.

Viewing available administrators

To view your available administrators, go to the **Admins** page.

- Super administrators and limited administrators are listed on the **Admins** tab.
- Site-only administrators (service provider view only) are listed on the **Site Only Admins** tab.

The following controls are available on the two tabs. You may not be able to perform all these actions depending on the access granted to your user account.

- Click **Add Admin** to add a new administrator.
- Click the admin **Name** link to view or edit the account information.
- Under **Actions**, you can perform the following functions:
  - **Resend Confirmation Email** sends another confirmation email to the email address for the account.
  - **Edit** enables you to view or edit the account information.
  - **Delete** deletes an administrator.
- Click a column heading to sort the table by that column.

Adding an administrator

1. Click **Admins** and then click **Add Admin**.
2. In the first step of the **Add Admin** wizard, configure your administrator details.
   - **First Name** is the user’s first name.
   - **Last Name** is the user’s last name.
   - **Email** is the user’s email address. This is what the user will use to log in.
   - **Phone** (optional) is the user’s phone number.
• **Time Zone** is the user's time zone.

• **Account Type** determines the type of access you want to grant to this user for the Management Console.

<table>
<thead>
<tr>
<th>Management Console Component</th>
<th>Super Admin</th>
<th>Limited Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admins</td>
<td>X</td>
<td>View only</td>
</tr>
<tr>
<td>Alerts</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Dashboard</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Entities</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Overrides</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security Awareness Training</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Settings</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sites Lists (serve provider view only)</td>
<td>Based on site permissions</td>
<td>X</td>
</tr>
</tbody>
</table>

3. If you are in **business view**, click **Save** to add the administrator.

4. If you are in **service provider view**, click **Next** to continue to assign site administrator permissions.

5. Select the sites this administrator should have access to.

   • **Admin** has full access to the site.
   
   • **View Only** has view-only access to the site.
   
   • **No Access** denies access to the site. The user cannot see the site listed on the **Sites List** page.

6. Click **Save** to add the administrator.

**Editing an administrator**

**To edit an administrator:**

1. Go to the **Admins** page.

2. Click the admin **Name** link. The settings for the selected administrator are displayed.

3. Modify the settings on the **Details** or **Site Permissions (service provider view only)** tabs as needed.

4. When done, click **Save**.
Deleting an administrator

A deleted administrator can be added again. You cannot delete the only administrator as there must be at least one administrator per console.

To delete an administrator:

1. Go to the Admins page.
2. Under Actions, click Delete.
3. Confirm you want to delete the administrator by clicking Delete Admin.
Settings

The Settings tab contains various configuration sections. The available configurations vary if you are using the business view or the service provider view.

Business view settings

The Endpoint tab includes general site or company information.

- **Site / Company Name** is a unique name for the site or company.
- **Keycode** is a read-only field that displays the keycode assigned to the site or company. If the keycode is a trial, the number of days remaining in the trial period are also displayed. This is the keycode that is used in Endpoint Protection installations. This keycode is also on the Downloads tab.
- **Company Size** is a range that represents the size of the company.
- **Company Industry** should be the industry that best represents the company.
- **Comments** (optional) is any information that describes the site or company.
- **Site Seats** are the number of endpoints for the site you are configuring. This setting is not used for billing.
- **Default Endpoint Policy** is used for all new devices installed for this site unless the policy is assigned using inheritance from the group, site, or company. You can modify the policy the device uses after installation. Webroot recommends that you create a copy of this default endpoint policy and modify it according to policy best practices and your specific needs.
  - **Recommended Defaults** is intended for desktops and laptops. User interface and possibly unwanted applications (PUAs) are disabled. The setting to install DNS Protection is disabled in this policy.
  - **Recommended DNS Enabled** is the same as Recommended Defaults, except the setting to install DNS Protection is enabled.
  - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
  - **Silent Audit** is based on the Recommended Defaults policy, except the remediation function is disabled to minimize production impact. It catches known threats, but not undetermined threats.
    - All visible aspects of Webroot (user interface, system tray icon, add/remove programs entry) are hidden.
    - Use the undetermined threats reports to identify items to add to your block and allow overrides.
    - Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.
    - Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.
• The only specific setting that the **Unmanaged** policy has is whether to show the user interface. It uses the settings of prior policies.
  
  • Intended for technical support, troubleshooting, and when no policy management is needed.
  
  • Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
  
  • Should not be used in production.

• In the **Report Distribution** List, specify a comma-separated list of up to ten email addresses to receive the generated reports.

The **Subscriptions** tab allows you to learn about, upgrade, or renew your Webroot products. If you purchased through an RMM partner, you may be redirected to the partner site.

The **Account Information** tab provides information on the primary account holder.

• The **Site / Company Name** is the company name used to define the console. Click **Rename** to edit the console name.

• The **Company Address** is specified for you when your account is created. If you need to modify the address, contact Webroot.

• **Contact Email** is the email of the primary account for the selected console. If you need to modify the email, contact Webroot.

• **Contact Phone** is specified for you when your account is created. If you need to modify the phone number, contact Webroot.

• **Parent Keycode** is the keycode assigned to the selected console. Do not use this keycode for installations. You should use the keycode assigned to the site (found on the **Endpoint** tab) for installations. Click **Renew/Upgrade** to update your subscription.

• **View Usage** opens a separate console where you can view your usage for the previous year. Click **My Usage**, log in when prompted, and, if prompted, select a console. Once logged in, you will have tabs for usage and billing.
  
  • In the **My Usage** tab, the report shows a rolling 30 day total from the date selected on the **My Usage** page.

    • Export the usage data by clicking the **Download CSV** link.

    • Drill down to see site usage by clicking the **Site Usage** button; you can also export the usage data for that site.

• **Pay Invoices** opens a separate console where you can view your billing history. Click **My Billing**, log in when prompted, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.

  • In the **My Billing** tab, online payment features are available if you are paying Webroot directly. If you are paying a service provider or third party, the online payment features will not be available.

  • From the billing page, select an account. If needed, create an account following the on-screen instructions and then verify the email that you receive.

  • Review your invoices and if desired, you can make a payment.
• You can also set up AutoPay to have your billing automatically paid using a saved credit card. Follow the on-screen instructions for saving the credit card information. If you want to discontinue AutoPay, contact wrAccountsReceivable@opentext.com or your sales representative.

• In the Login Settings section, you can change your password, change your security questions, enable 2FA, and change your security code.

The Downloads tab contains links for the Windows and macOS agent installations. It also contains a copy of the keycode that is built in and applied to the installation. Use these installation files to manually install on a device. See Deploying agents on page 81.

The Web Block Page Settings tab allows you to customize the notification page that is displayed when URLs are blocked.

• Drag and drop a Logo to the dotted box if you want your own logo to appear on the notification page. You can also click the dotted box and select the logo.
  • The logo file name extensions must be either .png, .gif, or .jpeg.
  • The maximum height of the logo is 50 pixels.
  • The width will be adjusted automatically to maintain the aspect ratio of the logo.
  • The file size limit is 1 MB.
  • When a logo has been added, the Webroot logo changes to “powered by Webroot.”
  • To remove a logo that you have uploaded, hover over the dotted box and click Delete current image. The powered by Webroot logo changes back to the standard Webroot logo.

• The Website not allowed text and graphics below the logo and above the formatting toolbar automatically appear on the notification page. The text and graphics cannot be modified or deleted.

• Enter Additional information into the free form field below the formatting bar.
  • You can modify or delete this text.
  • Enter a maximum of 500 characters.

• Click Reset to Default Settings to reset the logo and additional information back to the default settings.

The Unity API Access tab enables you to access the Unity API.

• This is a REST API that you can use to automate access to Webroot services and information, such as billing, reporting, and so on.

• To get started, click Create New Client Credential. Follow the 3-step process, then acknowledge that you have made note of the client secret. You will need to use the client ID and client secret in order to authenticate with the API to access information or take action.

• You can also enable Notification API, which allows you to receive near real-time Unity API Notifications based on a set of events that you can subscribe to on different domain levels.

• You can create up to 20 unique client credentials. Once you have created at least one client credential, you can manage its Unity API settings from the Unity API Access table. From there, the following actions are available:
• **New**—Opens the Create New Client Credential dialog box.

• **Edit**—Opens the Edit Client Credential dialog box, which allows you to modify the selected client credential name, description, and purpose for using the Unity API. You can enable or disable API notifications in Step 2 by answering “Do you plan to use the event notification API?” with either Yes or No.

• **Delete**—Deletes the selected client credential record.

• **Renew Secret**—Renews the client credential secret for the selected credential. This will expire the previously set secret and revoke any future requests attempted using this credential with the old secret.

• **Suspend**—Temporarily revokes a client’s API Access. To re-enable access for the selected client credential, click **Resume**.

The **Advanced Settings** tab contains two advanced settings.

• Click **Edit** to set or remove a filter, and to see the history of data filter changes. Data filters enable you to limit the data that is displayed in the console. Narrowing your filters may improve page loading performance, depending on how much data is being loaded, but it will limit what you see. When you apply or clear filters, it may take a few minutes to update the data depending on the amount the deployment size and the amount of data to display.

• Click **Convert** if you want to change to **service provider view**. This allows you to have multiple sites, such as companies, business, organizational units, and so on, in the Management Console. Each site will have separate keycodes and billing. Selecting the service provider option is not reversible.

**Service provider view settings**

The **Subscriptions** tab allows you to learn about, upgrade, or renew your Webroot products. If you purchased through an RMM partner, you may be redirected to the partner site.

The **Account Information** tab provides information on the primary account holder.

• The **Site / Company Name** is the company name used to define the console. Click **Rename** to edit the console name.

• The **Company Address** is specified for you when your account is created. If you need to modify the address, contact Webroot.

• **Contact Email** is the email of the primary account for the selected console. If you need to modify the email, contact Webroot.

• **Contact Phone** is specified for you when your account is created. If you need to modify the phone number, contact Webroot.

• **Parent Keycode** is the keycode assigned to the selected console. Do not use this keycode for installations. You should use the keycode assigned to the site (found on the **Endpoint** tab) for installations. Click **Renew/Upgrade** to update your subscription.

• **View Usage** opens a separate console where you can view your usage for the previous year. Click **My Usage**, log in when prompted, and, if prompted, select a console. Once logged in, you will have tabs for usage and billing.
In the **My Usage** tab, the report shows a rolling 30 day total from the date selected on the **My Usage** page.

- Export the usage data by clicking the **Download CSV** link.
- Drill down to see site usage by clicking the **Site Usage** button; you can also export the usage data for that site.

**Pay Invoices** opens a separate console where you can view your billing history. Click **My Billing**, log in when prompted, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.

- In the **My Billing** tab, online payment features are available if you are paying Webroot directly. If you are paying a service provider or third party, the online payment features will not be available.
  - From the billing page, select an account. If needed, create an account following the on-screen instructions and then verify the email that you receive.
  - Review your invoices and if desired, you can make a payment.
  - You can also set up AutoPay to have your billing automatically paid using a saved credit card. Follow the on-screen instructions for saving the credit card information. If you want to discontinue AutoPay, contact wrAccountsReceivable@opentext.com or your sales representative.

- In the **Login Settings** section, you can change your **password**, change your **security questions**, enable **2FA**, and change your **security code**.

The **Data Filter** tab enables you to apply a time-based filter to all sites. Select the time frame you want to use and click **Save**. You can override this setting from within an individual site. The history of data filter changes is also displayed.

The **Web Block Page Settings** tab allows you to customize the notification page that is displayed when URLs are blocked.

- Drag and drop a **Logo** to the dotted box if you want your own logo to appear on the notification page. You can also click the dotted box and select the logo.
  - The logo file name extensions must be either `.png`, `.gif`, or `.jpeg`.
  - The maximum height of the logo is 50 pixels.
  - The width will be adjusted automatically to maintain the aspect ratio of the logo.
  - The file size limit is 1 MB.
  - When a logo has been added, the Webroot logo changes to “powered by Webroot.”
  - To remove a logo that you have uploaded, hover over the dotted box and click **Delete current image**. The powered by Webroot logo changes back to the standard Webroot logo.

- The **Website not allowed** text and graphics below the logo and above the formatting toolbar automatically appear on the notification page. The text and graphics cannot be modified or deleted.
- Enter **Additional information** into the free form field below the formatting bar.
• You can modify or delete this text.
• Enter a maximum of 500 characters.

• Click **Reset to Default Settings** to reset the logo and additional information back to the default settings.

The **Unity API Access** tab enables you to access the Unity API.

• This is a REST API that you can use to automate access to Webroot services and information, such as billing, reporting, and so on.

• To get started, click **Create New Client Credential**. Follow the 3-step process, then acknowledge that you have made note of the client secret. You will need to use the client ID and client secret in order to authenticate with the API to access information or take action.

• You can also enable Notification API, which allows you to receive near real-time Unity API Notifications based on a set of events that you can subscribe to on different domain levels.

• You can create up to 20 unique client credentials. Once you have created at least one client credential, you can manage its Unity API settings from the Unity API Access table. From there, the following actions are available:

  • **New**—Opens the **Create New Client Credential** dialog box.
  • **Edit**—Opens the **Edit Client Credential** dialog box, which allows you to modify the selected client credential name, description, and purpose for using the Unity API. You can enable or disable API notifications in Step 2 by answering "Do you plan to use the event notification API?" with either Yes or No.
  • **Delete**—Deletes the selected client credential record.
  • **Renew Secret**—Renews the client credential secret for the selected credential. This will expire the previously set secret and revoke any future requests attempted using this credential with the old secret.
  • **Suspend**—Temporarily revokes a client's API Access. To re-enable access for the selected client credential, click **Resume**.
DNS Protection

DNS Protection works in conjunction with Webroot Endpoint Protection and is purchased separately. It is a domain filtering service that uses DNS to provide internet usage restrictions both across the network and independent of the network.

If you have DNS Protection enabled, your Endpoint Protection interface may include some tabs or other elements that would otherwise not be displayed.

Getting started with DNS Protection

1. Register, set up, and deploy Endpoint Protection. See Getting Started with Endpoint Protection.
2. Enable and configure DNS Protection. See Enabling and Configuring DNS Protection.
3. Ensure the endpoints are covered by DNS Protection.
   - This can be done by deploying agents to the devices using policies. See Using policies to deploy the DNS Protection agent on page 108
   - You can also set up your network to cover all devices within the network, regardless of whether they have the DNS protection agent. See Configuring the network on page 109

Enabling and configuring DNS Protection

Before you can deploy the DNS Protection agent, you must enable and configure DNS Protection.

There are slight differences in how to do this depending on whether you are in the business view or service provider view.

To enable and configure DNS Protection in business view:

1. Click DNS Protection in the navigation pane.
2. Enable the DNS Protection setting using the slider control.
3. If required, select your keycode type.
   - Full provides the full product with no limitations. You will be billed for this service.
   - Trial provides the full product, limited to a free, 30-day trial.
4. Under Agent Settings, select a default DNS site policy for the roaming agent. This can be modified on the Policies page.
   - DNS High Protection blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
   - DNS Medium Protection blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
   - Custom policies may also be available.
5. Under **Agent Settings**, create a domain bypass list to have domains resolved locally.
   - The list only applies to the DNS Protection agent.
   - Entries in the list are passed to the local DNS resolver rather than being resolved by the DNS Protection Agent.
   - Wildcards can be used to include any Subdomains.
   - Include your internal domain in the bypass list.

6. Under **Network Settings** you can enter details to protect network connected devices that do not have the agent installed.
   - Identify the public IPv4 address used for internet access (WAN IP).
   - To make use of a domain name within our service, you need to use a third party Dynamic DNS service to transmit a changing IP address to a static domain name. Endpoint Protection uses this service to determine what IP address we should use to accept DNS requests from.
   - If you have dynamic IP support, entering a domain name resolves to the IP address. Third party dynamic DNS services are needed for this to be able to transmit a changing IP address to a static domain name.
   - Select a policy for that network. Any DNS requests received from this WAN IP are resolved based on this filter.
   - Requests from unregistered IP addresses or from IP addresses under expired or disabled sites do not receive a response.
   - Select **Add Network** to add multiple networks.

7. Under **Network Settings**, use the Network Location menu to identify the best Webroot DNS services for your region.
   - Select the correct Network Location for the site on which you have enabled DNS Protection.
   - The best primary and secondary Webroot DNS services are shown.
   - Once you have identified the best resolvers, update your DNS forwarders.

8. Under **Advanced Settings**, select whether the agent can be installed on servers.
   - When checked, the DNS Protection agent installs on servers.
   - This is not recommended on DNS servers as it can cause DNS resolution problems.
   - DNS servers should be protected by configuring the DNS forwarders.
   - Other servers, such as terminal services, can run DNS Protection if you selected the **Allow DNS Agent to run on Servers** check box.

9. When done, click **Save**.

To enable and configure DNS protection in service provider view:
1. Click Sites List and expand the columns using the slider.

2. For the site you are working with, in the DNS Protection column, check if DNS Protection is either Active or in a Trial period by hovering over the DNS Protection icon.
   - Blue background indicates DNS is active.
   - Grey background indicates DNS is inactive. Click the Start Trial link to start a free 30-day trial of DNS Protection. You are prompted to take one of two actions. These actions are not required to get started.
     - Download Software enables you to download the agent software.
     - Configure DNS Settings enables you to customize your DNS network settings.
       - This step allows you to protect devices without the agent installed by registering the WAN IP address associated with the network.
       - You do not need to configure this setting to get started.
   - White background indicates DNS is in trial period. Click the Upgrade link to convert to a full version, which you will be billed for.
   - Slash mark indicates the trial period is expired. Click the Upgrade link to convert to a full version, which you will be billed for.

3. To configure the DNS Protection settings for this site, hover over the DNS Protection icon and click the Configure button.

4. Under Agent Settings, select a default DNS site policy for the roaming agent. This can be modified on the Policies page.
   - DNS High Protection blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
   - DNS Medium Protection blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
   - Custom policies may also be available.

5. Under Agent Settings, create a domain bypass list to have domains resolved locally.
   - The list only applies to the DNS Protection agent.
   - Entries in the list are passed to the local DNS resolver rather than being resolved by the DNS Protection Agent.
   - Wildcards can be used to include any Subdomains.
   - Include your internal domain in the bypass list.

6. Under Network Settings you can enter details to protect network connected devices that do not have the agent installed.
   - Identify the public IPv4 address used for internet access (WAN IP).
   - To make use of a domain name within our service, you need to use a third party Dynamic DNS service to transmit a changing IP address to a static domain name. Endpoint Protection uses this service to determine what IP address we should use to accept DNS
requests from.

- If you have dynamic IP support, entering a domain name resolves to the IP address. Third party dynamic DNS services are needed for this to be able to transmit a changing IP address to a static domain name.
- Select a policy for that network. Any DNS requests received from this WAN IP are resolved based on this filter.
- Requests from unregistered IP addresses or from IP addresses under expired or disabled sites do not receive a response.
- Select Add Network to add multiple networks.

7. Under **Network Settings**, use the Network Location menu to identify the best Webroot DNS services for your region.
   - Select the correct Network Location for the site on which you have enabled DNS Protection.
   - The best primary and secondary Webroot DNS services are shown.
   - Once you have identified the best resolvers, update your DNS forwarders.

8. Under **Advanced Settings**, select whether the agent can be installed on servers.
   - When checked, the DNS Protection agent installs on servers.
   - This is not recommended on DNS servers as it can cause DNS resolution problems.
   - DNS servers should be protected by configuring the DNS forwarders.
   - Other servers, such as terminal services, can run DNS Protection if you selected the **Allow DNS Agent to run on Servers** check box.

9. When done, click **Save**.

**Installing network certificates and licenses**

The notification page displayed when URLs are blocked is called the **Block Page**.

To correctly display the Block Page when a restricted site is encountered, you must install the Webroot certificates to the Trusted Root Authorities Certificate Store (typically `..\Certificates - Current User\Trusted Root Certification Authorities\Certificates`). Certificates are automatically installed with the DNS Protection agent.

Your devices are protected without the certificates; however, instead of the **Block Page**, a certificate error appears. You can install the certificates manually or through the `certinstaller.exe` tool as follows:

- Certificate Installer:
  
  https://download.webroot.com/DNS/certinstaller.exe
- Certificates:
  
  https://download.webroot.com/DNS/certificates/webroot-certificate.p7b
  https://download.webroot.com/DNS/certificates/webroot-certificate.pem
Managing DNS Protection policies

To review or modify DNS Protection Policies:

1. Open Manage > Policies.
2. From the DNS Protection tab, select the policy you want to view or modify.

The Policies page is divided into several sections:

- **Privacy Settings** control user privacy settings and the information that is logged.
  - **Hide User Information** improves privacy by replacing the user name and the domain requested with the word Hidden in the logs. If requests are made in the Security Risk category, the domain is still logged for visibility.
  - **Local Echo** echoes DNS requests made by the DNS Protection Agent to the local network’s DNS resolver, providing visibility to these requests for your firewall or DNS server. To improve privacy, a DNS resolver can be specified, and requests will only be echoed when it is available.
  - **Fail Open** avoids a possible DNS interruption if the Webroot DNS resolvers are unavailable by deferring DNS resolution to the local resolver or returning without filtering.

- **Security Settings** specify whether to block or allow certain sites.
  - **Keyloggers and Monitoring** are sites that include downloads and discussions for software agents that track keystrokes or web surfing habits.
  - **Malware Sites** are sites known to contain malicious content including executables, drive-by infection sites, malicious scripts, viruses, or Trojans.
  - **Phishing and Other Frauds** are sites known to pose as reputable sites, usually to harvest personal information from a user. These sites are typically quite short-lived, so examples don’t last long.
  - **Proxy Avoidance and Anonymizers** are sites that use proxy servers or other methods to bypass URL filtering or monitoring.
  - **Spyware and Adbwares** are sites that are known to contain spyware or adware that provides or promotes information gathering or tracking that is unknown to or without the explicit consent of the user. This policy also includes sites that contain unsolicited advertising pop-ups and programs that may be installed on users’ computers.
  - **Bot Nets** are URLs or IP addresses known to be part of a Bot network from which network attacks are launched. Attacks may include SPAM messages, denial of service (DOS) attacks, SQL injections, proxy jacking, and other unsolicited contact.
  - **SPAM URLs** are URLs contained in spam messages.

- **Content Settings** specify whether to block or allow content that is inappropriate, illegal, or sexually explicit in nature.
• Human Resources Protections
  • Abused Drugs sites show illegal, illicit, or abused drugs, including legal highs, glue sniffing, misuse of prescription drugs, or abuse of other legal substances.
  • Adult and Pornography sites contain sexually explicit material for the purpose of arousing sexual interest, including sites with adult products such as sex toys and videos. This policy also includes online groups sites that are sexually explicit, sites with erotic stories or textual descriptions of sexual acts, sites for adult services such as video conferencing, escort services, and strip clubs, and sites with sexually explicit art.
  • Dating sites focus on establishing personal relationships.
  • Sex Education sites depict information on reproduction, sexual development, safe sex practices, sexually transmitted diseases, sexuality, birth control and contraceptives, tips for better sex, and products used for sexual enhancement.
  • Swimsuits & Intimate Apparel sites show swimsuits, intimate apparel, or other types of suggestive clothing.
  • Gross sites show blood or bodily functions, such as vomit.
  • Nudity sites contain nude or semi-nude depictions of the human body, that may not be sexual in intent but may include things like nudist or naturist sites, nude paintings, or photo galleries of artistic nature.
  • Alcohol and Tobacco sites provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.
• Questionable/Legal
  • Cult and Occult sites provide methods, means of instruction, or other resources that attempt to affect or influence real events using astrology (including horoscopes), spells, curses, magic powers, or supernatural beings.
  • Gambling or lottery sites include sites that use real or virtual money; sites that contain information or advice for placing wagers, participating in lotteries, gambling, or running numbers; virtual casinos and offshore gambling ventures; sports picks and betting pools; and virtual sports and fantasy leagues that offer large rewards or request significant wagers. Hotels and resort sites that do not enable gambling on the site are categorized as Lifestyle, Travel or General Information, Local information.
  • Marijuana sites depict marijuana use, cultivation, history, culture, or legal issues.
  • Hacking sites depict illegal or questionable access to or the use of communications equipment/software or sites for the development and distribution of programs that may compromise networks and systems, including sites that avoid licensing and feeds for computer programs and
other systems.

- **Weapons** sites provide sales reviews and descriptions of weapons such as guns, knives, or martial arts devices, including sites that provide information on accessories or other modifications.

- **Pay to Surf** sites pay users in the form of cash or prizes for clicking on reading specific links in emails or webpages.

- **Questionable** sites manipulate the browser user experience or client in some unusual, unexpected, or suspicious manner. Also includes get rich quick sites.

- **Hate and Racism** sites support hate crime or racist content or language.

- **Violence** sites advocate violence, violent depictions, or methods, including game/comic violence and suicide.

- **Cheating** sites support cheating and contain materials such as free essays, exam copies, and plagiarism.

- **Illegal** sites depict criminal activity including how not to get caught and copyright and intellectual property violations.

- **Abortion** sites depicting abortion, either pro-life or pro-choice.

- **Social Media/internet Communication**
  - **Social Networking** sites that have user communities where users interact, post messages, pictures, and otherwise communicate.
  - **Personal Sites and Blogs** are sites posted by individuals or groups, including blogs.
  - **Online Greeting Cards** sites offer e-cards.
  - **Search Engines** use key words or phrases and return results that include text, websites, images, videos, and files.
  - **Internet Portals** are sites that aggregate a broader set of internet content and topics.
  - **Web Advertisement** are sites that contain advertisements, media content, and banners.
  - **Web based email** are sites offering web-based email and email clients.
  - **Internet Communications** are sites offering internet telephony, messaging, VoIP services, WiFi, and related businesses.
  - **Dynamically Generated Content** are sites that generate content dynamically based on arguments passed to the URL or other information (like geo-location).
  - **Parked Domains** are sites that host limited content or click-through ads that may generate revenue for the hosting entity, but generally do not contain content useful to the user.
• **Private IP Addresses and URLs** are sites assigned to a private domain and IP addresses reserved by organizations that distribute IP addresses for private networks.

• **Shopping**
  
  • **Auctions** support the offering and purchasing of goods between individuals as their main purpose, excluding classified advertisements.
  
  • **Shopping** sites are for department stores, retail stores, company catalogs and other entities that allow online consumer or business shopping and the purchase of goods and services.
  
  • **Shareware and Freeware** sites enable downloading free software, open source code, or downloads that request a donation, including screen savers, icons, wallpapers, utilities, and ringtones.

• **Entertainment**
  
  • **Entertainment and Arts** include motion pictures, videos, television, music and programming guides, books, comics, movie theaters, galleries, artists or reviews on entertainment, performing arts (such as theater, vaudeville, opera, or symphonies), museums, galleries, libraries, and artist sites (such as sculpture or photography).
  
  • **Streaming Media** are sites for sales, delivery, or streaming of audio or video content, including sites that provide downloads for such viewers.
  
  • **Peer to Peer** sites provide peer-to-peer clients and access, including torrents and music download programs.
  
  • **Games** sites are for game playing or downloading, video games, computer games, electronic games, tips and advice on games or how to obtain cheat codes. Also includes sites dedicated to selling board games, journals and magazines dedicated to game playing, support or host online sweepstakes and giveaways, and fantasy sports sites that also host games or game playing.
  
  • **Music** sites are for music sales, distribution, streaming, information on musical groups and performances, lyrics, and the music business.

• **Lifestyle**
  
  • **Travel** sites are for airlines and flight booking agencies, travel planning, reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
  
  • **Home and Garden** sites are about home issues and products, such as maintenance, home safety, decor, cooking, gardening, home electronics, and design.
  
  • **Religion** sites are about conventional or unconventional religious or quasi-religious subjects, including churches, synagogues, or other houses of worship.
  
  • **Hunting and Fishing** sites are about sport hunting, gun clubs, and fishing.
• Society sites cover a variety of topics, groups, and associations relevant to the general populace, and broad issues that impact a variety of people, including safety, children, societies, and philanthropic groups.

• Sports sites are team or conference websites, international, national, college, professional scores and schedules, sports-related online magazines or newsletters.

• Fashion and Beauty sites show fashion or glamor, magazines, beauty, clothes, cosmetics, and style.

• Recreation and Hobbies are sites with information, associations, forums, and publications on recreational pastimes such as collecting kit airplanes; outdoor activities such as hiking, camping, and climbing; specific arts, craft, or techniques; animal and pet related information, training, shows, techniques, and humane societies.

• Business/Government/Services

• Real Estate are sites for renting, buying or selling real estate or properties; tips on buying or selling a home; real estate agents; rental or relocation services and property improvement.

• Computer and internet Security are sites related to computer and internet security and security discussion groups.

• Financial Services are sites offering banking services and other types of financial information, such as loans, accountancy, actuaries, banks, mortgages, and general insurance companies, excluding sites that offer market information, brokerage or trading services.

• Business and Economy are sites for business firms, corporate websites, business information, economics, marketing, management, and entrepreneurship.

• Computer and Internet Info are sites containing general computer and internet information, including technical information. Also includes software as a service (SaaS) sites and other sites that deliver internet services.

• Military are sites for the military branches, armed services, and military history.

• Individual Stock Advice and Tools are sites that promote or facilitate securities trading and management of investment assets, including market information on financial investment strategies, quotes, and news.

• Training and Tools are sites for distance education and trade schools, online courses, vocational training, software training, and skills training.

• Personal Storage are sites that provide online storage and posting of files, music, pictures, and other data.

• Government are sites related to government (local, county, state, and national), government agencies, and government services such as taxation, public, and emergency services. Also includes sites that discuss or explain
laws of various governmental entities.

- **Content Delivery Networks** are sites for the delivery of content and data for third parties, including ads, media, files, images, and videos.

- **Motor Vehicles** are sites for car reviews, vehicle purchasing, sales tips, parts catalogs, auto trading, photos, discussion of vehicles, motorcycles, boats, cars, trucks and RVs, and journals and magazines on vehicle modifications.

- **Web Hosting** are sites that offer free or paid hosting services for webpages and information concerning their development, publication, and promotion of websites.

- **General Information**
  - **Legal** are sites related to legal topics and law firms as well as sites for discussions and analysis of legal issues.
  - **Local Information** are sites for city guides and tourist information, including restaurants, area/regional information, and local points of interest.
  - **Job Search** are sites that help find employment, tools for locating prospective employers, employers looking for employees, and career search and career placement from schools.
  - **Translation** refers to language translation sites that allow users to see pages in other languages. These sites can allow users to circumvent filtering as the target page’s content is presented within the context of the translator’s URL.
  - **Reference and Research** are sites for personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogs, genealogy, and scientific information.
  - **Philosophy and Political Advocacy** are sites for politics, philosophy, discussions, promotion of a particular viewpoint or stance to further a cause.
  - **Educational Institutions** are sites for pre-school, elementary, secondary, high school, college, university, and vocational school, and other educational content and information, including enrollment, tuition, and syllabus.
  - **Kids** are sites designed specifically for children and teenagers.
  - **News and Media** are sites with current events or contemporary issues of the day, including radio stations, magazines, newspapers, headline news sites, newswire services, personalized news services, and weather sites.
  - **Health and Medicine** are sites for general health, fitness, well-being, including traditional and non-traditional methods and topics. Also includes sites with medical information on ailments, various conditions, dentistry, psychiatry, optometry, and other specialties, hospitals and doctor offices, medical insurance, and cosmetic surgery.
• **Image and Video Search** are sites that provide photo and image searches, online photo albums, digital photo exchange, and image hosting.

• **Uncategorized Domains** are sites that Webroot has not categorized in any of the above categories.

• **Additional filtering.** Many search engines provide the option to impose a filter restricting explicit, adult, or inappropriate content. This can be done through DNS by returning the corresponding IP address associated with the filter.

  • When **Enable Google SafeSearch** is selected, DNS requests for www.google.com are resolved to forcesafesearch.google.com to filter explicit content from the search results.

  • When **Enable DuckDuckGo Safe Search** is selected, DNS requests for www.duckduckgo.com are resolved to safe.duckduckgo.com to filter adult content from the search results.

  • When **Enable Bing SafeSearch** is selected, DNS requests for www.bing.com are resolved to strict.bing.com to filter inappropriate content from the search results.

  • When **Enable YouTube Restricted Mode I Moderate Mode** is selected, DNS requests for www.youtube.com are resolved to restrictmoderate.youtube.com.

  • When **Strict Mode** is selected, DNS requests for www.youtube.com are resolved to restrict.youtube.com.

**Providing DNS Protection by deploying an agent**

When a DNS Protection agent is deployed and installed on an endpoint, the following occurs:

• The installation includes a service that inspects and saves the settings for the active network adapters at startup and when the connection status of a network adapter changes.

• It then sets the network adapter DNS settings (both IPv4 and IPv6) to loopback addresses, so that DNS requests are answered by the agent.

• The agent sends Active Directory or local DNS requests to the saved DNS settings, but filters internet DNS requests using the assigned DNS Protection policy.

• While the DNS Protection agent service is running, any network adapter DNS changes are disregarded and the changes are set back to the loopback addresses.

• If the service is stopped, the network adapter DNS settings are reverted to the saved settings.

• Certificates are automatically installed.

DNS Protection agents will automatically uninstall in the following situations:

• If you are using a trial of DNS Protection and it expires, DNS Protection is automatically uninstalled the next time the device checks in, and network adapter DNS settings are reverted to the saved settings.

• If the Endpoint Protection policy configuration is changed to no longer install DNS Protection, DNS Protection is automatically uninstalled the next time the device checks in, and network adapter DNS settings are reverted to the saved settings.
• If the Endpoint Protection policy a device is using is changed to a policy that does not have the DNS Protection installation configured, DNS Protection will be automatically uninstalled the next time the device checks in, and network adapter DNS settings will be reverted to the saved settings.

If the DNS Protection agent is uninstalled manually from a device, but the Endpoint Protection policy is still configured to install DNS Protection, DNS Protection will be installed the next time the device checks in.

**Using policies to deploy the DNS Protection agent**

Windows devices already running Endpoint Protection have the DNS Protection agent automatically installed using the **Install DNS Protection policy** setting in Endpoint Protection policies.

• The Endpoint Protection policy you use to install DNS must be a policy that you have created, copied, or imported. Default policies are not editable.

• The DNS protection agent is installed when the Endpoint Protection policy setting you have set up is enabled.

• Once DNS Protection is installed, all devices using that policy are protected.

• Only Windows devices can be protected using this method.

**To use a policy to deploy the DNS Protection agent:**

1. From either the **business view** or **service provider view**, navigate to **Manage > Policies**.
2. Select the **Endpoint Protection** tab.
3. Locate the Endpoint Protection policy for the devices on which you want to run DNS Protection. The policy you select must be a policy you created, copied, or imported. Default policies are not editable.
4. In the **Actions** menu, click **Edit**.
5. In the **DNS Protection** section, turn **Install DNS Protection** to **ON**.
6. Click **Save**.
7. Click **Back** to return to the policy list.

The next time devices using this policy check in, the DNS Protection agent is installed.

**Providing DNS Protection over a network**

By registering the IP address or domain associated with the network, **DNS Protection** can protect all devices on the network, even those not running the **DNS Protection** agent.

This allows you to control content on WiFi and guest networks as well as limit content available over different circuit types. The networks you specify forward DNS requests to specified Webroot DNS Protection servers for resolution.

The devices must be connected to the network, either on-site or using a VPN, to have **DNS Protection**.

Mac devices can have **DNS Protection** when using network-based protection.
Configuring the network

To configure the network for DNS Protection:

1. Go to the **DNS Protection** tab.
   - In **business view**, open the **DNS Protection** tab.
   - In **service provider view**, go to the **Sites List** tab, click the site you want to configure, then open the **DNS Protection** tab.

2. In the **Agent Settings** section, select the default policy.

3. In the **Domain Bypass List** section, you can enter one or more domains that should never be blocked by the Webroot DNS Protection servers. Enter a **Domain** and click **Add Domain**.
   - You can use wildcards to include all resources under a single domain.
   - Add more domains by adding additional rows.
   - You can add up to 500 entries.
   - If you need to edit or delete a row, use the **Actions** for that table row.

4. In the **Network Settings** section:
   a. Enter the **Domain/IP Address** for a network that you want to register to use the Webroot DNS Protection servers.
      - Use a WAN IP address.
      - To find your WAN IP address, open a web browser and search for "my IP."
   b. Select a **Policy** to use for this network.
      - There are two default policies, or you may have created your own.
   c. Click **Add Network**.
   d. Add more networks by adding additional rows, up to 250 entries.
   e. If you need to edit or delete a row, use the **Actions** for that table row.

All devices using this network now have Active Directory DNS requests handled by the Webroot DNS Protection servers.

5. In the **DNS Resolver Lookup** section, select a **Network Location** that is close to the physical location of your network. The Webroot DNS Protection servers that will be used as forwarders for external resolution for your DNS servers are displayed.

6. To filter DNS requests on servers, select **Enable Agent Install on Servers**. This provides visibility by server name of all internet requests that have been made from your servers. We do not recommend using this option on a DNS server as you may have resolution issues.

7. Click **Save**.

**To test your network configuration:**

1. From a device on the network, open the command prompt.
2. Query the domain by entering the following command:
NSLookup

3. Set the lookup server by entering the following command:
   server 35.226.80.229

4. Check several sites to confirm valid responses. Some network environments append a suffix to DNS lookups. For example, a dot (period) has been added to the end of www.webroot.com below to avoid possible resolution problems.

```
C:\users\administrator>nslookup
Default Server: domain.com
Address: 112.42.75.6

> server 35.226.80.229
Default Server: 54.55.54.45.wsadns.webroot.com
Address: 35.226.80.229

Server: 54.55.54.45.wsadns.webroot.com
Address: 35.226.80.229

Non-authoritative answer
Name: www.webroot.com.ssopt.net
Addresses: 69.25.154.83
64.95.189.177
Aliases: www.webroot.com
```

5. Update your routers or DNS forwarders to use the Webroot DNS Protection servers.
   - For example, on a Windows DNS server, go to Server Manager > Tools > DNS.
   - Right-click your DNS server in the tree and select Properties.
   - On the Forwarders tab, add the Webroot DNS Protection servers to the list of forwarders.

**Overrides for DNS Protection**

Overrides allow you to identify files and URLs that should be allowed or blocked regardless of a policy setting or how Webroot might define the file or URL.
In service provider view, Global file overrides are applied to all sites that have Include Global Overrides enabled in the site details.

Specific site rules always override global rules.

Policy settings take precedence over group settings.

Changes in overrides are applied to devices at their next polling interval, as configured in the Endpoint Protection policy that the device is using. To manually push changes out before that interval, use the Re-Verify Data agent command.

To access overrides, go to Manage > Overrides.

**Allowing and blocking websites for DNS Protection**

If you are not using DNS Protection, the allowed/blocked URLs specified in the Web Overrides tab are related to the Web Threat Shield policy settings.

If you are using DNS Protection, the web overrides specified in the Web Overrides tab are your DNS Protection overrides.

**DNS Protection reports**

Click Reports in the navigation pane to see all reporting options.

DNS Protection reports are only applicable if you are using DNS Protection.

- **DNS: Active Hosts** shows complete browsing history and internet usage.
- **DNS: Botnet Command & Control Blocked** shows sites categorized as a botnet using command and control software and have been blocked.
- **DNS: Top Blocked Category** shows sites most frequently blocked, by category.
- **DNS: Top Blocked Domain** shows the top 12 domains most frequently blocked.
- **DNS: Top Requested Category** shows the most frequently requested sites, by category.
- **DNS: Top Sites by Number of Requests** shows the number of requests by day for the top requested sites.
Security Awareness Training

Webroot Security Awareness Training works in conjunction with Webroot Endpoint Protection and is purchased separately. It is a hosted program designed to increase understanding and practical implementation of cybersecurity best practices. The program includes a phishing simulator, training courses, and other tools.

The Security Awareness Training modules are managed through campaigns. A campaign can be a single phishing simulation or set of training courses sent to a group of target users. Campaigns also provide reporting and management of your security awareness program.

Consider the following when designing and running campaigns:

- Everyone should participate. Include new hires and existing employees, across every department. Include all levels of employees. Service providers should train their own staff as well.
- Review the group receiving the campaign to make sure the training is relevant in terms of specific threats or risks and industry regulations and compliance.
- Do not assume any level of technical knowledge. Instead, start with basics and then get more specific.
- Provide clear participation guidelines to everyone receiving training.
- Behavioral change takes time.
- Security training should be reinforced on a regular basis.
- Consider running phishing simulations and training campaigns monthly.
- Measure, evaluate, and report routinely.
- Be aware that water cooler talk about a phishing test may skew the accuracy of the results.
- Communicate testing results to everyone and acknowledge employee participation.
- Communicate new risks regularly.

Getting started with Security Awareness Training

Before you begin, make sure your email server will not block the phishing and training emails sent to your users.

To get started with Security Awareness Training:

1. Register and set up Endpoint Protection. You do not need to deploy agents to use Security Awareness Training. See Getting started with Endpoint Protection on page 10.
2. Enable and configure Security Awareness Training. See Enabling Security Awareness Training on page 112.
3. Target users for training. See Targeting users for training on page 113.

Enabling Security Awareness Training

To enable Security Awareness Training:
1. Go to **Security Awareness Training**.
   - In **business view**, click **Security Awareness Training** in the navigation pane and then open the **Settings** tab.
   - In **service provider view**, click **Sites List** in the navigation pane, open the site, and then open the **Security Awareness Training** tab.

2. Turn on the **Security Awareness Training** switch.

3. If required, select your keycode type.
   - **Full** indicates a keycode that enables full use of the product with no limitations. You will be billed for this service.
   - **Trial** indicates a keycode that enables full use of the product, limited to a free, 30-day trial.

4. Click **Save**.

Once Security Awareness Training is enabled, there are two areas in the interface in which to manage its functionality.

To manage your campaigns, click **Security Awareness Training** in the navigation pane.

**To configure Security Awareness Training settings:**

- In **business view**, click **Security Awareness Training** in the navigation pane and then open the **Settings** tab.
- In **service provider view**, click **Sites List** in the navigation pane, open the site, and then open the **Security Awareness Training** tab.

**Targeting users for training**

Once Security Awareness Training is enabled, you need to target the users you want to include in training. This is done by identifying a domain that contains the users you want to target. If you are using the service provider view, you need to identify the domain for each site.

**To target users for training:**

1. Go to the settings for Security Awareness Training.
   - In **business view**, click **Security Awareness Training** in the navigation pane and then open the **Settings** tab.
   - In **service provider view**, click **Sites List** in the navigation pane, open the site, and then open the **Security Awareness Training** tab.

2. Configure the domain to use to target your users.
   1. In **business view**, use the options on the **Security Awareness Training > Settings** tab.
   2. In **service provider view**, click **Sites List** in the navigation pane, open the site, then open the **Security Awareness Training** tab.

3. You can either configure the domain automatically, using Active Directory Integration, or manually, using Domain Verification.
• **Active Directory Integration** synchronizes with Azure Active Directory to identify the domain. It also synchronizes a list of users in the domain that you can target for security training. See the [Knowledge Base](#).

You can see the synchronization status on the **Security Awareness Training settings** page. If needed, you can also click **Disable** to stop synchronizing from Azure.

• **Domain Verification** identifies the domain through a verification email, then enables users to be added. Email addresses on ISP or public domains (for example gmail.com) are restricted and cannot be used. Email addresses must be valid company or organization addresses.

  • In the **Add New Domain** box, enter an email address.
    • If the email you enter is a **Domain Member**, campaigns can be created and run, but the breach report is not accessible.
    • If the email you enter is a system level **Domain Admin** (i.e., administrator, info, postmaster, root, system, or webmaster), campaigns can be created and run, and the breach report is accessible.

  • Click **Send Verification Request** to send a verification email to the specified email address.

  • Once you get the email, click the verification link in the message to confirm access to that domain.

  • After access to the domain is confirmed, click **Security Awareness Training** on the navigation pane and open the **Users** tab.

  • Select a site (service provider view only)

• Click **Add Users to Site**.

  • **Enter Users Manually** indicates you will manually specify the name and email for each user you want to target for training.

  • **Set up Active Directory** integration synchronizes using Azure Active Directory. See the [Knowledge Base](#).

• **Upload Users from File** indicates you are going to import the users you want to target for training. The file should contain no more than 15,000 records.

  • **CSV** indicates a .csv comma-separated list of users. The file must contain the users' first name, last name, and email address. It can optionally contain a unique ID and tags.

  • **LDIF** indicates an .ldif file exported from LDAP/Active Directory. The following fields will be used to add users for training:
    • **givenname** (required) populates as the user's first name.
    • **sn** (required) populates as the user's last name.
    • **mail** (required) populates as the user's email address.
Managing users

You can add, edit, and delete users from within a site.

To manage users:

1. Click **Security Awareness Training** in the navigation pane and open the **Users** tab.
2. Click the site you want to work with (service provider view only).
3. Click **Add Users to Site**.

   - **Enter Users Manually** enables you to specify the name and email for each user you want to target for training.
   - **Upload Users from File** indicates you are going to import the users you want to target for training. The file should contain no more than 15,000 records.
     - **CSV** indicates a .csv comma-separated list of users. The file must contain the users' first name, last name, and email address. It can optionally contain a unique ID and tags.
     - **LDIF** indicates an .ldif file exported from LDAP/Active Directory. The following fields will be used to add users for training:
       - **givenname** (required) populates as the user's first name.
       - **sn** (required) populates as the user's last name.
       - **mail** (required) populates as the user's email address.
       - **objectGUID** (optional) populates as the user's unique ID.
       - **Ou** (optional) are organizational units that populate as tags.
     - **Select **Set up Active Directory integration** to synchronize using Azure Active Directory.
       - Click **Configure Now**.
       - Copy the **Secret Token** and use it to configure your Azure Active Directory tenant following the on-screen instructions.

To delete users from the site, select the check box next to the users' name and click **Delete Selected Users**.

Creating and managing distribution lists

You can create Security Awareness Training distribution lists to organize your users into groups. This is useful if you are sending phishing simulations or training courses to a subset of your users for targeted training.

To create and manage a distribution list:
1. Click **Security Awareness Training** in the navigation pane and open the **Users** tab.

2. Click the site you want to work with (service provider view only). This site should already be enabled for Security Awareness Training and have at least one user assigned.

3. Click the **Create Distribution List** button to create a new Security Awareness Training distribution list.
   - **Distribution List Name** specifies a name for the Security Awareness Training distribution list.
   - The **Company** list displays the available users. Click a user in this list to move it to the **Distribution List Members** list.
   - Use the **Search** boxes to narrow either list to only those users that meet the search criteria. Click the x to clear the search criteria.
   - Click **Add All** to add all of the users in the company list to the **Distribution List Members** list. If you have applied a search filter, only the entries showing in the **Company** list will be added.
   - The **Distribution List Members** list displays all users to be included in the distribution list. The list being displayed shows all users in the list, regardless of any search filtering. To remove a user, click a user name and move it back to the company name list.
   - Click **Remove All** to remove all items from the **Distribution List Members** list and move them back to the company name list.
   - Click **Save** to save the new Security Awareness Training distribution list.

To edit an existing distribution list, select the distribution list name, then click the **Edit Distribution List** button.

To delete an existing distribution list, select the distribution list name, then click the **Delete Distribution List** button.

**Creating a new campaign**

Before you begin, make sure your email server does not block the phishing simulation and training emails sent to your users.

1. Click **Security Awareness Training** on the navigation pane, and make sure the **Campaigns** tab is selected.

2. Click **New Campaign**. The New Campaign dialog is displayed.

3. Build the campaign in Section 1.
   - **Campaign Name** specifies a descriptive name for the campaign. This is only viewable by admins.
   - Select **Campaign Type** to specify the type of campaign to create.
     - **Phishing** is an email-based phishing simulation that will test and report on how many users clicked the phishing link.
• **Training** is a training campaign that will educate users and report on how many users completed the training. Selecting training provides a way to specify an optional title of the training campaign and an optional message on the landing page.

• Select **Email Template** to specify a template for your emails. You can filter the thumbnails displayed by entering search text or selecting a category filter.

• Click the **Customize Template** link to customize how the email will be delivered and displayed. Your intent for these fields will vary depending on if you are customizing an email for phishing or training. For example, for phishing you want the information to appear legitimate so that users are tested. For training, you want the information to appear legitimate so that users will not think it is phishing and delete the training invitation.

  • **Sender Name** is the name of the person, alias, group, or organization you want the email to be from.

  • **Sender Address** is the address that you want the email to be from.

  • **Email Subject** is the subject line of the email.

  • **Email Body** is the body of the email. You can edit the template image and also link to an image of your own. For more information about adding images to custom templates, see Linking an image from custom templates on page 120.

• Click **Save As New** to create a new template based on your customizations

• Click **Apply Edits** to modify the template you are customizing.

• Click **Landing Page URL** (phishing campaigns only) to select a domain. This is the URL the user will be sent to from the phishing email. You can customize the URL with a subdomain to make it more relevant to the phishing email or your users.

• In the **Landing Page** section (phishing campaigns only), select what you want to display when the **Landing Page URL** is clicked.

  • **Infographic** displays a web-based training page. It provides immediate education to users that they have clicked on a phishing simulation. This choice alerts users that a simulation is in progress.

    • **Select Infographic Template** enables you to choose the infographic to be displayed.

    • Click **Customize Template** if you want to modify the body of the infographic page.

  • **Broken Link** displays a 404 type of error page. This choice does not provide any immediate education. It tests users without alerting them that a simulation is in progress.

    • **404 Type** enables you to choose the type of broken link error to be displayed.
• **Lure Page** takes users to a web page and extends the simulation by testing to see if they will enter information. If users enter information, they will be redirected to a web-based training page. That page provides immediate education to users that they have clicked on a phishing simulation. If users make it this far, it alerts them that a simulation is in progress.

  - Select **Lure Page Template** enables you to choose the lure page to be displayed.
  - Click **Customize Template** to modify the body of the lure page.
  - **Destination Upon Posting Data** enables you to select an infographic to be displayed if the user enters information on the lure page.
  - Click **Customize Template** to modify the body of the infographic page.

• **Select Email Template** (training only) provides thumbnails from which to select a training invitation email template. These templates are fully customizable.

• **Select Training Courses** (training only) enables you to elect up to 10 courses per training campaign by scrolling through the thumbnails or filtering by course name using the **Search by name** box. You can also select a language for the training campaign and specify the display order on the landing page by dragging the courses to different positions in the selection list.

4. Select the sites to include in the campaign in Section 2. Click the heading to expand it.

  - The **Select Sites** table lists the available sites. It does not include expired sites or sites without any users. Click a site in this list to move it to the **Sites Selected** list.
    
    - Use the **Search** box to narrow either list to only those sites that meet the search criteria. Click the x to clear the search criteria.
    
    - Clicking **Show Distribution Lists** shows all available Security Awareness Training distribution lists. A distribution list only sends the campaign to those users in list, rather than all users in a site.
    
    - Click **Add All** to add all of the sites and distribution lists currently displayed in the **Select Sites** list to the **Sites Selected** list. If you have applied a search filter or are not showing Security Awareness Training distribution lists, only the entries showing in the **Select Sites** list are added.

  - The **Sites Selected** table lists all the sites and Security Awareness Training distribution lists to be included in the campaign. The list being displayed shows all items in the list, regardless of any search filtering. Click a site in this list to remove an item from the **Sites Selected** list and move it back to the **Select Sites** list.

  - Click **Remove All** to remove all items from the **Sites Selected** list and move them back to the **Select Sites** list.

5. Schedule the campaign in Section 3. Select the section to expand it.

  - Select **Auto-Enrollment** to automatically add new users to this campaign when they are added to the site or distribution list selected for the campaign. If the campaign is still
active, the new users will receive the campaign.

- **Launch Date** specifies the date you want the campaign to start. If you are automatically enrolling users,

- The **Duration** field is different depending on if you are automatically enrolling users. Users who attempt to access a campaign after it has ended see a message that the campaign is no longer active.

  - If you are automatically enrolling users, select the length of time enrolled users remain in the campaign. The campaign ends at 11:59 pm on the last day. If you select **Indefinitely**, the user remains enrolled in the campaign until the campaign is manually ended.

  - If you are not automatically enrolling users, select how long you want the campaign to run. If you do not set an end date, the campaign never expires, unless you manually end the campaign. If you set an end date, the campaign ends at 11:59 pm on the last day.

- **Delivery Time** is the time you want the campaign emails to be sent. Campaign scheduling times are specified according to the local computer time zone. For example, if your computer is using Eastern time and you select 10:00am, the time will automatically be adjusted to 7:00am when viewing on a computer using Pacific time.

  - **Deliver emails at time of launch** specifies that all the emails are sent as soon as the campaign starts.

  - **Deliver emails at custom time** sends all of the emails at the specified time.

  - **Spread email delivery out over period of days** spreads the delivery of the emails over the specified number of days.

- Select **After the campaign ends, send Campaign Summary Report automatically** to automatically send the administrator who created the campaign a report after the campaign has ended. If the campaign targeted multiple sites or distribution lists, the email contains links to download the reports for all of the sites or distributions lists that were included. Other administrators can access reports from the **Security Awareness Training** page.

6. Review the campaign in Section 4. Click the section to expand it. This section allows you to review the campaign configuration. Any campaign configuration settings that are incomplete are identified. In this section, you can also enter a single email address and click **Send Preview**. Repeat for multiple email addresses. Each email address receives a preview of what the campaign looks like and how it function.

7. Click one of the following buttons.

  - **Cancel** exits the campaign creation without saving. You will lose the campaign settings you have configured.

  - **Save & Close** exits the campaign and saves the campaign settings you have configured. The campaign remains in draft status and is not be started, even when the specified launch date is reached.

  - **Launch Campaign** exits the campaign, saves the campaign settings you have
configured, and starts the campaign when the specified launch date is reached. If the launch date is immediate, the campaign is started immediately.

**Linking an image from custom templates**

You can customize any email template with your own images by linking the image in your custom template. In accordance with our terms and conditions, you must comply with all relevant copyright and usage terms to use the image in your campaign.

Consider the following when adding images into your customized email template:

- The image address must be a valid URL hosted on the internet.
- The URL must be publicly accessible in a web browser.
- The image must not be hotlink-protected.
- The image must be available to be embedded in third-party websites.

**Enabling Autopilot**

Security Awareness Training enables you to target users with pre-scheduled training and phishing campaigns on a monthly basis using the Autopilot program.

**To enroll users in SAT Autopilot:**

1. In the Security Awareness Training section of the Management Console, click the Autopilot tab.
2. To familiarize yourself with the program, click View Autopilot Campaign Schedule.
3. Turn on the Autopilot switch.
4. (Optional) Enter a single email address to automatically send the Campaign Summary Report to when each campaign ends. Note that the message will contain a link to a single zip file that includes individual reports for each site enrolled in the campaign.
5. Select sites or distribution lists that you want to enroll into Autopilot campaigns.
6. Click Save.

**To disable Autopilot campaigns:**

1. Turn off the Autopilot switch.
2. To opt out of any scheduled Autopilot campaigns, go to the Campaigns tab.
3. On the Actions menu for the selected Autopilot campaign, click End Campaign.

For more information about SAT Autopilot, see the Frequently Asked Questions.

**Viewing and managing available campaigns**

To view the available campaigns, open Security Awareness Training from the navigation pane and make sure you are on the Campaigns tab. This page shows a high-level overview of the number of sites using Security Awareness Training and the number of campaigns for the last 90 days.

You are not limited to viewing only your own campaigns. You can see, edit, and launch draft campaigns created by other administrators.
The following controls are available on the Campaign Management table:

- **Enter text in the Search box** to narrow the list to only those rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Click New Campaign** to create a new campaign. See *Creating a new campaign* on page 116.
- **Click Filters** to open and close the filter panel. Select one or more filters to apply.
- **To sort** a column, click the column heading.
- **Click the campaign Name link** of an active, scheduled, or completed campaign to view the summary report for that campaign.
- **Click the Site name link** to go to the legacy Security Awareness Training console. This is an older console that will be phased out in the future.

- **Under Actions**, you can perform the following functions:
  - **End Campaign** immediately ends a campaign. Users who attempt to access a campaign after it has ended will see an error message.
  - **Send Reminder Now** immediately sends an email reminder to users who have not completed the training campaign.
  - **Edit Campaign** allows you to edit a campaign. This option is only available for draft campaigns.
  - **Archive Campaign** keeps a campaign that is completed and no longer active. You can review archived campaigns.
  - **Delete Campaign** deletes a draft campaign. You cannot review deleted campaigns.
  - **Copy Campaign** creates a copy of a campaign.
  - At the bottom of the Campaign Management table, rows and paging controls allow you to view more or less on a page and move between pages of the table.

### Viewing available training courses

To see the available training courses, go to Security Awareness Training and then select the Content Library tab.

The available training courses are categorized by tabs. Within a tab, you see the courses for that category including the course name, description, and length. Click on a training course to see how the course is graded and who the course publisher is. From the detailed course view, you can click Preview Course to go through the course yourself or click Add to Campaign to create a new campaign with the selected training course.

Text entered in the Search box narrows the courses displayed to only those that contain the search text. If desired, you can also click Download Source List as CSV to see the high-level details about each course in a .csv file.

### Viewing a campaign summary report

If your campaign has not yet launched, its status will be Scheduled. While the campaign is in Scheduled status, no data is generated. However, you can click the campaign Name link to view the campaign settings.
Once your campaign has generated activity, you can view its campaign summary report. Go to the Security Awareness Training tab and click the campaign Name link to view its summary report. The report is divided into sections as follows:

- The top section contains high-level information about the campaign, including the launch, duration, and enrolled users.

- **Results** are displayed in either Sankey or Bar Graph format, depending on which selection you choose. Below the chart are detailed results for each targeted user.
  - **Sankey** is the best option for evaluating more in-depth information about the campaign as the diagram shows all events logged for each user. The height of the dark vertical bar for each bucket represents the total number of users that have logged that type of event. Only one instance of an event is logged for each user, even if that user clicks the link multiple times. For more information about campaign events, see *Interpreting campaign events* on page 123.
  - **Bar Graph** is the best option for providing a quick reference as the chart only displays the most recent priority event logged for each user.

- **Email used** is the email used for the campaign.

- **Landing page** (phishing campaigns only) displays any lure, infographic, or broken link specified for the campaign.

- **Training courses** (training campaigns only) displays any courses specified for the campaign.

- Click **Export PDF** or **Export CSV** to download the summary report in that file format. The CSV file provides additional detailed activity data such as email delivery codes.
Interpreting campaign events

The following Security Awareness Training events map directly to the Sankey diagram shown in the campaign summary report:

- **Enrolled** – The target user has been enrolled in the campaign.
- **Processed** – The email message has been accepted and queued up for delivery.
- **Deferred** – Generally this means that the recipient server has deferred the delivery for a later time. This can occur when the recipient server is loaded and unable to receive the message at this time. The message will try to resend for up to 72 hours after the initial send was attempted.
- **Delivered** – The recipient email system has responded with a successful "delivered" message. However, once the email is inside of the recipient's network, the message may still be filtered/suppressed by internal spam filters.
- **Open** – This event is logged by loading an email tracking pixel and may be suppressed by the email client if the pixel is not loaded.
- **Click** – This event may have phantom logs due to spam systems probing the email URL(s), which will log a "click" event.
- **Education Visit** – The target user has visited the education page (infographic). This can be either directly from the phishing email or from the lure page (if enabled).
- **Lure Visit** – The target user has visited the phishing lure page. A click event will log from the user clicking the phishing email link, which directs the user to the lure page.
- **Training Visit** – The target user has visited the course launch page. This can be either directly from the training invite email or phishing email (if it is a hybrid campaign), or from interacting with a hybrid phishing campaign lure page (if enabled).
- **Campaign Complete** – The target user has successfully completed all activities assigned in a single campaign.

The remaining campaign events are mapped and tallied as follows:

- **Bounce** – This event is only tallied if all emails to the target bounce.
- **Dropped** – This event is only tallied if all emails to the target drop.
- **Training Started** – This bucket includes the following events: Training Attempted, Course Attempted, Training Passed, Training Complete, and Course Complete. It is only tallied if the user has attempted at least one course.

Security Awareness Training reports

Click **Reports** in the navigation pane to see all reporting options.

Security Awareness Training reports are only applicable if you are using Security Awareness Training.

- **SAT: Phishing Clicks** shows click rates by site.
- **SAT: Training Progress** shows training rates by site.
- **SAT: Usage Report** shows usage statistics.