Notices

Webroot Endpoint Protection, DNS Protection, and Security Awareness Training

Administrator Guide, revision Sunday, October 24, 2021

Information in this document is for the following products.

- Endpoint Protection
- DNS Protection
- Security Awareness Training

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 by 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.

© 2021 Webroot. All rights reserved.
Contents

Chapter 1 Overview ................................................................. 5
Chapter 2 Requirements .......................................................... 7
Chapter 3 Get started ............................................................. 10
  Register for a trial or purchase the product .................. 12
  Create an account ......................................................... 13
  Set up two-factor authentication .............................. 14
  Select Management Console view ........................... 15
  Create your first site (service providers only) ....... 17
  Deploy agent to devices ........................................... 21
  Enable DNS Protection ............................................. 22
  Install DNS Protection using an Endpoint Protection policy .. 23
  Enable Security Awareness Training ...................... 24
  Target the users for training ................................ 25
  Create your first phishing campaign .................... 27
Chapter 4 Management Console ............................................. 32
Chapter 5 Sites (service providers only) ................................. 35
  View available sites .................................................. 36
  Add a site .................................................................. 38
  Manage a site ............................................................. 42
Chapter 6 Dashboard ............................................................... 45
Chapter 7 Entities ................................................................. 48
  View available entities ............................................. 49
  Manage an entity ........................................................ 52
Chapter 8 Policies ................................................................. 54
  View available policies ............................................. 56
  Add a new policy ........................................................ 58
  Copy an existing policy .............................................. 59
  Import an existing policy from another site ........... 60
  Edit a policy ............................................................... 61
  Delete a policy ............................................................. 62
  Endpoint Protection policy settings ...................... 63
  Endpoint Protection policy best practices .......... 77
  DNS Protection policy settings ................................. 81
Chapter 9 Overrides ............................................................... 87
Chapter 10 Security Awareness Training ............................... 90
  Enable Security Awareness Training .................. 91
  Target the users for training ................................ 92
  Manage Security Awareness Training users and distribution lists 94
  View available campaigns ..................................... 97
  View available training courses ......................... 99
  Create a new campaign .......................................... 100
  View a campaign summary report ....................... 105
Chapter 11 Reports ................................................................. 106
  Run an on-demand report .................................................. 107
  Scheduled reports ............................................................ 109
    View available scheduled reports ................................... 110
    Add a scheduled report ................................................ 111
    View available scheduled report templates ....................... 113
    Add a scheduled report template ................................... 114
    View scheduled report history ....................................... 115
  Report types .................................................................... 116

Chapter 12 Alerts and alert distribution lists ......................... 118
  View and manage alerts and alert distribution lists ............... 119
  Add an alert .................................................................. 120
  Add an alert distribution list .......................................... 124

Chapter 13 Administrators .................................................. 125
  View available administrators ......................................... 126
  Add an administrator ..................................................... 127
  Edit an administrator .................................................... 129
  Delete an administrator ................................................ 130

Chapter 14 Settings ................................................................ 131

Chapter 15 DNS Protection ................................................. 136
  Assign the default DNS Protection policy ............................ 137
  Configure the network .................................................... 138

Chapter 16 Agents ............................................................... 140
  Install on Windows or MacOS using the installation wizard .... 142
  Install on Windows or MacOS from the command line .......... 143
  Install on Windows using Msiexec .................................... 145
  Install on Windows using group policy .............................. 146
Chapter 1 Overview

This Administrator Guide is for businesses who manage their own cybersecurity and for service providers who manage cybersecurity for their customers. It covers detailed aspects about three Webroot products, including how to use the Webroot Management Console.

- **Endpoint Protection**—Endpoint protection, or endpoint security, is a general term that describes cybersecurity services for network endpoints. Endpoints are laptops, desktops, smartphones, tablets, servers, and virtual machines. Endpoint protection and security may include antivirus and antimalware, web filtering, and more. It helps businesses keep critical systems, intellectual property, customer data, employees, and guests safe from ransomware, phishing, malware, and other cyberattacks.

  Webroot Endpoint Protection is for businesses who want to provide fast, effective, and easy-to-use security, for themselves or their customers, for laptops, desktops, servers, and virtual machines. It is a fully cloud-based endpoint security solution that uses the power of machine learning to continuously monitor devices for threat detection, protection, and prevention.

- **DNS Protection**—Webroot DNS Protection is a domain filtering service designed to provide granular control over Internet access. It protects users from malicious browser activity and enables Internet usage restrictions both across the network and independent of the network. DNS Protection protects your servers by registering the WAN IP address associated with the network. Desktops, laptops, and virtual machines will have Active Directory DNS requests handled by the server, and they can also use the DNS Protection agent to filter when off the network. (The agent is not supported on DNS or RDS Servers.)

- **Security Awareness Training**—The goal of a security awareness program is to increase understanding and practical implementation of security best practices. Webroot Security Awareness Training is a hosted security awareness program. It includes a fully-featured phishing simulator and training courses, managed through campaigns. A campaign is a single phishing simulation or training course sent to a group of users. Campaigns also provide reporting and management of your security awareness program.

  If you are not familiar with security awareness concepts and best practices, review the following list. Keep in mind, the list is not exhaustive because hackers are continuously coming up with new methods to try and bypass security.

  - **Malware**—Malware is a collective name for dangerous programs or code, including viruses, spyware, and ransomware. It is a shortened name for malicious software. Malware attacks are typically launched by clicking an infected attachment in an email.
    - **Virus**—A virus is a program that may replicate itself. It infects computer programs by inserting its own code.
    - **Spyware**—Spyware is a program that spies on computer activity.
    - **Ransomware**—Ransomware are programs that block access to data or threaten to publish data unless a ransom is paid.
  
  - **Social engineering**—Social engineering is a collective name for tricking users into revealing sensitive information. It also includes attempting to get users to download an attachment that will infect their computer and possibly the network with malware. Social engineering includes phishing, baiting, email hacking, and other manipulative tactics.
• **Phishing**—Phishing is sending a fraudulent email that appears to be from a reputable company in order to get the recipient of the email to make a purchase or payment or reveal sensitive information, like passwords or account numbers. Spear phishing is a targeted version of phishing.

• **Baiting**—Baiting is using a false promise to attract a victim's greed or curiosity. An example of physical baiting is leaving a malware-infected flash drive, baited to look authentic (company logo or identifier like a company payroll list) in a conspicuous area (lobby, parking lot, restroom, and so on). Someone who inserts the flash drive into a computer will have malware automatically installed. Online baiting can be enticing ads or promises that lead to malicious web sites or encourage someone to download a malware infected file.

• **Email hacking**—Email hacking is the unauthorized access to or manipulation of an email account or email correspondence. Email is an essential business communication method, but it can also serve as a tool for cybercrime, allowing hackers to invade your computer network.

• **Password security**—Password requirements should be complex enough to survive hackers’ attempts at brute force logins. Passwords should be updated regularly and after any potential security breach. When possible, use multi-factor authentication to add an extra layer of security.

• **Endpoint/Device security**—All operating systems and applications on all endpoints/devices (servers, desktops, laptops, tables, mobile devices) should be patched and up to date. Hackers take advantage of vulnerabilities in older or outdated systems and applications.

• **WiFi security**—Wireless connectivity should be limited to secure networks. Hackers can intercept data transmitted over public WiFi networks.

• **Mobile device security**—Mobile devices should only be used for company business on secure networks. Mobile devices pose a threat because they can be used for many functions. Mobile devices are often not secured and their small size and portability increase the risk of loss or theft.

• **Physical security**—Physical security includes not only the importance of physical awareness of portable devices (laptops, tables, phones), but also the importance of the physical office and its security.

• **Travel security**—All of the security awareness concepts and best practices are just as important, maybe even more so, when outside of the office.

---

Each Webroot product is separate. You may not have access to everything detailed in this documentation if you are not using all of the individual products.
Chapter 2 Requirements

Because Webroot products are services, there are generally no special requirements for devices. However, each product has a few general requirements.

- **Endpoint Protection**—These requirements apply to devices running Endpoint Protection.
  - **Operating system**—Endpoint Protection is supported on the following desktops and servers.
    - **Windows desktops**
      - Windows 11
      - Windows 10
      - Windows 8 and 8.1
      - Windows 7
    - **Windows servers**
      - Windows Server 2019 Datacenter Server with Desktop Experience and Standard Server with Desktop Experience
      - Windows Server 2016 Standard, Enterprise and Datacenter
      - Windows Server 2012 R2 Standard and Essentials
      - Windows Server 2008 R2 Foundation, Standard, and Enterprise
      - Windows Server 2003 Standard, Enterprise, and R2 for Embedded Systems
      - Windows Embedded Standard 2009 SP2 and SP3
      - Windows XP Embedded SP1
      - Windows Embedded for POS Version 1.0


- **Apple**
  - MacOS 11 Big Sur (Apple M1 ARM or Intel processors)
  - macOS 10.15 Catalina
  - macOS 10.14 Mojave
  - macOS 10.13 High Sierra
- **Firewall**—If your machines are using a firewall, you will need to open ports for access.
  - **Port 443**—Open port 443 for HTTPS for both inbound and outbound communication for the following:
    - *.webroot.com
    - *.*.webrootcloudav.com (or *.webrootcloudav.com if your firewall supports double dotted subdomain names)
    - wrskynet.s3.amazonaws.com/*
• wrskynet-eu.s3-eu-west-1.amazonaws.com/*
• https://wrskynet-oregon.s3-us-west-2.amazonaws.com/*

• **Port 80 and Port 443**—Open port 80 for HTTP and port 443 for HTTPS for both inbound and outbound communication for the following.
  • WSAWebFilteringPortal.elasticbeanstalk.com
  • *.webrootanywhere.com

**DNS Protection**—These requirements apply to the network environments configured for DNS Protection and to devices running the DNS Protection agent.

• **Firewall**—You must allow communication with the DNS Protection service through any firewalls.
  • **Network**—For network protection, you must open port 53 for outbound TCP and UDP communication to IP address 45.54.55.54 and 45.54.55.55.
  • **Agent**—For devices running the DNS Protection agent, you must open ports 443 and 5222 for outbound TCP communication to IP address 35.244.252.192.

• **VPNs**—Because some VPNs do not allow DNS requests to be filtered, not all VPNs are supported with the DNS Protection service. The following VPNs are supported.
  • **Network**—For network protection, you can use any of the following VPNs.
    • Cisco AnyConnect
    • Pure VPN
    • Safer VPN
    • SonicWall NetExtender
    • WatchGuard VPN
  • **Agent**—For devices running the DNS Protection agent, you can use any of the following VPNs.
    • Fortinet VPN
    • PulseSecure
    • SonicWall Mobile Connect

• **Security Awareness Training**—These requirements are needed to use Security Awareness Training.
  • **Phishing**—To receive the phishing simulation emails, users must have a valid email in the targeted domain.
  • **Training**—To view the training courses, most modern web browsers are supported.
  • **Email server**—Make sure your email server will not block the phishing simulation and training emails. You need to allow 167.89.85.54 for phishing simulation and 149.72.237.117 for training. If you are using Microsoft or Google, you may want to take additional recommended steps to allow emails through by email header as well. See the following articles for details.
    • [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](#)

• **Webroot Management Console**—There are no special restrictions or limitations to using the Webroot Management Console, however, keep in mind the following.
• Recent versions of Google Chrome, Mozilla Firefox, and Apple Safari are supported and are the preferred browsers.
• You can use Microsoft Edge and Opera, however you may experience layout or appearance issues.
• Microsoft Internet Explorer is not supported.
Chapter 3 Get started

Because Endpoint Protection is required to use the other products, you should start with the Endpoint Protection process. This will help you become familiar with basic concepts in the Webroot Management Console. You can build from there by adding DNS Protection and Security Awareness Training.

- **Endpoint Protection**—You need to complete the following sections, in order, to get started using Endpoint Protection.
  1. *Register for a trial or purchase the product* on page 12—You should have completed this step already, but if you have not, you should register for a trial version or purchase product.
  2. *Create an account* on page 13—you will need to create an account to access the Webroot Management Console.
  3. *Set up two-factor authentication* on page 14—you can optionally set up two-factor authentication (2FA) to help prevent unauthorized access to your account.
  4. *Select Management Console view* on page 15—Each organization is assigned its own Management Console. In some cases, you may be assigned more than one Management Console. The Management Console has two different views. One view, called the business view, is generally used by an organization managing their own security. The second view, called the service provider view, is generally used by an organization managing security for other customers. The first time a new console is accessed (after configuring or skipping 2FA), the Management Console view will need to be established.
  5. *Create your first site (service providers only)* on page 17—if you selected the service provider view, you need to create your first site. This step is not applicable to the business view and can be skipped. Sites are only available in the Management Console service provider view. They are representations of your customers. They may be businesses or companies, or they can also represent departments, regions, office locations, or other organizational units you might want to designate. Sites allow you to manage a large number of devices by your defined organizational units.
  6. *Deploy agent to devices* on page 21—Finally, you can deploy agents to devices and begin protecting them. 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.

- **DNS Protection**—The easiest way to get started with DNS Protection is to use devices that are already running Endpoint Protection. You can easily test the DNS Protection functionality and when you are comfortable with it, go back and configure and customize additional DNS Protection settings.

Make sure you have completed the get started process for Endpoint Protection and have Endpoint Protection successfully running on at least one device, then complete the following two steps to get started with DNS Protection.

  1. *Enable DNS Protection* on page 22—if you have not already enabled DNS Protection, you will need to do that first.
  2. *Install DNS Protection using an Endpoint Protection policy* on page 23—for devices already running Endpoint Protection, you need to enable one option in the
Endpoint Protection policy to install DNS Protection on all devices using that policy. Once DNS Protection is installed, the device is being protected.

- **Security Awareness Training**—For your first Security Awareness Training campaign, you need to complete the following sections, in order, to get started using Security Awareness Training. (These steps are based on having already completed steps 1-5 under Endpoint Protection.)

  1. *Enable Security Awareness Training* on page 24—If you have not already enabled Security Awareness Training, you will need to do that first.
  2. *Target the users for training* on page 25—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 for security training. If you are using the service provider view, you need to identify the domain for each site.
  3. *Create your first phishing campaign* on page 27—After you have verified the domain to use for security training, you can create and launch your first campaign.

  Make sure your email server will not block the phishing simulation and training emails sent to your users. See *Requirements* on page 7 for details.
Register for a trial or purchase the product

If you have not registered for a trial or purchased a product, use the following steps. If you already have registered for a trial or purchased a product, continue with Create an account on page 13.

2. Click For Business in the navigation menu.
3. Under Products in the menu, click Endpoint Protection.
4. Click How to Buy or scroll down to the Trial or Buy section.
5. Determine if you want to register for a trial or purchase product.
   - **Trial**—If you want to register for a trial, click Start Trial, select the Webroot Business Endpoint Protection product as well as other products desired, and click Add Trial. Follow the on-screen steps to activate the trial.
   - **Purchase**—If you want to purchase product, click Buy Now and follow the on-screen steps to purchase product. If you need to purchase large subscriptions, contact sales at the on-screen number.

---

Endpoint Protection is required to trial or purchase any of the additional products.
Create an account

After you have registered for a trial or purchased product, you will receive a welcome email. Generally within 5-10 minutes after the welcome email, you will receive another email to create an account to access the Webroot Management Console.

1. Click the registration link in the email you received.
2. Use the temporary password from the email on the registration page.
3. Enter your new password, security information, and phone number.

If you are not using two-factor authentication, the security code is used when you log in. You will be asked to enter two of the security code characters, randomly selected by position.

4. Make sure you agree to the terms and click Confirm.
Set up two-factor authentication

Once your account is active, you can set up two-factor authentication (2FA) to help prevent unauthorized access to your account. This is an optional step.

1. Install an authenticator app on an Android or iOS mobile device or tablet. You can use Google Authenticator, Microsoft Authenticator, LastPass Authenticator, Authy 2-Factor Authentication, or any other authenticator app.

2. Log in to the Management Console at https://my.webrootanywhere.com/.

3. If this is your first time logging in, you will be prompted to set up 2FA. Click Setup 2FA. If you previously skipped setting up 2FA, go to the Admins tab and click your name in the list. In the Login Settings box on the right click Enable 2FA.

4. When prompted, select and answer your two security questions and click Continue.

5. 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. Keep in mind, the code is case-sensitive.

6. After you have scanned or entered the code, you will receive a verification code. Enter the code in Step 4 in the Management Console and click Verify Code.

7. Confirm your successful verification. If verification failed, you will need to enter a new code from your authenticator app. Keep in mind, codes are only valid for 30 seconds.

8. Once successful, click Go to Console and log in again.

With two-factor authentication, you will use the code from the authenticator app each time you log in, rather than your personal security code. If you are not using two-factor authentication, the security code is used when you log in. You will be asked to enter two of the security code characters, randomly selected by position.
Select Management Console view

Each organization is assigned its own Management Console. In some cases, you may be assigned more than one Management Console. The Management Console has two different views. One view, called the business view, is generally used by an organization managing their own security. The second view, called the service provider view, is generally used by an organization managing security for other customers. The first time a new console is accessed (after configuring or skipping 2FA), the Management Console view will need to be established.

1. Log in to the Management Console at https://my.webrootanywhere.com/.

2. If this is the first time this console is being accessed, you will be prompted to select your Management Console view. If someone else has already logged into this console, that person will have already selected the console view.

   ![Select Management Console view](image)

   - **Business**—If you are managing devices within your own business and are using a single keycode for all devices and billing, click Select under Business. This option will show a single site display in the Management Console. (You can use groups to help organize your devices.)
   - **Managed Service Provider**—If you are managing devices for multiple customers (companies, businesses, organizational units, and so on) and are using separate keycodes and billing for each, click Select under Managed Service Provider. This option will show multiple sites in the Management Console.

     If you select the business option, you can upgrade to the service provider option later. Selecting the service provider option is not reversible.

3. If you selected the business view, you need to define your company. You will not see this screen, if you selected the service provider view or if someone else has already selected the business view and defined the company.

Chapter 3 Get started
Please complete the following information:

**BUSINESS**

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

* Indicates a required field

**Site/Company Name** *

Number of Devices *

**Company Industry** *

Select an Industry

**Company Size** *

Select a Company Size

Click **Select** to complete the company configuration.

- **Site / Company Name**—Specify a unique name for the site or company.
- **Number of Devices**—Specify the number of devices that will be managed.
- **Company Industry**—Select the industry that represents the company.
- **Company Size**—Select the range that represents the size of the company.
Create your first site (service providers only)

If you selected the service provider view in the Management Console, you need to create your first site. If you selected the business view, this section is not applicable to your configuration and can be skipped.

Sites are only available in the Management Console service provider view. They are representations of your customers. They may be businesses or companies, or they can also represent departments, regions, office locations, or other organizational units you might want to designate. Sites allow you to manage a large number of devices by your defined organizational units.

1. Click Sites List and then click Add Site.
2. In the first step of the Add Site wizard, configure your site details.

- Site / Company Name—Specify a unique name for the site or company.
- Site Type—Select the type of site.
  - External Company—Select this option if the site is an external company that is purchasing services from you.
  - Internal Site—Select this option if the site is within your own company, for example a location or office.
- Company Size—if you selected an external company, select the range that represents the size of the company. This field will be hidden if you selected an internal site.
- Company Industry—if you selected an external company, select the industry that represents the company. This field will be hidden if you selected an internal site.
• **Billing Cycle**—If you selected an external company, select a billing cycle. This is a billing cycle that you define and use as needed for this site. This is not a billing cycle associated with Webroot. This field will be hidden if you selected an internal site.

• **Billing Date**—If you selected an external company, select a month and date for billing. This is a billing date that you define and use as needed for this site. This is not a billing date associated with Webroot. This field will be hidden if you selected an internal site.

• **Report Distribution List**—Specify a comma-separated list of up to ten email addresses. Each address will receive the generated reports that are configured to be sent to the report distribution list.

• **Include Global Policies**—When enabled, all global policies will be available for this site to use. When a global policy is being used and that global policy changes, each device using the policy will get the change. Once enabled, this option cannot be changed. When disabled, global policies will not be used and only the default policies, without future changes, will be available.

• **Include Global Overrides**—When enabled, global policy overrides will be 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 will use that override and block that file. When this option is disabled, global overrides from other sites will not be applied to this site, and all overrides for this site will have to be manually configured.

• **Comments**—Optionally enter any comments describing the site or company.

• **Tags**—Optionally select a tag to label this site. This is useful if you want to filter sites by tags.

3. Click **Next** to continue.

4. In the second step of the **Add Site** wizard, select the permissions to grant to this site. By default, the account that created the site will be given full administrator permissions, so you will not see that account in the list. All other accounts will be listed and default to **No Access**. If you want other administrators to be able to view or access this site, you must grant those administrator permissions.

   ![Add Site wizard screenshot](image)

   - **Admin**—This permission level allows full access to the site.
   - **View Only**—This permission can only view the site. There is no management or control available.
   - **No Access**—This permission 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**—Select Full if you purchased product or **30 day trial** if you registered for a trial.

- **Site Seats**—Specify the number of seats (endpoints or devices) for the site or company you are configuring. This setting is for your internal reference. It is not used for billing.

- **Default Endpoint Policy**—Select a default policy. The selected policy will be used for all new devices that are installed for this site or company, unless the policy is assigned using inheritance from the group, site, or company for the device. (You can modify the policy the device uses after installation.)
  - **Recommended Defaults**—This policy is intended for desktops and laptops. User interface and PUAs (possibly unwanted applications) are disabled. The setting to install DNS Protection is disabled in this policy.
  - **Recommended DNS Enabled**—This policy is identical to **Recommended Defaults**, except the setting to install DNS Protection is enabled.
  - **Recommended Server Defaults**—This policy is intended for server environments. It focuses on resource utilization and minimal impact on the server.
  - **Silent Audit**—This policy is based on the **Recommended Defaults** policy, however, it has the remediation function disabled to minimize production impact. This means it will catch known threats, but not undetermined threats. Use the undetermined threats reports to help you identify items to add to your block and allow overrides. Generally, this policy should only be used for a short duration, for example during initial setup to identify potential production false positives.
  - **Unmanaged**—This policy is intended for technical support, troubleshooting, and when no policy management is needed. This policy cannot be managed, but it turns the agent into a local, unmanaged application that can be controlled directly by the end-user. You should not use this policy in production.

- **Data Filter**—If you want to limit the data that is displayed in the console, you can apply data filters. These filters will show or hide data depending on your filter. For example, if you select **2 Months**, all devices that have not connected for two months will be excluded from the data shown for this site. This option 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.

7. Click **Next** to continue.

8. You can optionally configure DNS Protection. If you skip this for now, you can enable it later from the **Settings** tab. See **Enable DNS Protection** on page 22 if you are just getting started or see **DNS Protection** on page 136 for details.

9. Click **Next** to continue.

10. You can optionally configure Security Awareness Training. If you skip this for now, you can enable it later from the **Settings** tab. See **Enable Security Awareness Training** on page 24 if you are just getting started or see **Security Awareness Training** on page 90 for details.

11. Click **Save** to complete the site configuration and to assign a keycode to the site.
Deploy agent to devices

Once you have a site configured, you can deploy the Webroot agent to devices and begin protecting them.

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.

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

- **DNS Protection**—If you will be using DNS Protection on devices to filter DNS requests when the devices are off the network, you will use the same agent that is used with Endpoint Protection.

The agent installation files are .exe for Windows and .dmg for Apple.

1. Locate the installation file download links in the Management Console.
   - **Business view**—If you are using the business view, go to the **Settings** tab and then the **Downloads** tab to find the installation file download links.
   - **Service provider view**—If you are using the service provider view, use the following steps to locate the installation file download links.
     a. In the Management Console, click **Sites List**.
     b. Locate your site in the list and click the site name hyperlink.
     c. Click the **Endpoint Protection** tab.

2. Select the Windows or Apple download link as appropriate to download the file.
3. Copy the **Keycode** for your company or for the site.
4. Copy, post, email, or use another method to get the installation file to the device you want to install on.
5. Install the agent.
   - For Windows, run the .exe file.
   - For Apple, run the .dmg file and then open the **Applications** folder and double-click the Webroot icon to launch the installer.

Follow the on-screen prompts to complete the installation.

Once the installation is complete and the agents check in with the Management Console, you will see the **Devices** column populate. The agent should complete the first scan for threats in seconds or minutes and report back to the Management Console. If DNS Protection is enabled, filtering will begin immediately.
Enable DNS Protection

If you have not already enabled DNS Protection, you will need to do that first. If you have already enabled it, continue with *Install DNS Protection using an Endpoint Protection policy* on page 23.

The process for enabling DNS Protection is different depending on your console view.

- **Business view**
  1. Go to the DNS Protection tab.
  2. Enable the setting *Enable SecureAnywhere DNS*.
  3. Select your keycode type.
     - **Full**—This option is the full product with no limitations. You will be billed for this service.
     - **Trial**—This option is the full product, however, it is limited to a free, 30-day trial.
  4. Click *Save Changes*.
  5. Continue with *Install DNS Protection using an Endpoint Protection policy* on page 23.

- **Service provider view**
  1. Click *Sites List*.
  2. For the site that you want to enable DNS Protection, click one of the following buttons in the DNS Protection column.
     - **Start Trial**—This button starts a free, 30-day trial.
     - **Upgrade**—This button converts a trial to a full version. You will be billed for this service.
  3. When starting a trial, you will be prompted to take two actions. Review these steps, but they are not required to get started.
     - **Download Software**—Clicking this button will take you to the site management Endpoint Protection tab where you can download the agent software for installation. You would only need to perform this step if you are using DNS Protection on devices that do not have Endpoint Protection. Devices that have Endpoint Protection already running can have DNS Protection installed using an Endpoint Protection policy setting. To get started, use at least one device that has Endpoint Protection successfully running on it.
     - **Configure DNS Settings**—Clicking this button will take you to the site management DNS Protection tab where you can customize your DNS network settings. This step allows you to protect servers by registering the WAN IP address associated with the network. You do not need to configure this setting to get started.
  4. Close the dialog box and continue with *Install DNS Protection using an Endpoint Protection policy* on page 23.
Install DNS Protection using an Endpoint Protection policy

For devices already running Endpoint Protection, you need to enable one option in the Endpoint Protection policy to install DNS Protection on all devices using that policy. Once DNS Protection is installed, the device is being protected.

1. Click Manage and then click Policies. Select the Endpoint Protection tab.
2. Locate the Endpoint Protection policy for the devices where you want to run DNS Protection.
3. Using the Actions menu at the right side of the table row for that policy, select Edit. You will only see this menu option if it is a policy you created, copied, or imported. Default policies are not editable.

4. In the DNS Protection section, enable the option Install DNS Protection.
5. Click Save.
6. Click Back to go back to the policy list.

The next time devices using this policy check in, the DNS Protection agent will be installed.
Enable Security Awareness Training

If you have not already enabled Security Awareness Training, you will need to do that first. If you have already enabled it, continue with Target the users for training on page 25.

1. If you are using the business view, go to the Security Awareness Training tab. If you are using the service provider view, go to Sites list, click the site name hyperlink, and then within the site details, click the Security Awareness Training tab.

2. Enable Security Awareness Training.

3. Select your keycode type.
   - **Full**—This option is the full product with no limitations. You will be billed for this service.
   - **Trial**—This option is the full product, however, it is limited to a free, 30-day trial.

4. Click Save.
Target the 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 for security training. If you are using the service provider view, you need to identify the domain for each site.

1. If you are using the business view, go to the Security Awareness Training tab. If you are using the service provider view, go to Sites list, click the site name hyperlink, and then within the site details, click the Security Awareness Training tab.

2. Select the type of domain identification you want to use and complete the associated process.
   - **Active Directory Integration**—This method synchronizes with Azure Active Directory to identify the domain. It will also synchronize a list of users in the domain that you can target for security training.
     a. Click Configure Azure AD Integration.
     b. Copy the Secret Token that is displayed and use it to configure your Azure Active Directory tenant following the on-screen instructions.

You can see the synchronization status and the last update from Azure Active Directory. If needed, you can also click Disable to stop synchronizing from Azure.

   - **Domain Verification**—This method identifies the domain through a verification email and then users are added.
     a. Enter an email address in Add New Domain.
        - **Domain Member**—If the email address you enter is a member of the domain, campaigns can be created and run, but the breach report will not be accessible.
        - **Domain Admin**—If the email address you enter is a system level email on the domain (admin, administrator, info, postmaster, root, system, or webmaster), campaigns can be created and run, and the breach report will be accessible.

> 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.

   b. Click Send Verification Request to send a verification email to the specified email address.
   c. Once you get the email, click the verification link in the message to confirm access to that domain.
   d. After access to the domain is confirmed, go to the main Security Awareness Training tab and click the Users tab.
   e. Select a site.
   f. Click Add Users to Site.
   g. Select how you want to add the users.

   - **Enter Users Manually**—Select this option and manually specify the name and email for each user you want to target for training.
- **Upload Users from File**—Select this option to import the users you want to target for training. The file should contain no more than 15,000 records.
  - **CSV**—You can use 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**—You can use an .ldif file exported from LDAP/Active Directory. The following fields will be used to add users for training:
    - `givenname`—This entry is required and will be populated as the user's first name.
    - `sn`—This entry is required and will be populated as the user's last name.
    - `mail`—This entry is required and will be populated as the user's email address.
    - `objectGUID`—This entry is optional and will be populated as the user's unique ID.
    - `ou`—These entries (organizational units) are optional and will be populated as tags.
- **Set up Active Directory integration**—Select this option to synchronize using Azure Active Directory.
  a. Click **Configure Now**.
  b. Copy the **Secret Token** that is displayed and use it to configure your Azure Active Directory tenant following the on-screen instructions.

---

If you want to send phishing simulations or training courses to a subset of your users for targeted training, you can create Security Awareness Training distribution lists to organize your users into groups. See *Manage Security Awareness Training users and distribution lists* on page 94 for details.
Create your first phishing campaign

Ideally for your first phishing campaign, you want to gauge how susceptible users are to phishing and determine the general level of security awareness. An email that appears to be an internal communication from HR or IT will get the most attention. You should use a 404 broken link response to minimize recognition of the phishing test. By minimizing water cooler talk about a phishing test, you will get more accurate results.

1. Go to the Security Awareness Training tab.
2. Click New Campaign.
3. Build the campaign. The campaign settings are under the first heading.

- **Campaign Name**—Specify a descriptive name for the campaign. This is for your use only, not something the users will see.

- **Campaign Type**—For your first campaign, select Phishing. This is an email-based phishing simulation. It will test and report on how many users clicked the phishing link.

- **Select Email Template**—Scroll through the thumbnails that show the phishing emails. You can filter the thumbnails displayed by entering search text or selecting a category filter. For your first campaign, you could search on the word Bonus and select the HR: Bonus Increase template, which looks like an email from HR.

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**—Specify the name of the person, alias, group, or organization you want the email to be from.
- **Sender Address**—Specify the address that you want the email to be from.
- **Email Subject**—Specify the subject line of the email.
- **Email Body**—Specify the body of the email.

After you have customized the email template, you can click **Save As New** to create a new template based on your customizations or click **Apply Edits** to modify the template you are customizing.

- **Landing Page URL**—Select a domain. This is the URL the user will be sent to from the phishing email. You can optionally customize the URL with a subdomain to make it more relevant to the phishing email or your users.
- **Landing Page**—Select what you want to display when the **Landing Page URL** is clicked.
  
  - **Infographic**—This option will display a web-based training page. It provides immediate education to users that have clicked on a phishing simulation. This choice alerts users that a simulation is in progress.
    
    - **Select Infographic Template**—Select an infographic that will be displayed. Click **Customize Template** if you want to modify the body of the infographic page.
  
  - **Broken Link**—This option will display 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**—Select the type of broken link error that will be displayed.
  
  - **Lure Page**—This option 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 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**—Select the lure page that will be displayed. Click **Customize Template** if you want to modify the body of the lure page.
    
    - **Destination Upon Posting Data**—Select an infographic that will be displayed if the user enters information on the lure page. Click **Customize Template** if you want to modify the body of the infographic page.

4. Click the second heading to expand it. This section allows you to select the sites to include in the campaign.
• **Select Sites**—This 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.

• **Search for**—Using search, you can narrow either list to only those sites that meet the search criteria. Click the x to clear the search criteria.

• **Show Distribution Lists**—If you have Security Awareness Training distribution lists created, you can enable this option to view the Security Awareness Training distribution lists associated with each site. A selected Security Awareness Training distribution list will only send the campaign to those users in the Security Awareness Training distribution list, rather than all users in a site.

• **Add All**—Click this link to add all of the sites and Security Awareness Training 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 will be added.

• **Sites Selected**—This table lists all of the sites and Security Awareness Training distribution lists that will be included in the campaign. Even if you are using search to narrow the displayed list, all of the sites in the list will be included in the campaign. Click a site in this list to remove an item from the **Sites Selected** list and move it back to the **Select Sites** list.

• **Remove All**—Click this link to remove all items from the **Sites Selected** list and move them back to the **Select Sites** list.

5. Select the third section to expand it. This section allows you to schedule the campaign.
- **Auto-Enrollment**—Select this option to automatically add new users to this campaign when they are added to the site or distribution list selected for the campaign. As long as the campaign is still active, the new users will receive the campaign.

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

- **Duration**—This field is different depending on if you are automatically enrolling users.
  - **Automatic enrollment**—If you are automatically enrolling users, select the length of time enrolled user will remain in the campaign. The campaign will end at 11:59pm on the last day. If you select **Indefinitely**, the user will remain enrolled in the campaign until the campaign is manually ended.
  - **No automatic enrollment**—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 will never expire, unless you manually end the campaign. If you set an end date, the campaign will end at 11:59pm on the last day.

Users who attempt to access a campaign after it has ended will see a message that the campaign is no longer active.

- **Delivery Time**—Select the time when you want the campaign emails to be sent.
  - **Deliver emails at time of launch**—This option sends all of the emails as soon as the campaign starts.
  - **Deliver emails at custom time**—This option sends all of the emails at the specified time.
  - **Spread email delivery out over period of days**—This option spreads the delivery of the emails over the specified number of days.

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.
• **After campaign ends, send Campaign Summary Report automatically**—Select this option 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 will contain 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. See *View a campaign summary report* on page 105 for details.

6. Click the fourth 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 addresses and click **Send Preview**. Repeat for multiple email addresses. Each email address will see a preview of what the campaign will look like and how it will function.

7. Click one of the following buttons.

  • **Cancel**—This button will exit the campaign creation. You will lose the campaign settings you have configured.

  • **Save & Close**—This button will exit the campaign and save the campaign settings you have configured. The campaign will remain in draft status and will not be started, even when the specified launch date is reached.

  • **Launch Campaign**—This button will exit the campaign, save the campaign settings you have configured, and start the campaign when the specified launch date is reached. If the launch date is immediate, the campaign will be started immediately.

---

Make sure your email server will not block the phishing simulation and training emails sent to your users. See *Requirements* on page 7 for details.
Chapter 4 Management Console

Log in to the Management Console at https://my.webrootanywhere.com/.

If this is the first time anyone has accessed the Management Console, you need to complete the initial console configuration.

1. *Create an account* on page 13—You must have an account to access the Management Console.
2. *Set up two-factor authentication* on page 14—You can optionally set up two-factor authentication (2FA) to help prevent unauthorized access to your account.
3. *Select Management Console view* on page 15—The first time the Management Console is accessed (after configuring or skipping 2FA), you will need to select your console view.

What you see in the Management Console is dependent on the console view you are using (business or service provider) and the access granted to your account. The console is organized with navigation on the left and interactive pages on the right.

- **Management Console Business View**

![Management Console Business View](image)

- **Management Console Service Provider View**

![Management Console Service Provider View](image)
• **Navigation**—You can get to the main console pages by using the navigation links at the left side of the console. You can collapse and expand the size of the navigation links using the < or > icon at the bottom of the navigation pane.

• **Console switcher**—In most cases, your console name will be statically displayed. In a few cases when you have been assigned more than one Management Console, the console name will be a drop-down list of the consoles you have access to. This list is called the console switcher and it allows you to select a different console to switch to that console view. You also have the ability to rename your console, if needed. Keep in mind that renaming a console will change the name for everyone who logs in to that console.

• **Sites List**—If you are using the service provider view, this tab shows all of the sites you have access to. You can view and manage individual sites from this page. See *Sites (service providers only)* on page 35 for details. If you are using the business view, you will not see this tab.

• **Dashboard**—The Dashboard tab gives you 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 45 for details.

• **Manage**—This tab contains three management sub-tabs.
  
  • **Entities**—Entities are your devices and groups. Devices are the endpoints. Groups are organizational units. Groups allow you to manage devices together, for example to apply a specific policy to a group of devices. The Entities tab is where you view, organize, and manage the devices and groups. See *Entities* on page 48 for details.

  • **Policies**—A policy configures the behavior of the agent, for example, how often a device is scanned, what scan settings are used, how the scan is performed, and so on. There are several default policies for Endpoint Protection and DNS Protection which can be used as is or they can be modified to fit your specific needs. There is
also an Endpoint Protection unmanaged policy which allows end-users to select and manage their own settings. See Policies on page 54 for details.

- **Overrides**—Overrides allow you to identify files and URLs that should be allowed or blocked, overriding a policy setting or how Webroot might define the file or URL. See Overrides on page 87 for details.

- **DNS Protection**—If you are using the business view, this tab shows the DNS protection configuration. See DNS Protection on page 136 for details. If you are using the service provider view, you will not see this tab because DNS protection is managed per site. To see the DNS protection configuration for a site, you need to see the site configuration. See Manage a site on page 42 for details.

- **Security Awareness Training**—This tab is where you manage your Security Awareness Training campaigns. See Security Awareness Training on page 90 for details.

- **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. See Report types on page 116 for details on the different reports available. See Reports on page 106 for details.

- **Alerts**—An alert is an email notifications to notify you when a threat is detected or when the Webroot agent is installed on a device. You can also generate alerts that are threat and installation summaries. An alert distribution list is a list of one or more email addresses that alerts will be sent to. See Alerts and alert distribution lists on page 118 for details.

- **Admins**—This tab shows the administrators, or accounts, that exist in your console. See Administrators on page 125 for details.

- **Settings**—This tab contains various configuration sections. The available configurations vary if you are using the Management Console business view or the service provider view. See Settings on page 131 for details.

- **Resources**—No matter which page you are on in the console, there are several links at the upper right corner of the page that provide access to common resources and links.

  - **Resource center**—The inside the circle is the Resource center. It includes links to service status and general product information.

  - **Help and Support**—The question mark inside the circle is for help and support. It includes documentation resources and a link to the support site where you can open a support ticket. Once the ticket is submitted, it will be immediately available to Webroot support representatives.

  - **Log out**—Under your login name, you will find the link to log out of the console.
Chapter 5 Sites (service providers only)

Sites are only available in the Management Console service provider view. They are representations of your customers. They may be businesses or companies, or they can also represent departments, regions, office locations, or other organizational units you might want to designate. Sites allow you to manage a large number of devices by your defined organizational units.

The following tasks are available for sites.

- View available sites on page 36
- Add a site on page 38
- Manage a site on page 42
View available sites

To view your available sites, click Sites List. The table lists the sites you have access to, including high level information about each site.

A white exclamation point in a blue circle next to the number of devices indicates a data filter has been applied to the site. To clear the filter, see Settings on page 131.

A blue clock icon next to a number in the column Endpoint Seats indicates that these seats will not count against the billable total while the site is a trial. If you hover over the icon, you will see how long the trial has left or if it is expired.

The following controls are available on the sites table.

- **Product list**—By default, the table information displayed is for all products. Select an individual product from the product list to show table information specific to that product and the subscription.
- **Search**—Text entered in the box will narrow the list displayed to only those rows that contain the search text. The search checks the entire table, not just the visible rows. However, any applied filters will limit the search to only those rows displayed by the filter.
- **Add Site**—Click this button to add a new site. See Add a site on page 38 for details.
- **Export**—Click this button to download the list of sites based on the search and filter that are applied to the site lite. The download file is a comma-separated file (.csv).
- **Refresh**—Click this button to refresh the list of sites. Any search and filter you have specified will continue to be applied to the site list after the refresh.
- **Filters**—Click this button to toggle the filter panel open and closed. A green circle with a number on the Filters button indicates the number of filters currently being applied.

Within the filter panel, expand a section to see the filters available. Select one or more filters to apply. You can also hover your mouse to the right of a filter and click exclude if it appears. The one item will be excluded and all other items for that filter type will be included.

Click Reset to clear any selections for a single filter, or click Reset Filters at the bottom of the filter panel to clear all filters.

- **Sort**—Click a column heading to sort the table by that column.
- **Expand Subscriptions** and **Collapse Subscriptions**—Click the left or right triangle icon to the right of the Site column to expand and collapse the product subscription columns. These columns show you the status of each product subscription.
• **Active**—A blue-filled circle with a white letter is an active subscription.

• **Inactive**—A gray-filled circle with a black letter is an inactive subscription.

• **Trial, active**—A white-filled circle with a blue letter is an active trial subscription.

• **Trail, expired**—A white-filled circle with a blue letter and a blue slash through the circle is an expired trial subscription.

• **Expired**—A red-filled circle with a white letter and a white slash is an expired, paid subscription.

• **Suspended**—A black-filled circle with a white letter is a suspended subscription.

• **Site name hyperlink**—Click the name of a site in the table in the Site column to manage that site. Depending on your permissions (administrator access or view-only access), you will be able to view or manage the site. See *Administrators* on page 125 for details on permissions, and see *Manage a site* on page 42 for details on site management.

• **Keycode**—Click the key icon in the Site column to see the keycode assigned to the site. Copy the code if needed.

• **Actions, Legacy console**—In the menu or in the hover text for a subscription, click the box with diagonal arrow icon to open the legacy console for Endpoint Protection or Security Awareness Training.

• **Actions, Configure**—In the menu or in the hover text for a subscription, click the gear icon to manage the subscription.

• **Actions, Start Trial**—In the menu or in the hover text for a subscription, you will see this button if the site has never had that subscription enabled. Click the button to start a trial. The trial is a fully functional, free, 30-day trial.

• **Actions, Upgrade**—In the menu or in the hover text for a subscription, you will see this button if the subscription is a trial and you want to upgrade to a paying subscription.

• **Actions, Buy**—In the menu or in the hover text for a subscription, you will see this button if the subscription has expired and you want to renew your subscription.

• **Actions, Re-enable**—In the menu or in the hover text for a subscription, you will see this button if the subscription has been disabled. Click the button to re-enable the subscription.

• **Rows and paging**—At the bottom of the table are rows and paging controls allowing you to view more or less on a page and move between pages of the table.
Add a site

Use the following instructions to add a site.

1. Click **Sites List** and then click **Add Site**.
2. In the first step of the **Add Site** wizard, configure your site details.

- **Site / Company Name**—Specify a unique name for the site or company.
- **Site Type**—Select the type of site.
  - **External Company**—Select this option if the site is an external company that is purchasing services from you.
  - **Internal Site**—Select this option if the site is within your own company, for example a location or office.
- **Company Size**—If you selected an external company, select the range that represents the size of the company. This field will be hidden if you selected an internal site.
- **Company Industry**—If you selected an external company, select the industry that represents the company. This field will be hidden if you selected an internal site.
- **Billing Cycle**—If you selected an external company, select a billing cycle. This is a billing cycle that you define and use as needed for this site. This is not a billing cycle associated with Webroot. This field will be hidden if you selected an internal site.
- **Billing Date**—If you selected an external company, select a month and date for billing. This is a billing date that you define and use as needed for this site. This is not a billing date associated with Webroot. This field will be hidden if you selected an internal site.
• **Report Distribution List**—Specify a comma-separated list of up to ten email addresses. Each address will receive the generated reports that are configured to be sent to the report distribution list.

• **Include Global Policies**—When enabled, all global policies will be available for this site to use. When a global policy is being used and that global policy changes, each device using the policy will get the change. Once enabled, this option cannot be changed. When disabled, global policies will not be used and only the default policies, without future changes, will be available.

• **Include Global Overrides**—When enabled, global policy overrides will be 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 will use that override and block that file. When this option is disabled, global overrides from other sites will not be applied to this site, and all overrides for this site will have to be manually configured.

• **Comments**—Optionally enter any comments describing the site or company.

• **Tags**—Optionally select a tag to label this site. This is useful if you want to filter sites by tags.

3. Click **Next** to continue.

4. In the second step of the **Add Site** wizard, select the permissions to grant to this site. By default, the account that created the site will be given full administrator permissions, so you will not see that account in the list. All other accounts will be listed and default to **No Access**. If you want other administrators to be able to view or access this site, you must grant those administrator permissions.

   ![Add Site Permissions](image)

   • **Admin**—This permission level allows full access to the site.
   
   • **View Only**—This permission can only view the site. There is no management or control available.
   
   • **No Access**—This permission 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**—Select **Full** if you purchased product or **30 day trial** if you registered for a trial.

• **Site Seats**—Specify the number of seats (endpoints or devices) for the site or company you are configuring. This setting is for your internal reference. It is not used for billing.

• **Default Endpoint Policy**—Select a default policy. The selected policy will be used for all new devices that are installed for this site or company, unless the policy is assigned using inheritance from the group, site, or company for the device. (You can modify the policy the device uses after installation.)
  
  • **Recommended Defaults**—This policy is intended for desktops and laptops. User interface and PUAs (possibly unwanted applications) are disabled. The setting to install DNS Protection is disabled in this policy.
  
  • **Recommended DNS Enabled**—This policy is identical to **Recommended Defaults**, except the setting to install DNS Protection is enabled.
  
  • **Recommended Server Defaults**—This policy is intended for server environments. It focuses on resource utilization and minimal impact on the server.
  
  • **Silent Audit**—This policy is based on the **Recommended Defaults** policy, however, it has the remediation function disabled to minimize production impact. This means it will catch known threats, but not undetermined threats. Use the undetermined threats reports to help you identify items to add to your block and allow overrides. Generally, this policy should only be used for a short duration, for example during initial setup to identify potential production false positives.
  
  • **Unmanaged**—This policy is intended for technical support, troubleshooting, and when no policy management is needed. This policy cannot be managed, but it turns the agent into a local, unmanaged application that can be controlled directly by the end-user. You should not use this policy in production.

• **Data Filter**—If you want to limit the data that is displayed in the console, you can apply data filters. These filters will show or hide data depending on your filter. For example, if you select **2 Months**, all devices that have not connected for two months will be excluded from the data shown for this site. This option 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.

7. Click **Next** to continue.

8. You can optionally configure DNS Protection. If you skip this for now, you can enable it later from the **Settings** tab. See *Enable DNS Protection* on page 22 if you are just getting started or see *DNS Protection* on page 136 for details.

9. Click **Next** to continue.

10. You can optionally configure Security Awareness Training. If you skip this for now, you can enable it later from the **Settings** tab. See *Enable Security Awareness Training* on page 24 if you are just getting started or see *Security Awareness Training* on page 90 for details.

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

Use the following instructions to manage a site.

1. Click Sites List.
2. Click the site name hyperlink of the site you want to manage in the Site column.

Once on the page to manage a site, you can use the site switcher which is the drop-down list at the top of the page. It allows you to easily switch between sites. You will also see the status of the individual sites next to the site name in the drop-down list.

3. Manage the site as needed.

- **Summary**—This tab provides a high level overview of the devices on this site. You can also see a list of the administrators for this site.
  - **View Devices**—This link in the Devices Requiring Attention tile is only visible if you have at least one device that needs attention. Click the link to go to the Entities page. See Entities on page 48 for details.
  - **Edit**—Click this link in the Admins table to go to the Admin Permissions tab where you can modify the administrators for the site. See Administrators on page 125 for details.
  - **Suspend**—Click this button in the Suspend Protection tile 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 and 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.

- **Resume**—Click this button in the Resume Protection tile to resume suspended protected. Infections will begin resolving and, if you are using DNS Protection, the service will be enabled and DNS traffic handled according to policy settings.

- **Deactivate Site**—Click this button in the Deactivate Site tile to deactivate the site keycode. This action will send an uninstall command to all devices using that keycode. This is a permanent action that cannot be reversed. Deactivated sites will not be billed.

- **Delete Site**—Click this button to delete a deactivated site from the console. You will no longer be able to view any data for this site. This is a permanent action that cannot be reversed.

- **Details**—This tab identifies the details of the site. This is the information you provided when you created the site. Modify any of the settings as needed. See *Add a site* on page 38 for details on the site settings.

- **Admin Permissions**—This 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.

- **Endpoint Protection**—This tab shows the subscription status and the default site settings. It also contains download links for the agent installation files.

  - **Site Seats**—Specify the number of seats (endpoints or devices) for the site or company you are configuring. This setting is for your internal reference. It is not used for billing.

- **Default Endpoint Policy**—Select a default policy. The selected policy will be used for all new devices that are installed for this site or company, unless the policy is assigned using inheritance from the group, site, or company for the device. (You can modify the policy the device uses after installation.)

  - **Recommended Defaults**—This policy is intended for desktops and laptops. User interface and PUAs (possibly unwanted applications) are disabled. The setting to install DNS Protection is disabled in this policy.
  
  - **Recommended DNS Enabled**—This policy is identical to Recommended Defaults, except the setting to install DNS Protection is enabled.
  
  - **Recommended Server Defaults**—This policy is intended for server environments. It focuses on resource utilization and minimal impact on the server.

  - **Silent Audit**—This policy is based on the Recommended Defaults policy, however, it has the remediation function disabled to minimize production impact. This means it will catch known threats, but not undetermined threats. Use the undetermined threats reports to help you identify items to add to your block and allow overrides. Generally, this policy should only be used for a short duration, for example during initial setup to identify potential production false positives.

  - **Unmanaged**—This policy is intended for technical support, troubleshooting, and when no policy management is needed. This policy cannot be
managed, but it turns the agent into a local, unmanaged application that can be controlled directly by the end-user. You should not use this policy in production.

- **Data Filter**—If you want to limit the data is that is displayed in the console, you can apply data filters. These filters will show or hide data depending on your filter. For example, if you select 2 Months, all devices that have not connected for two months will be excluded from the data shown for this site. This option 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.

- **Go to Endpoint Protection Console**—Click this link if you have a need to use the legacy Endpoint Protection console.

- **Download Software**—This section contains links to the agent installation files. These links and files are specific to the site and keycode. See Agents on page 140 for details.

- **DNS Protection**—This tab is where you can enable or disable DNS Protection as well as configure DNS Protection configuration for the site. See DNS Protection on page 136 for details.

- **Security Awareness Training**—This tab is where you can enable or disable Security Awareness Training as well as target the users you want to include in training, by identifying a domain that contains the users (email addresses) you want to target for security training. You can use Azure Active Directory integration or a manual process to identify the domain. See Security Awareness Training on page 90 for details.

4. When you have finished managing the site, click **Save** to save any changes. Then click **Back** to go back to the sites list.
Chapter 6 Dashboard

The Dashboard tab gives you 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.

- **Business view**

  At the left of the page are three tiles that provide high level statistics for Endpoint Protection, DNS Protection, and Security Awareness Training. These statistics help you analyze each component at a glance. This is a quick method to identify devices that are infected, devices that have not checked in (if DNS Protection is enabled), and how many training campaigns are active (if Security Awareness Training is enabled). Buttons and hyperlinks within the tiles allow you to move to specific pages of the console or to enable products you are not using.

  At the right of the page, various charts detail activity. You can drill down within chart components by clicking on chart data or machine names.

- **Service Provider view**

  At the top of the page is a Dashboard Summary which shows high level statistics for your sites, seats, and devices. Hover over Sites to see a breakdown of the number. You can also click Need attention or Expiring soon to go to the Sites List page and view details on individual sites.

  At the bottom of the page, various charts detail activity. You can drill down within chart components by clicking on chart data. In some cases, you can drill down a second level within the displayed details.
The following controls are available for the service provider view Dashboard.

- **Add chart**—Click this button to add another chart. Select the chart data, enter a name for the chart, select the type of chart to create, and for some charts, you can configure the time period for the chart. Once the chart is defined, click **Add Chart**.
- **Site Filter**—Click this button to set or clear the filter that determines which sites are reported in the charts.
  - **All**—All sites will be displayed in the charts.
  - **Select sites**—Only the selected sites will be displayed in the charts. Use the **Select all** and **Select none** buttons as needed. Clicking on a site name toggles the site to selected (green checkmark) or not selected (red X).
- **Reset dashboard**—Click this button to reset the chart layout, display, and filter back to the default.
- **Layout**—Click one of the layout buttons in the upper right corner to change the chart display to one to four charts per row. You can also drag and drop charts to sort them in your desired view.
- **Edit**—Within a chart tile, click **Edit** (gear icon) to modify the chart.
- **Delete**—Within a chart tile, click **Remove** (X icon) to remove a chart from the Dashboard.

---

Devices must be running agent version 8.0.4.134 or later to be accurately represented in the Dashboard totals, except for the Threat Detection History and Device Activations charts.

Firewall Status, Rootkit Shield Status, Infrared Status, Silent Mode, and Offline Shield Status are not supported on MacOS.
Migrated keycodes (when a device is moved from one site to another) may cause discrepancies in device counts.
Entities are your devices and groups. Devices are the endpoints. Groups are organizational units. Groups allow you to manage devices together, for example to apply a specific policy to a group of devices. The **Entities** tab is where you view, organize, and manage the devices and groups.

The following tasks are available for entities.

- *View available entities* on page 49
- *Manage an entity* on page 52
View available entities

To view your available entities, expand Manage if needed, and then click Entities.

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

When you select a site or group, you can see the status for each device in the selected site or group. 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.

When you drill down and are looking at devices within a group, the icon to the left of the device name quickly identifies the type of device.

- **Windows icon**—Windows desktop
- **Server icon**—Windows server
- **Apple icon**—MacOS desktop
- **Location icon**—IP address

The icon to the left of the policy name quickly identifies the policy assigned to the device. Hover over an icon to see the full policy name and assignment method.

- **Monitor icon**—The policy is assigned directly to the device.
- **Building icon**—The policy is assigned to the device using a site policy.
- **Connected boxes icon**—The policy is assigned to the device using a group policy.
- **Circle with letter i**—There is more than one policy assigned to the device.

The following controls are available on the entities table.

- **Search**—Text entered in the box will narrow the list displayed to only those rows that contain the search text. The search checks the entire table, not just the visible rows.
• **Agent Commands**—Select a command to run on the device. Commands that apply to Windows only are identified with a Windows icon. Commands that apply to both Windows and MacOS are identified by a combination Windows and Apple icon.
  
  - **Run Scan**—Starts a scan of the selected devices immediately.
  - **Clean Up**—Starts a scan of the device immediately and quarantines any malicious files. After the scan is complete, you can see the results in the **Scan History**.
  - **Uninstall Agent**—Uninstalls the agent from the selected devices. Keep in mind, 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 assigned to the site.
  - **Re-Verify Data**—Verifies the database on the selected devices when the next scan occurs. This option can be used 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 you want to allow.
  - **Run Customer Support Script**—Runs scripts to update devices or remove infections. Webroot will provide any necessary scripts. You will only need to specify a path to the script file.
  - **Run System Optimizer**—Starts the System Optimizer process immediately.
  - **Reset Agent**—This command is a tool used by technical support in specific situations. Do not run this command without assistance from technical support.
  - **Restart Device**—Sends a reboot command to the selected devices. Once the device receives the command, the reboot will happen immediately. There is no notification to the user before the reboot occurs.
  - **View 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**—When one or more devices are selected, you can move the devices to another group. If you are using the service provider view, the groups must be within the same site. You will need to 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**—When one or more devices are selected, you can change the policy assigned to the selected devices.
  - **Filters**—Click this button to toggle the filter panel open and closed. A green circle with a number on the **Filters** button indicates the number of filters currently being applied.

  Within the filter panel, expand a section to see the filters available. Select one or more filters to apply. You can also hover your mouse to the right of a filter and click exclude if it appears. The one item will be excluded and all other items for that filter type will be included.

  Click **Reset** to clear any selections for a single filter, or click **Reset Filters** at the bottom of the filter panel to clear all filters.
  
  - **Create Group**—Click the + icon to create a new group for the selected site. For the service provider view, you must have a site selected to create a new group.
• **Delete Group**—When a user-created group is selected, click the - icon to delete the selected group. You must specify a new group to move any devices that exist in the group you are deleting.

• **Edit Group**—When a user-created group is selected, click the paper and pencil icon to modify the name of the group or the policy assigned to the group.

• **Device name hyperlink**—Click on the name of a device to see details for that device. See *Manage an entity* on page 52 for details.
Manage an entity

Use the following instructions to manage a device.

1. Click Manage and then Entities.
2. If you are using the service provider view, select the site that contains the device you want to manage.
3. Select the group that contains the device you want to manage.
4. Find the device in the list and click the device name hyperlink.
5. Manage the device as needed using the available buttons and the actions on the various tabs.

- **Agent Commands**—Select a command to run on the device. Commands that apply to Windows only are identified with a Windows icon. Commands that apply to both Windows and MacOS are identified by a combination Windows and Apple icon.
  - **Run Scan**—Starts a scan of the selected devices immediately.
  - **Clean Up**—Starts a scan of the device immediately and quarantines any malicious files. After the scan is complete, you can see the results in the Scan History.
  - **Uninstall Agent**—Uninstalls the agent from the selected devices. Keep in mind, 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 assigned to the site.
  - **Re-Verify Data**—Verifies the database on the selected devices when the next scan occurs. This option can be used 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 you want to allow.
• **Run Customer Support Script**—Runs scripts to update devices or remove infections. Webroot will provide any necessary scripts. You will only need to specify a path to the script file.

• **Run System Optimizer**—Starts the System Optimizer process immediately

• **Reset Agent**—This command is a tool used by technical support in specific situations. Do not run this command without assistance from technical support.

• **Restart Device**—Sends a reboot command to the selected devices. Once the device receives the command, the reboot will happen immediately. There is no notification to the user before the reboot occurs.

• **View 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**—Click this button to change the policy the device is using.

• **Summary**—This tab provides high-level information for the device. If the device needs attention or threats have been detected, click the link to go to the **Threats Detected** tab.

• **Threats Detected**—This tab contains two tables that identify infections.
  
  • **File Threat Detections**—This table shows any infected files. Click a file name to see details on the file and the malware detected.
  
  • **Evasion Shield Script Detections**—This table shows any infected scripts. Click a script name to see details of the infected script.
  
  • **Clean Up**—Starts a scan of the device immediately and quarantines any malicious files. After the scan is complete, you can see the results in the **Scan History**.

• **Actions, Add File to Allow List**—Specifies this file as an allowed file.

• **Actions, Restore from Quarantine**—Removes the file from quarantine and restores it to its original location.

• **Web Threat Shield Blocks**—This tab displays the URLs that have been blocked by Web Threat Shield.
  
  • **Actions, Add URL to Allow List**—Specifies this URL as an allowed URL.

• **DNS Protection**—This tab displays the URLs that have been blocked by DNS Protection.
  
  • **Actions, Add URL to Allow List**—Specifies this URL as an allowed URL.

• **Scan History**—This tab displays the history of scans for the device. If a thread was detected during a scan, expand the table row to see details of the threat.
  
  • **File name**—Click the file name to see details on the file and the malware detected.
  
  • **Actions, Add File to Allow List**—Specifies this file as an allowed file.
  
  • **Actions, Restore from Quarantine**—Removes the file from quarantine and restores it to its original location.

6. When you have finished managing the device, click **Back** to go back to the **Entities** tab.
Chapter 8 Policies

A policy configures the behavior of the agent, for example, how often a device is scanned, what scan settings are used, how the scan is performed, and so on. There are several default policies for Endpoint Protection and DNS Protection which can be used as is or they can be modified to fit your specific needs. There is also an Endpoint Protection unmanaged policy which allows end-users to select and manage their own settings.

- **Recommended Defaults**—This policy is intended for desktops and laptops. User interface and PUAs (possibly unwanted applications) are disabled. The setting to install DNS Protection is disabled in this policy.
- **Recommended DNS Enabled**—This policy is identical to **Recommended Defaults**, except the setting to install DNS Protection is enabled.
- **Recommended Server Defaults**—This policy is intended for server environments. It focuses on resource utilization and minimal impact on the server.
- **Silent Audit**—This policy is based on the **Recommended Defaults** policy, however, it has the remediation function disabled to minimize production impact. This means it will catch known threats, but not undetermined threats. Use the undetermined threats reports to help you identify items to add to your block and allow overrides. Generally, this policy should only be used for a short duration, for example during initial setup to identify potential production false positives.
- **Unmanaged**—This policy is intended for technical support, troubleshooting, and when no policy management is needed. This policy cannot be managed, but it turns the agent into a local, unmanaged application that can be controlled directly by the end-user. You should not use this policy in production.

You may want to consider creating and using multiple policies. Think about the following questions and situations when determining policies to create and use.

- Consider groups of people and groups of computer types. What are your logical groups? For example, you may need different policies for executives and non-executives, workstations and servers, different departments, or even different roles within a department.
- Break logical groups down even further. Are there functions that require different policy settings? For example, RDS/Terminal Servers may need different settings than other servers. Another example is that you may want to consider different policy settings for machines you want to allow to be shut down versus those that cannot be shut down.
- Do you need to block particular applications or websites for some of your logical groups?
- Are your policy names going to be easily understood? For example, if you create a default policy for workstations, name that policy Workstations. If you have another policy for workstations and DNS Protection, name that policy Workstations + DNS. When you have multiple policies, it is useful to have a descriptive name that quickly identifies the type of settings that are enabled in the policy. You might also consider including in the policy name any applications or web sites that are blocked.

The following tasks are available for policies.
• View available policies on page 56
• Add a new policy on page 58
• Copy an existing policy on page 59
• Import an existing policy from another site on page 60
• Edit a policy on page 61
• Delete a policy on page 62

In addition to those tasks, see Endpoint Protection policy settings on page 63 and DNS Protection policy settings on page 81 for details on each of the individual policy settings. You should also review Endpoint Protection policy best practices on page 77 for additional guidelines on policy settings.
View available policies

To view your available policies, expand Manage and then click Policies. There are several default policies for Endpoint Protection and DNS Protection which can be used as is or they can be modified to fit your specific needs. There is also an Endpoint Protection unmanaged policy which allows end-users to select and manage their own settings.

- **Recommended Defaults**—This policy is intended for desktops and laptops. User interface and PUAs (possibly unwanted applications) are disabled. The setting to install DNS Protection is disabled in this policy.
- **Recommended DNS Enabled**—This policy is identical to Recommended Defaults, except the setting to install DNS Protection is enabled.
- **Recommended Server Defaults**—This policy is intended for server environments. It focuses on resource utilization and minimal impact on the server.
- **Silent Audit**—This policy is based on the Recommended Defaults policy, however, it has the remediation function disabled to minimize production impact. This means it will catch known threats, but not undetermined threats. Use the undetermined threats reports to help you identify items to add to your block and allow overrides. Generally, this policy should only be used for a short duration, for example during initial setup to identify potential production false positives.
- **Unmanaged**—This policy is intended for technical support, troubleshooting, and when no policy management is needed. This policy cannot be managed, but it turns the agent into a local, unmanaged application that can be controlled directly by the end-user. You should not use this policy in production.

 Default policies are identified with a lock icon. Default policies can be viewed and copied. They cannot be edited or deleted. User-created policies are identified with a person icon. They can be edited, copied, or deleted.

The following controls are available on the policies table on either the Endpoint Protection or DNS Protection tab.

- **Add Policy**—Click this button to create a new policy. See Add a new policy on page 58 for details.
- **Import Policy**—Click this button to import an existing policy from another site or console. See Import an existing policy from another site on page 60 for details.
- **Table hyperlink**—Click on the name of a policy in the table to either view or edit it. Default policies will be viewed. User-created policies will be editable.
- **Actions, View**—Use this menu item to review the policy settings assigned to a default policy.
• **Actions, Copy**—Use this menu item to copy an existing policy. See *Copy an existing policy* on page 59 for details.

• **Actions, Edit**—Use this menu item to edit the policy settings assigned to a policy you created, copied, or imported. See *Edit a policy* on page 61 for details.

• **Actions, Delete**—Use this menu item to delete a user-created policy. See *Delete a policy* on page 62 for details.
Add a new policy

Use the following instructions to create a new policy.

1. Click Manage and then click Policies. Select either the Endpoint Protection or DNS Protection tab.

2. Click Add Policy.

3. Provide a unique Name and a Description. Each field is limited to 50 alphanumeric characters.

4. The policy is created with default settings. If desired, modify any of the policy settings. See Endpoint Protection policy settings on page 63 or DNS Protection policy settings on page 81 for details.

5. After your policy has been defined, click Save.

6. Click Back to go back to the policy list.
Copy an existing policy

Use the following instructions to copy an existing policy. This process will create a new policy based on the policy you are copying.

1. Click Manage and then click Policies. Select either the Endpoint Protection or DNS Protection tab.
2. Use the Actions menu at the right side of the table row and select Copy.
3. Provide a unique Name and a Description. Each field is limited to 50 alphanumeric characters.
4. The policy is created using the settings of the policy you copied. If desired, modify any of the policy settings. See Endpoint Protection policy settings on page 63 or DNS Protection policy settings on page 81 for details.
5. After your policy has been modified, click Save.
6. Click Cancel to go back to the policy list.
Import an existing policy from another site

Use the following instructions to import an existing policy from another site or, if you have access to multiple consoles, from another console.

1. Click Manage and then click Policies. Select either the Endpoint Protection or DNS Protection tab.

2. Click Import Policy.

3. Select the Site that contains the policy you want to import.

4. Select the Policy you want to import. Only the policies on the selected site will be listed.

   You will not be able to import a policy if the name of the policy you are importing already exists. You will need to rename the existing policy to a different, unique name, and then you can import the policy.

5. Click Import Policy.

Once the policy has been imported, you can edit it if desired. See Edit a policy on page 61 for details.
Edit a policy

Use the following instructions to edit a user-created policy.

1. Click Manage and then click Policies. Select either the Endpoint Protection or DNS Protection tab.

2. Click on a policy name hyperlink or use the Actions menu at the right side of a table row and select Edit. You will only see this menu option if it is a policy you created, copied, or imported. Default policies are not editable.

3. Modify the Name, Description, or any of the Policy Settings. See Endpoint Protection policy settings on page 63 or DNS Protection policy settings on page 81 for details.

4. After your policy has been edited, click Save.

5. Click Back to go back to the policy list.
Delete a policy

Use the following instructions to delete a policy 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. Click Manage and then click Policies. Select either the Endpoint Protection or DNS Protection tab.
2. Use the Actions menu at the right side of the table row and select Delete.
3. When prompted, select the Replacement Policy. This is the policy any devices using the policy you are deleting will be assigned to.
4. Click Delete Policy.
Endpoint Protection policy settings

The following pages contain descriptions of all possible policy settings. Review the key questions and situations in Policies on page 54 when determining what settings to use for a policy.

In the Management Console, settings that apply to Windows only are identified with a Windows icon. Settings that apply to both Windows and MacOS are identified by a combination Windows and Apple icon.

At the bottom of the page, you can see Policy Usage which indicates which sites and groups are using the policy.

Basic Configuration

These settings 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 will be available on the desktop.</td>
<td>No shortcut will be visible.</td>
</tr>
<tr>
<td>Show a system tray icon</td>
<td>An Endpoint Protection icon will be available in the system tray.</td>
<td>No icon will be in the system tray.</td>
</tr>
<tr>
<td>Show a splash screen on bootup</td>
<td>An Endpoint Protection screen will display during system boot.</td>
<td>No screen will be displayed during system boot.</td>
</tr>
<tr>
<td>Show SecureAnywhere in the Start Menu</td>
<td>Endpoint Protection will be available in the Start menu.</td>
<td>Endpoint Protection will not be available in the Start menu.</td>
</tr>
<tr>
<td>Show SecureAnywhere in Add/Remove Programs</td>
<td>Endpoint Protection will be listed in Add/Remove Programs or Programs and Features, depending on your Windows version.</td>
<td>Endpoint Protection will not be listed in Add/Remove Programs or Programs and Features.</td>
</tr>
<tr>
<td>Show SecureAnywhere in Windows Action Center</td>
<td>Endpoint Protection will be listed in the Action Center, under Virus &amp; threat protection.</td>
<td>Endpoint Protection will not be listed in the Action Center.</td>
</tr>
<tr>
<td>Hide the SecureAnywhere keycode and subscription information on-screen</td>
<td>The keycode and subscription information will be hidden (except for the first four digits) within the agent.</td>
<td>The keycode and subscription information will be displayed.</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
<td>The agent will automatically download and apply updates without notifying the end-user.</td>
<td>The agent will not automatically download or apply updates.</td>
</tr>
</tbody>
</table>
### Operate background functions using fewer CPU resources
- Non-scan functionality will be run in the background to save CPU resources.
- All Endpoint Protection functionality will be run in the foreground.

### Favor low disk usage over verbose logging
- The Endpoint Protection log will only maintain the last four log items.
- The Endpoint Protection log will maintain all log items.

### Lower resource usage when intensive applications or games are detected
- Endpoint Protection functions will be postponed while the end-user is gaming, watching videos, or using other intensive applications.
- Endpoint Protection functions will not be postponed.

### Allow SecureAnywhere to be shut down manually
- Endpoint Protection can be shut down from the system tray icon.
- The option to shut down Endpoint Protection from the system tray will not be available.

### Force non-critical notifications into the background
- Endpoint Protection will only display critical messages in the system tray. Information messages will be hidden.
- Both critical and information messages will be displayed in the system tray.

### Fade out warning messages automatically
- Endpoint Protection messages in the system tray will automatically disappear after a few seconds.
- The end-user must close Endpoint Protection messages in the system tray

### Store Execution History details
- Data will be stored in the Execution History log.
- No data will be stored in the Execution History log.

### Poll interval
- This option is not an enable/disable setting. It specifies how often the agent will check for updates. The default setting is 24 hours. The recommended setting is 15 minutes.

### Scan Schedule
These settings 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 will be performed using the defined schedule.</td>
<td>Scans will run once a day at the approximate time you installed the software. (Runs at install time and then roughly 24 hours thereafter.)</td>
</tr>
<tr>
<td>Scan Frequency</td>
<td>This option is not an enable/disable setting. It specifies how often the device will be scanned.</td>
<td>This option is not an enable/disable setting. It specifies how often the device will be scanned.</td>
</tr>
<tr>
<td>Time</td>
<td>This option is not an enable/disable setting. It specifies when the device will be scanned.</td>
<td>This option is not an enable/disable setting. It specifies when the device will be scanned.</td>
</tr>
</tbody>
</table>
Scan on bootup if the computer is off at the scheduled time

<table>
<thead>
<tr>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed scans will occur within an hour after bootup.</td>
<td>Missed scans will be skipped.</td>
</tr>
</tbody>
</table>

Hide the scan progress window during scheduled scans

<table>
<thead>
<tr>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scans will run silently in the background.</td>
<td>Scan progress will be displayed in a window.</td>
</tr>
</tbody>
</table>

Only notify me if an infection is found during a scheduled scan

<table>
<thead>
<tr>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>An alert will be shown only if a threat is found.</td>
<td>A status window will display when the scan completes, even if there are no threats found.</td>
</tr>
</tbody>
</table>

Do not perform scheduled scans when on battery power

<table>
<thead>
<tr>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scans will be skipped when using battery power.</td>
<td>Scans will occur using any power source.</td>
</tr>
</tbody>
</table>

Do not perform scheduled scans when a full screen application or game is open

<table>
<thead>
<tr>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scans will be skipped when a full screen application, such as a movie or game, is being used.</td>
<td>Scans will occur when full screen applications are being used.</td>
</tr>
</tbody>
</table>

Randomize the time of scheduled scans up to one hour for distributed scanning

<table>
<thead>
<tr>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>The scan will run within an hour of the scheduled time.</td>
<td>The scan will run at the scheduled time. If you need to schedule scans for an exact time, turn this setting off.</td>
</tr>
</tbody>
</table>

Perform a scheduled Quick Scan instead of a Deep Scan

<table>
<thead>
<tr>
<th>When the policy setting is enabled</th>
<th>When the policy setting is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only a quick scan of memory will be performed.</td>
<td>The scan will check the entire machine.</td>
</tr>
</tbody>
</table>

**Scan Settings**

These settings 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, will be scanned.</td>
<td>The master boot record will not be scanned.</td>
</tr>
<tr>
<td>Enable Enhanced Rootkit Detection</td>
<td>Endpoint Protection will scan for rootkits and other malicious software hidden on disk or in protected system areas. These are created by spyware developers in an attempt to avoid detection and removal.</td>
<td>Endpoint Protection will not scan for rootkits and other malicious software.</td>
</tr>
<tr>
<td>Policy Description</td>
<td>Default Behavior</td>
<td>Alternative Behavior</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable &quot;right-click&quot; scanning in Windows Explorer</td>
<td>A right-click menu will be available in Windows Explorer to immediately scan a file.</td>
<td>The right-click menu will not be available.</td>
</tr>
<tr>
<td>Update the currently scanned folder immediately as scanned</td>
<td>The Endpoint Protection display will update each time a file is scanned.</td>
<td>The Endpoint Protection display will be 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 will be used to run a scan, but the scan might run slower.</td>
<td>More memory will be used to run a scan, so the scan will run faster.</td>
</tr>
<tr>
<td>Favor low CPU usage over fast scanning</td>
<td>Less processor usage will be used to run a scan, but the scan might run slower.</td>
<td>More processor usage will be used to run a scan, so the scan will run faster.</td>
</tr>
<tr>
<td>Show the &quot;Authenticating Files&quot; popup when a new file is scanned on-execution</td>
<td>A small window showing the scan will appear when an end-user executes a file for the first time.</td>
<td>Nothing will appear 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 will be saved to the scan log, resulting in a larger log file.</td>
<td>Only executable file data will be saved to the scan log, resulting in a smaller log file.</td>
</tr>
<tr>
<td>Scan archived files</td>
<td>The file types zip, rar, cab, and 7-zip will be scanned.</td>
<td>These file types will not be scanned.</td>
</tr>
<tr>
<td>Automatically reboot during cleanup without prompting</td>
<td>A reboot will automatically occur after a clean-up to remove malware.</td>
<td>The user will be prompted to reboot after a clean-up to remove malware.</td>
</tr>
<tr>
<td>Never reboot during malware cleanup</td>
<td>The machine will not reboot during a clean-up to remove malware.</td>
<td>A reboot will not be prevented during a clean-up to remove malware. The clean-up 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 will be 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 will be sent to quarantine during scheduled scans.</td>
</tr>
<tr>
<td>Enable Enhanced Support</td>
<td>Logs will be sent to Webroot customer support.</td>
<td>No logs will be sent to Webroot.</td>
</tr>
<tr>
<td>Show Infected Scan Results</td>
<td>Results of the scan will be automatically displayed when the scan is complete.</td>
<td>Nothing will be displayed, even if a threat is found.</td>
</tr>
</tbody>
</table>
Detect Possibly Unwanted Applications (PUAs) as malicious

Possibly unwanted applications (programs that may not be malicious but could be unwanted or create security concerns, such as adware or toolbars) will be blocked from installation or removed, if possible, from the machine.

Given the number of attacks that come through adware, browser add-ons, and other utilities, the recommended setting is on. It may create more false positives, but it will also identify more malicious code.

These applications will not be blocked or removed.

Allow files to be submitted for threat research

Files will be sent to Webroot for threat research.

No files will be sent to Webroot.

### Self Protection

These settings 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 will attempt to protect itself by launching a protective scan.</td>
<td>Endpoint Protection will not attempt to protect itself.</td>
</tr>
</tbody>
</table>
| Self protection Level | This option is not an enable/disable setting. It specifies the self-protection detection level.  
  - Minimum—This level protects the Endpoint Protection settings. Use this level if you have other security products installed.  
  - Medium—This level prevents other programs from disabling Endpoint Protection. Use this level for maximum compatibility with other security products.  
  - Maximum—This level protects the Endpoint Protection processes. This is the recommended level if you have no other security products. | |

### Heuristics

There is a separate section for heuristics for local drive, USB drives, the Internet, the network, CD/DVD drives, and when the machine is offline. The default settings are the recommended settings, and you should not modify any of them. Do not change these settings without assistance from technical support.

### Realtime Shield

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

**Behavior Shield**

These settings 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>You will be prompted for suspicious threats, and known threats will be immediately blocked and quarantined.</td>
<td>Threats will not be alerted or blocked.</td>
</tr>
<tr>
<td>Assess the intent of new programs before allowing them to execute</td>
<td>Endpoint Protection will examine a program's activity before allowing it to run. If it appears safe, Endpoint Protection will allow it to launch and continue to monitor its activity.</td>
<td>Programs will not be examined.</td>
</tr>
<tr>
<td>Enable advanced behavior interpretation to identify complex threats</td>
<td>Endpoint Protection will examine a program to determine its intent. For example, malware may modify a registry entry and then send an email.</td>
<td>Programs will not be examined.</td>
</tr>
<tr>
<td>Track the behavior of untrusted programs for advanced threat removal</td>
<td>Endpoint Protection will examine only those programs that have not been classified as safe or a threat.</td>
<td>Programs will not be examined.</td>
</tr>
<tr>
<td>Automatically perform the recommended action instead of showing warning messages</td>
<td>Endpoint Protection will determine if a threat should be allowed or blocked.</td>
<td>The end-user will be 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 will alert if the program tries to make changes to a device when the device is offline.</td>
<td>Programs will not be alerted if they try to make changes to a device when the device is offline.</td>
</tr>
</tbody>
</table>

**Core System Shield**

These settings control the monitoring of 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>You will be prompted for suspicious threats, and known threats will be immediately blocked and quarantined.</td>
<td>Threats will not be alerted or blocked.</td>
</tr>
<tr>
<td>Assess system modifications before they are allowed to take place</td>
<td>Endpoint Protection will intercept any attempt to make system changes, for example a new service installation.</td>
<td>Endpoint Protection will not intercept any attempt to make system changes.</td>
</tr>
<tr>
<td>Detect and repair broken system components</td>
<td>Endpoint Protection will detect and restore corrupted components or files.</td>
<td>Endpoint Protection will not detect or restore corrupted components or files.</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>Prevent untrusted programs from modifying kernel memory</td>
<td>Programs that are not classified will be blocked from changing kernel memory.</td>
<td>Programs that are not classified will not be blocked from changing kernel memory.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying system processes</td>
<td>Programs that are not classified will be blocked from changing system processes.</td>
<td>Programs that are not classified will not be blocked from changing system processes.</td>
</tr>
<tr>
<td>Verify the integrity of the LSP chain and other system structures</td>
<td>Endpoint Protection will monitor the Layered Service Provider (LSP) chain and other system structures for corruption.</td>
<td>Endpoint Protection will 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 will alert when an attempt is made to modify the hosts file.</td>
<td>Endpoint Protection will not alert when an attempt is made to modify the hosts file.</td>
</tr>
</tbody>
</table>

**Web Threat Shield**

These settings control browsing the Internet and clicking results in search engine.

<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 will monitor Internet browsing and alert on suspicious sites. It will also analyze search engine result links.</td>
<td>There will be no Internet browsing monitoring or search engine analysis.</td>
</tr>
<tr>
<td>Activate browser extension</td>
<td>Users will 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 will not see reputation icons when viewing web search results.</td>
</tr>
<tr>
<td>Block malicious websites</td>
<td>Endpoint Protection will block known malicious websites.</td>
<td>No websites will be blocked.</td>
</tr>
<tr>
<td>Enable real time anti-phishing</td>
<td>Endpoint Protection will alert on zero-day phishing sites, which are sites that have never been seen before and are not classified.</td>
<td>Zero-day phishing sites will not be alerted.</td>
</tr>
<tr>
<td>Show safety ratings when using search engines</td>
<td>Search engine result links will be identified as trusted sites (green checkmark) or suspicious sites (red X).</td>
<td>Search engine results will not be identified.</td>
</tr>
<tr>
<td>Enable web filtering driver</td>
<td>Additional protections against malicious connections, including when browser extensions are disabled, will be used.</td>
<td>Additional protections against malicious connections will not be used.</td>
</tr>
<tr>
<td>Suppress the user's ability to bypass blocked websites</td>
<td>End-users will not be able to bypass the block page presented when a known malicious website is detected.</td>
<td>A user will be able to bypass the block page.</td>
</tr>
<tr>
<td>Suppress the user's ability to request website review</td>
<td>End-users will not be able to submit a website review request from the block page presented when a known malicious website is detected.</td>
<td>A user will be able to request a website review from a block page.</td>
</tr>
</tbody>
</table>

**Identity Shield**

These settings 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 will monitor online transactions. On MacOS, this option controls the Secure Keyboard Entry Mode setting.</td>
<td>Online transactions will not be monitored.</td>
</tr>
<tr>
<td>Look for identity threats online</td>
<td>Endpoint Protection will analyze and alert when it detects malicious content.</td>
<td>Content will not be analyzed.</td>
</tr>
<tr>
<td>Verify websites when visited to determine legitimacy</td>
<td>Endpoint Protection will analyze and alert when a website's IP address has been redirected or has been identified as a threat.</td>
<td>Website IP addresses will not be analyzed.</td>
</tr>
<tr>
<td>Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks</td>
<td>Endpoint Protection will analyze and alert when a website is redirected, such as a man-in-the-middle attack.</td>
<td>Website redirects will not be analyzed.</td>
</tr>
<tr>
<td>Block websites from creating high risk tracking information</td>
<td>Endpoint Protection will block third-party cookies if they originate from a malicious site.</td>
<td>Third-party cookies will not be blocked.</td>
</tr>
<tr>
<td>Prevent programs from accessing protected credentials</td>
<td>Endpoint Protection will block 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 will not be blocked from accessing credentials.</td>
</tr>
<tr>
<td>Warn before blocking untrusted programs from accessing protected data</td>
<td>Endpoint Protection will alert when programs attempt to access data.</td>
<td>Programs accessing data will not be alerted.</td>
</tr>
<tr>
<td>Allow trusted screen capture programs access to protected screen contents</td>
<td>Trusted screen capture programs will function, regardless of the content displayed on screen.</td>
<td>Screen capture programs will not be able to access protected screen contents.</td>
</tr>
</tbody>
</table>
Enable Identity Shield compatibility mode
Certain applications are allowed to run that the Identity Shield might normally block. For example, you may need to enable this option if devices have issues running applications. Even when enabled, the Identity Shield core functionality will still protect the device.
Identity Shield will continue to block all applications that it identifies as malicious.

Enable keylogging protection in non-Latin systems
Endpoint Protection will protect devices using non-Latin languages, such as Japanese and Chinese, from keyloggers.
There will be no protection from keyloggers.

**Firewall**
These settings 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 will monitor outgoing traffic. (Windows firewall will monitor incoming traffic.) The Endpoint Protection firewall will be looking for untrusted processes trying to connect to the Internet and steal personal information. If the firewall detects suspicious traffic, you will be alerted.</td>
<td>Outgoing traffic will not be monitored.</td>
</tr>
<tr>
<td>Firewall level</td>
<td>This option is not an enable/disable setting. It specifies the level of firewall protection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default Allow—This option will allow all processes to connect to the Internet, unless explicitly blocked by the agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Warn unknown and infected—This options will look for any new, untrusted processes connecting to the Internet or if the device is infected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Warn unknown—This option will look for any new, untrusted process connecting to the Internet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default Block—This option will look for any process connecting to the Internet, unless explicitly blocked by the agent.</td>
<td></td>
</tr>
<tr>
<td>Show firewall management warnings</td>
<td>A warning will be displayed when Windows firewall is off.</td>
<td>No warnings will be displayed when Windows firewall is off.</td>
</tr>
<tr>
<td>Show firewall process warnings</td>
<td>Firewall level warnings will be displayed.</td>
<td>No warnings will be displayed and the process is allowed.</td>
</tr>
</tbody>
</table>

**User Interface**
This setting controls if the user interface is available on end-user devices.

When set to **Show**, end-users will be able to see and access the Endpoint Protection user interface on their device. They will be able to perform a scan, but they cannot manage the agent or modify any settings.

When set to **Hide**, end-users will be prompted to contact their administrator if they attempt to access the Endpoint Protection user interface. The **Hide** option also hides the system tray icon on MacOS. It does not hide the system tray icon on Windows.

**System Optimizer**

These settings control Windows cleanup tasks. These are not security tasks, such as removing malware or threats, but instead are general cleanup tasks such as removing unnecessary files and data.

<table>
<thead>
<tr>
<th><strong>Policy Setting</strong></th>
<th><strong>When the policy setting is enabled</strong></th>
<th><strong>When the policy setting is disabled</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage System Optimizer centrally</td>
<td>Displays the System Optimizer controls.</td>
<td>System Optimizer controls will not be displayed.</td>
</tr>
<tr>
<td>Days of week</td>
<td>System Optimizer will run on the selected day of the week.</td>
<td>System Optimizer will not run on the selected day of the week.</td>
</tr>
<tr>
<td>Run at specific time of day - hour</td>
<td>This option is not an enable/disable setting. It 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 is not an enable/disable setting. It 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 will run at bootup if the machine was off at the scheduled run time.</td>
<td>System Optimizer will only run at the scheduled run time.</td>
</tr>
<tr>
<td>Enable Windows Explorer right click secure file erasing</td>
<td>Windows Explorer will have 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 will not be displayed in Windows Explorer.</td>
</tr>
<tr>
<td>Recycle Bin</td>
<td>All files in the Recycle Bin will be deleted when System Optimizer runs.</td>
<td>Nothing will be deleted from the Recycle Bin.</td>
</tr>
<tr>
<td>Recent document history</td>
<td>The history of recently opened files will be deleted from the Start menu. (Only the history is deleted, not the actual files.)</td>
<td>No history will be deleted.</td>
</tr>
<tr>
<td>Start Menu click history</td>
<td>The history of shortcuts to recently opened programs will be deleted from the Start menu. (Only the history is deleted, not the actual shortcuts.)</td>
<td>No history will be deleted.</td>
</tr>
<tr>
<td>Run history</td>
<td>The history of commands will be deleted from the Run dialog. (A reboot may be needed to clear all commands.)</td>
<td>No history will be deleted.</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search history</td>
<td>The computer search history will be deleted. (Only the history is deleted, not any files or programs that were found during a search.)</td>
<td>No history will be deleted.</td>
</tr>
<tr>
<td>Start Menu order history</td>
<td>When a reboot occurs, any changes to the Start menu order will be reverted, and the menu will be in the default alphabetical order.</td>
<td>The Start menu order will not be reverted.</td>
</tr>
<tr>
<td>Clipboard contents</td>
<td>Content on the Clipboard will be cleared.</td>
<td>No content will be cleared.</td>
</tr>
<tr>
<td>Windows Temporary folder</td>
<td>All data in the Windows temporary folder, usually C:\Windows\Temp, will be deleted, unless the file is in use.</td>
<td>No data will be deleted.</td>
</tr>
<tr>
<td>System Temporary folder</td>
<td>All data in the system temporary folder will be deleted, unless the file is in use. The location of this folder varies depending on the Windows version, however, in newer versions of Windows, it is located in C:\Users\username\AppData\Local\Temp.</td>
<td>No data will be deleted.</td>
</tr>
<tr>
<td>Windows Update Temporary folder</td>
<td>All data in the Windows Update temporary folder, usually C:\Windows\SoftwareDistribution\Download, will be deleted, unless the file is in use.</td>
<td>No data will be deleted.</td>
</tr>
<tr>
<td>Windows Registry Streams</td>
<td>The Windows registry change history will be deleted. (Only the history is deleted, not any registry changes or keys.)</td>
<td>No history will be deleted.</td>
</tr>
<tr>
<td>Default logon user history</td>
<td>The registry key that stores the last user logged into the computer will be deleted. Users will 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 will not be deleted.</td>
</tr>
<tr>
<td>Memory dump files</td>
<td>All memory dump files (automatically created for certain Windows errors) will be deleted.</td>
<td>No dump files will be 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, will be deleted, unless the file is in use. The location of this folder varies depending on the Windows version, however, in newer versions of Windows, it is located in C:\Users\username\AppData\Local\Microsoft\Windows\Burn.</td>
<td>No data will be deleted.</td>
</tr>
<tr>
<td>Flash Cookies</td>
<td>Adobe Flash data will be deleted. (These are not actual cookies controlled by browser cookie privacy controls.)</td>
<td>No data will be deleted.</td>
</tr>
<tr>
<td>Address bar history</td>
<td>The history of visited websites will be deleted from Internet Explorer.</td>
<td>No history will be deleted.</td>
</tr>
<tr>
<td>Cookies</td>
<td>All cookies will be deleted. Users will have to re-enter passwords, shopping cart items, and other entries stored in cookies.</td>
<td>No cookies will be deleted.</td>
</tr>
</tbody>
</table>
Temporary Internet Files

All temporary browser files will be deleted.

No files will be deleted.

URL history

The history pane in Internet Explorer will be cleared.

No entries in the history pane will be deleted.

Setup Log

Internet Explorer update log files will be deleted.

No files will be deleted.

Microsoft Download Folder

Files in the Internet Explorer download folder will be deleted.

No files will be deleted.

MediaPlayer Bar History

The list of audio and video files recently opened with the media player in Internet Explorer will be deleted. It does not delete the files, only the list of recently opened files.

The list of recently opened files will not be deleted.

Autocomplete form information

Internet Explorer AutoComplete data will be deleted. Users will have to re-enter data on forms.

No data will be deleted.

Clean index.dat

When a reboot occurs, the index.dat file that stores Windows information such as web address, search queries, and recently opened files, will be deleted.

The index.dat file will not be deleted.

Control the level of security to apply when removing files

This option is not an enable/disable setting. It specifies how you want to handle data that will be deleted.

- **Normal**—Files will be deleted, bypassing the Recycle Bin. A recovery utility may be able to restore these files. This option is the fastest cleanup process.
- **Medium**—Files will be deleted, bypassing the Recycle Bin, and the location where the data was stored will be overwritten three times. A recovery utility would have a harder time restoring these files. This cleanup process will take longer than a normal cleanup process.
- **Maximum**—Files will be deleted, bypassing the Recycle Bin, and the location where the data was stored will be overwritten seven times, including space around the data location. This would be the most difficult files for a recovery utility to restore. This is the slowest cleanup process.

**DNS Protection**

This setting controls if DNS Protection is installed.

<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 will be installed with the Endpoint Protection agent.</td>
<td>DNS Protection will not be installed.</td>
</tr>
</tbody>
</table>

**Evasion Shield**

These settings are for detecting and blocking evasive attacks, including file-based (like malicious scripts), fileless, obfuscated, or encrypted attacks. It requires agents running version 9.0.29.00 or
When the policy setting is enabled | When the policy setting is disabled
---|---
**Script Protection**  
This setting is not an enable/disable setting. It specifies the level of script protection.  
- **Off**—Script protection is disabled and not detecting or blocking script threats.  
- **Detect and Report**—Script threats will be detected and alerted.  
- **Detect and Remediate**—Script threats will be detected, alerted, and quarantined.

**Foreign Code Shield**  
This setting is not an enable/disable setting. It specifies the level of protection against foreign code, which is code that has been injected into a portable executable (PE) file. Foreign Code Shield detects offending PE files, blocks them from executing, and quarantines them.  
- **Off**—Foreign code protection is disabled and not detecting or blocking foreign code threats.  
- **Detect and Remediate**—Foreign code threats will be detected, alerted, and quarantined.  
- **Detect and Report**—Foreign code threats will be detected and alerted.
Endpoint Protection policy best practices

In the majority of situations, the default Endpoint Protection policies should be considered baseline policies that will need to be modified to meet the specific needs of the groups the policy will be assigned to. The following are best practices that you may want to consider when creating policies.

- **Naming conventions**—If you anticipate multiple policies, consider your policy names. They should be easy to understand, describe who the policy is for, and perhaps even what the policy includes. For example, if you create a default policy for workstations, name that policy Workstations. If you have another policy for workstations and DNS Protection, name that policy Workstations + DNS. If the Workstations + DNS policy also blocks a specific application, you might name it Workstations + DNS + No Application_Name, where Application_Name is the name of the software you are blocking.

- **Workstations**—When creating a policy for workstations in your organization, make a copy of the Recommended Defaults policy and then modify each of the following settings.
  - **Basic Configuration**
    - **Poll interval**—Change this setting to 15 Mins. This reduces the length of time that the agent checks for setting changes or commands that are not immediately pushed to the agent.
  - **Scan Settings**
    - **Automatically remove threats found on the learning scan**—You might want to consider turning this option On. Removing threats during the learning scan creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.
    - **Detect Possibly Unwanted Applications (PUAs) as malicious**—Turn this option On. Given the number of attacks that come through adware, browser add-ons, and other utilities, the recommended setting is on. It may create more false positives, but it will also identify more malicious code.
  - **Behavior Shield**
    - **Automatically perform the recommended action instead of showing warning messages**—Turn this option On. Automatically taking the action addresses the issue immediately rather than delaying action until someone manually takes action based on a review of the warning.
  - **Core System Shield**
    - **Prevent any program from modifying the HOSTS file**—Turn this option On. This limits the ability to tamper with this file.
  - **User Interface**
    - **GUI**—Change this option to Show. There are no security issues with exposing the user interface, and having it easily available allows for easier troubleshooting.
  - **Evasion Shield**
    - **Script Protection**—At a minimum, you should set this option to Detect and Report so that threats are identified. Ideally, you should set this option to Detect and RemEDIATE so immediate action is taken when a threat is identified. Keep in mind with report versus remediate, it is easier to address and remove a block than
it is to fix a threat that has gotten through. This is especially important as attack methods evolve quickly.

- **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**

    - **Allow SecureAnywhere to be shut down manually**—Turn this setting **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 and you do not want the actions of one person to impact another person or the server.

    - **Poll interval**—Change this setting to **15 Mins**. This reduces the length of time that the agent checks for setting changes or commands that are not immediately pushed to the agent.

  - **Scan Settings**

    - **Automatically remove threats found on the learning scan**—You might want to consider turning this option **On**. Removing threats during the learning scan creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.

    - **Detect Possibly Unwanted Applications (PUAs) as malicious**—Turn this option **On**. Given the number of attacks that come through adware, browser add-ons, and other utilities, the recommended setting is on. It may create more false positives, but it will also identify more malicious code.

  - **Realtime Shield**

    - **Scan files when written or modified**—Turn this option **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**

    - **Automatically perform the recommended action instead of showing warning messages**—Turn this option **On**. Automatically taking the action addresses the issue immediately rather than delaying action until someone manually takes action based on a review of the warning.

  - **Evasion Shield**

    - **Script Protection**—At a minimum, you should set this option to **Detect and Report** so that threats are identified. Ideally, you should set this option to **Detect and Remediate** so immediate action is taken when a threat is identified. Keep in mind with report versus remediate, it is easier to address and remove a block than it is to fix a threat that has gotten through. This is especially important as attack methods evolve quickly.

- **RDS/Terminal Servers** —When creating a policy for servers that will be directly accessed, make a copy of the **Recommended Server Defaults** policy and then modify each of the following settings.
• **Basic Configuration**
  - **Show a system tray icon**—Turn this setting **Off**. Disabling this option provides more protection from Endpoint Protection being accessed from the system tray. This is especially important if multiple people have access to the server and you do not want the actions of one person to impact another person or the server.
  - **Show SecureAnywhere in the Start Menu**—Turn this setting **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 and you do not want the actions of one person to impact another person or the server.
  - **Show SecureAnywhere in Add/Remove Programs**—Turn this setting **Off**. Disabling this option provides more protection from Endpoint Protection being uninstalled. This is especially important if multiple people have access to the server and you do not want the actions of one person to impact another person or the server.
  - **Allow SecureAnywhere to be shut down manually**—Turn this setting **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 and you do not want the actions of one person to impact another person or the server.
  - **Poll interval**—Change this setting to **15 Mins**. This reduces the length of time that the agent checks for setting changes or commands that are not immediately pushed to the agent.

• **Scan Settings**
  - **Scan archived files**—Turn this setting **On**. This provides more thorough protection of the server.
  - **Automatically remove threats found on the learning scan**—You might want to consider turning this option **On**. Removing threats during the learning scan creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.
  - **Detect Possibly Unwanted Applications (PUAs) as malicious**—Turn this option **On**. Given the number of attacks that come through adware, browser addons, and other utilities, the recommended setting is on. It may create more false positives, but it will also identify more malicious code.

• **Realtime Shield**
  - **Scan files when written or modified**—Turn this option **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**
  - **Automatically perform the recommended action instead of showing warning messages**—Turn this option **On**. Automatically taking the action addresses the issue immediately rather than delaying action until someone manually takes action based on a review of the warning.
• Evasion Shield
  • Script Protection—At a minimum, you should set this option to Detect and Report so that threats are identified. Ideally, you should set this option to Detect and Remediate so immediate action is taken when a threat is identified. Keep in mind with report versus remediate, it is easier to address and remove a block than it is to fix a threat that has gotten through. This is especially important as attack methods evolve quickly.
DNS Protection policy settings

The following pages contain descriptions of all possible DNS Protection policy settings.

Privacy Settings

These settings control user privacy settings and the information that is logged.

- **Hide User Information**—If selected, user information is replaced with the word Hidden in the log. If not selected, user information will be included in the log.
- **Local Echo**—If selected, DNS requests will be sent to the local DNS server for visibility, but the Webroot DNS server will still resolve the request. If not selected, DNS requests will not be sent to the local DNS server for visibility.
- **Fail Open**—If selected, the local DNS server will resolve DNS requests if the Webroot DNS server is unavailable. If not selected, the local resolver will resolve requests.

Recommended

Security Risk, Human Resource Protections, and Questionable / Legal are the recommended settings for all DNS Protection policies. By default, all of these types of sites are selected for filtering in the default DNS High Protection policy. The DNS Medium Protection policy selects the types of sites in Security Risk and Human Resource Protections.

Security Risk

These sites may pose security risks when visited.

- **Keyloggers and Monitoring**—Sites that include downloads and discussions for software agents that track users' keystrokes or monitor their web surfing habits
- **Malware Sites**—Sites that are known to contain malicious content including executables, drive-by infection sites, malicious scripts, viruses, or Trojans
- **Phishing and Other Frauds**—Pharming (redirects to a fake site) and other sites that pose as a reputable site, usually to harvest information from a user
- **Proxy Avoidance and Anonymizers**—Sites that use proxy servers or other methods to bypass URL filtering or monitoring
- **Spyware and Adware**—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 setting also includes sites that contain unsolicited advertising pop-ups and programs that may be installed on users' computers.
- **Bot Nets**—URLs or IP addresses that are 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**—URLs contained in spam messages

Human Resource Protections

These sites are relevant to human resources departments.
• **Abused Drugs**—Sites for illegal, illicit, or abused drugs, including legal highs, glue sniffing, misuse of prescription drugs, or abuse of other legal substances

• **Adult and Pornography**—Sites with sexually explicit material for the purpose of arousing sexual interest, including sites with adult products such as sex toys and videos. This settings also includes online groups sites which 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 focused on establishing personal relationships

• **Sex Education**—Sites with 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 and Intimate Apparel**—Sites with swimsuits, intimate apparel, or other types of suggestive clothing

• **Gross**—Sites with blood or bodily functions, such as vomit

• **Nudity**—Sites with 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 or nude paintings or photo galleries of artistic nature

• **Alcohol and Tobacco**—Site that provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.

**Questionable/Legal**

These sites have questionable or legal risk.

• **Cult and Occult**—Sites that provide methods, means of instruction, or other resources that attempt to affect or influence real events through the use of astrology (including horoscopes), spells, curses, magic powers, or supernatural beings

• **Gambling**—Sites for gambling or lottery sites, including 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 for marijuana use, cultivation, history, culture, or legal issues

• **Hacking**—Sites for 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 that 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 that pay users in the form of cash or prizes for clicking on reading specific links in emails or web pages

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

• **Hate and Racism**—Sites that support hate crime or racist content or language
• **Violence**—Sites that advocate violence, violent depictions, or methods, including game/comic violence and suicide
• **Cheating**—Sites that support cheating and contain materials such as free essays, exam copies, and plagiarism
• **Illegal**—Sites for criminal activity including how not to get caught and copyright and intellectual property violations
• **Abortion**—Sites that are either pro-live or pro-choice

**Optional**

These settings are optional. By default, they are not selected for filtering.

**Social Media / Internet Communication**

These sites are related to social media and communication over the Internet.

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

**Shopping**

These sites are shopping related.

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

**Entertainment**
These are entertainment sites.

- **Entertainment and Arts**—Sites that 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**—Sites for sales, delivery, or streaming of audio or video content, including sites that provide downloads for such viewers

- **Peer to Peer**—Site that provide peer-to-peer clients and access, including torrents and music download programs

- **Games**—Sites 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 for music sales, distribution, streaming, information on musical groups and performances, lyrics, and the music business

**Lifestyle**

These sites are lifestyle related.

- **Travel**—Sites 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 for home issues and products, such as maintenance, home safety, decor, cooking, gardening, home electronics, and design

- **Religion**—Sites for conventional or unconventional religious or quasi-religious subjects, including churches, synagogues, or other houses of worship

- **Hunting and Fishing**—Sites for sport hunting, gun clubs, and fishing

- **Society**—Sites for 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 for team or conference websites, international, national, college, professional scores and schedules, sports-related online magazines or newsletters

- **Fashion and Beauty**—Sites for fashion or glamor, magazines, beauty, clothes, cosmetics, and style

- **Recreation and Hobbies**—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**

These sites are for business, government, or other service

- **Real Estate**—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**—Sites for computer and Internet security and security discussion groups
- **Financial Services**—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**—Sites for business firms, corporate websites, business information, economics, marketing, management, and entrepreneurship
- **Computer and Internet Info**—Sites for general computer and Internet information, including technical information. Also includes software as a service (SaaS) sites and other sites that deliver Internet services
- **Military**—Sites for the military branches, armed services, and military history
- **Individual Stock Advice and Tools**—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**—Sites for distance education and trade schools, online courses, vocational training, software training, and skills training
- **Personal Storage**—Sites that provide online storage and posting of files, music, pictures, and other data
- **Government**—Sites for 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**—Sites for the delivery of content and data for third parties, including ads, media, files, images, and videos
- **Motor Vehicles**—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**—Sites that offer free or paid hosting services for web pages and information concerning their development, publication, and promotion of web sites

**General Information**

These sites are general information sites.

- **Legal**—Legal sites and law firms and sites for discussions and analysis of legal issues
- **Local Information**—Sites for city guides and tourist information, including restaurants, area/regional information, and local points of interest
- **Job Search**—Sites that offer assistance in finding employment, tools for locating prospective employers, employers looking for employees, and career search and career placement from schools
- **Translation**—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**—Sites for personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogs, genealogy, and scientific information
• **Philosophy and Political Advocacy**—Sites for politics, philosophy, discussions, promotion of a particular viewpoint or stance in order to further a cause

• **Educational Institutions**—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**—Sites designed specifically for children and teenagers

• **News and Media**—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**—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**—Sites that provide photo and image searches, online photo albums, digital photo exchange, and image hosting

**Uncategorized Domains**

• **Uncategorized Domains**—Sites that Webroot has not categorized

**Additional Filtering**

• **Enable Google SafeSearch**—If selected, DNS requests for www.google.com are resolved to forcesafesearch.google.com to filter explicit content from the search results. If not selected, DNS requests for www.google.com will resolve to www.google.com.
Chapter 9 Overrides

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

To access overrides, expand Manage and then click Overrides.

- **File Allow List** and **File Block List**—These two tabs list the files and folders that have been allowed and blocked. Click on a table row to see details for that table row entry.

  If you are using the service provider view, file overrides will be applied to all sites that have **Include Global Overrides** enabled in the site details. If the global overrides option is disabled for a site, then you will need to use the legacy Endpoint Protection console to configure overrides per site.

- **Add**—Click this button to specify a file or folder that should be allowed or blocked. After you have configured the settings, click **Create**.
  - **Name/Description**—Specify a name or description to identify the entry.
  - **Override Type**—You can allow a file or folder or an MD5. You can only block an MD5. If you select an MD5, specify its 32-character hash. If you select a file or folder, complete the following fields.

    File and folder overrides are only supported on Webroot agent version 9.0.1 or later.

  - **File Mask**—Specify a specific file name or a wildcard. If you leave this field blank, all files in the specified folder will be allowed.
  - **Path/Folder Mask**—Specify an absolute file path or a file path using a system variable (like %SystemDrive%). Enter % to see a list of supported variables.
  - **Include Sub-Folders**—Enable this option if you want to include subfolders of the specified path.
  - **Detect if Malicious**—Enable this option to detect and remediate the file according to the assigned policy. Monitoring and journaling will be disabled when this option is enabled. If this option is disabled, the detect and remediate policy settings will not apply to the file.
  - **Delete**—Click this button to delete an entry you no longer want to allow or block.
  - **Import**—Click this button to import the defined overrides from another site. You have three additional options when importing overrides from another site.
    - **Remove Redundant Overrides**—When enabled, if the override exists on the site you are importing from and the site you are importing to, the redundant entry will be removed from the override import list, keeping the override you already have in
place. When disabled, redundant entries will not be removed.

- **Overwrite Existing Overrides**—When enabled, redundant entries that are not removed will overwrite existing entries. When disabled, redundant entries that are not removed will exist after the import.

- **Include Policy Based Overrides**—When enabled, if there are overrides assigned to the policy used by the site you are importing from, those overrides will be imported. When disabled, the policy overrides from the site will not be imported.

- **Refresh**—Click this button to update the table.

- **Edit**—Click on a table row to see and edit details for that table row entry. You can modify any of the settings for a folder/file. For an MD5, you can modify the name you gave to the entry, and you can move it back and forth between the File Allow List (good determination) and File Block List (bad determination).

- **Web Overrides**—This tab lists the URLs that have been allowed or blocked.

---

If you are not using DNS Protection, these web overrides are related to the **Web Threat Shield** policy settings. See *Endpoint Protection policy settings* on page 63 for details.

If you are using DNS Protection protection, these web overrides are your DNS Protection overrides and you will need to manage your web overrides for the **Web Threat Shield** policy settings through the legacy Endpoint Protection console.

---

- **Add**—Click this button to specify a URL that should be allowed or blocked. After you have configured the settings, click **Create**.
  
  - **Domain(s)**—Enter a comma-separated list of domains that you want to create a rule for. The protocol (for example, https or www) is not needed. For example, you can specify domain.com. Wildcards are supported. For example, you can specify *.domain.com.
  
  - **Scope**—If you are using the service provider view, select if the rule should apply to all sites that are configured to include global settings or just the selected site.

---

Specific site rules take precedence over global rules.

---

- **Policy**—If you want to associate this rule with a policy, enable this option and specify the policy. If you do not specify a policy, the override will be associated with the site.

- **Block/Allow**—Select if the domain should be blocked or allowed.

- **Block Malicious URLs**—Select if you want malicious URLs, for example, domains with known malware, to be blocked regardless of a rule.

- **Refresh**—Click this button to update the table.

- **Filters**—Expand or collapse the available filters using the up and down arrow at the right side of the page. You can narrow the list displayed to only those rows that contain the
Domain search text. Or you can narrow the results by selecting the Associated Policy or Block/Allow.

- **Sort**—Click a column heading to sort the table by that column.
- **Actions, Edit Override**—Use this menu item to edit the entry.
- **Actions, Delete Override**—Use this menu item to delete the entry.

Changes in overrides will be applied to devices at their next polling interval, which is configured in the Endpoint Protection policy the device is using. The default polling interval is 24 hours. If you want to manually push changes out before that interval, use the **Re-Verify Data** agent command. See View available entities on page 49 for details.
Chapter 10 Security Awareness Training

Security Awareness Training is managed through campaigns. A campaign is a single phishing simulation or training course sent to a group of users. Campaigns also provide reporting and management of your security awareness program. Keep in mind the following when designing and running campaigns.

- Everyone should participate. Make sure to include new hires and existing employees, across every department. Include all levels of employees. Service providers should train your 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 courses 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.

The following campaign and campaign-related tasks are available.

- Enable Security Awareness Training on page 91
- Target the users for training on page 92
- Manage Security Awareness Training users and distribution lists on page 94
- View available campaigns on page 97
- View available training courses on page 99
- Create a new campaign on page 100
- View a campaign summary report on page 105

Make sure your email server will not block the phishing simulation and training emails sent to your users. See Requirements on page 7 for details.
Enable Security Awareness Training

If you have not already enabled Security Awareness Training, you will need to do that first. If you have already enabled it, continue with Target the users for training on page 92.

1. If you are using the business view, go to the Security Awareness Training tab. If you are using the service provider view, go to Sites list, click the site name hyperlink, and then within the site details, click the Security Awareness Training tab.

2. Enable Security Awareness Training.

3. Select your keycode type.
   - **Full**—This option is the full product with no limitations. You will be billed for this service.
   - **Trial**—This option is the full product, however, it is limited to a free, 30-day trial.

4. Click Save.
Target the 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 for security training. If you are using the service provider view, you need to identify the domain for each site.

1. If you are using the business view, go to the Security Awareness Training tab. If you are using the service provider view, go to Sites list, click the site name hyperlink, and then within the site details, click the Security Awareness Training tab.

2. Select the type of domain identification you want to use and complete the associated process.
   - **Active Directory Integration**—This method synchronizes with Azure Active Directory to identify the domain. It will also synchronize a list of users in the domain that you can target for security training.
     a. Click Configure Azure AD Integration.
     b. Copy the Secret Token that is displayed and use it to configure your Azure Active Directory tenant following the on-screen instructions.
    
    You can see the synchronization status and the last update from Azure Active Directory. If needed, you can also click Disable to stop synchronizing from Azure.

   - **Domain Verification**—This method identifies the domain through a verification email and then users are added.
     a. Enter an email address in Add New Domain.
        - **Domain Member**—If the email address you enter is a member of the domain, campaigns can be created and run, but the breach report will not be accessible.
        - **Domain Admin**—If the email address you enter is a system level email on the domain (admin, administrator, info, postmaster, root, system, or webmaster), campaigns can be created and run, and the breach report will be accessible.

    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.

    b. Click Send Verification Request to send a verification email to the specified email address.
    c. Once you get the email, click the verification link in the message to confirm access to that domain.
    d. After access to the domain is confirmed, go to the main Security Awareness Training tab and click the Users tab.
    e. Select a site.
    f. Click Add Users to Site.
    g. Select how you want to add the users.
       - **Enter Users Manually**—Select this option and manually specify the name and email for each user you want to target for training.
• **Upload Users from File**—Select this option to import the users you want to target for training. The file should contain no more than 15,000 records.
  • **CSV**—You can use 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**—You can use an .ldif file exported from LDAP/Active Directory. The following fields will be used to add users for training.
    • `givenname`—This entry is required and will be populated as the user's first name.
    • `sn`—This entry is required and will be populated as the user's last name.
    • `mail`—This entry is required and will be populated as the user's email address.
    • `objectGUID`—This entry is optional and will be populated as the user's unique ID.
    • `ou`—These entries (organizational units) are optional and will be populated as tags.

• **Set up Active Directory integration**—Select this option to synchronize using Azure Active Directory.
  a. Click **Configure Now**.
  b. Copy the **Secret Token** that is displayed and use it to configure your Azure Active Directory tenant following the on-screen instructions.

---

If you want to send phishing simulations or training courses to a subset of your users for targeted training, you can create Security Awareness Training distribution lists to organize your users into groups. See *Manage Security Awareness Training users and distribution lists* on page 94 for details.
Manage Security Awareness Training users and distribution lists

You can manage the users you have targeted for phishing simulations and training courses. If desired, you can also create and manage Security Awareness Training distribution lists to organize your users into groups for targeted training.

From the Security Awareness Training tab, select the Users tab. For the service provider view, you can manage users at the site level or at the Security Awareness Training distribution list level. For the business view, you can manage users at the distribution list level.

- **Manage users at the site level**—For the service provider view, you can add and delete users at the site level by selecting a site name.
  - **Add**—To add new users to the site, click **Add Users to Site** and select how you want to add the users.
  - **Enter Users Manually**—Select this option and manually specify the name and email for each user you want to target for training.
  - **Upload Users from File**—Select this option to import the users you want to target for training. The file should contain no more than 15,000 records.
    - **CSV**—You can use 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**—You can use an .ldif file exported from LDAP/Active Directory. The following fields will be used to add users for training.
      - **givenname**—This entry is required and will be populated as the user's first name.
      - **sn**—This entry is required and will be populated as the user’s last name.
      - **mail**—This entry is required and will be populated as the user's email address.
      - **objectGUID**—This entry is optional and will be populated as the user's unique ID.
      - **ou**—These entries (organizational units) are optional and will be populated as tags.
  - **Set up Active Directory integration**—Select this option to synchronize using Azure Active Directory.
    a. Click **Configure Now**.
    b. Copy the **Secret Token** that is displayed and use it to configure your Azure Active Directory tenant following the on-screen instructions.
  - **Delete**—If you want to delete users from the site, mark the checkbox next to the users’ name and click **Delete Selected Users**.

- **Manage Security Awareness Training distribution lists**—You can add, edit, and delete users at the Security Awareness Training distribution level by selecting a site name or a Security Awareness Training distribution list name.
  - **Add**—To add a new Security Awareness Training distribution list when using the service provider view, select a site name and then click **Create Distribution List** (the plus icon).
If you are using the business view, click **Create Distribution List** (the plus icon).

<table>
<thead>
<tr>
<th>CREATE DISTRIBUTION LIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution List Name</td>
</tr>
<tr>
<td>Company name - All Users</td>
</tr>
<tr>
<td>Search for...</td>
</tr>
<tr>
<td>Add All</td>
</tr>
<tr>
<td>Name1 <a href="mailto:name1@domain.com">name1@domain.com</a></td>
</tr>
<tr>
<td>Name2 <a href="mailto:name2@domain.com">name2@domain.com</a></td>
</tr>
</tbody>
</table>

- **Distribution List Name**—Specify a name for the Security Awareness Training distribution list.
- **Company name**—The table under the company name lists the available users. Click a user in this list to move it to the **Distribution List Members** list.
- **Search for**—Using search, you can narrow either list to only those users that meet the search criteria. Click the x to clear the search criteria.
- **Add All**—Click this link to add all of the users currently displayed 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.
- **Distribution List Members**—This table lists all of the users that will be included in the Security Awareness Training distribution list. Even if you are using search to narrow the displayed list, all of the users in the list will be included in the Security Awareness Training distribution list.
Awareness Training distribution list. Click a user in this list to remove an item from the Distribution List Members list and move it back to the company name list.

- **Remove All**—Click this link 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.

- **Edit**—To edit an existing Security Awareness Training distribution list, select a Security Awareness Training distribution list name and then click **Edit Distribution List** (the pencil icon or the button).

- **Delete**—To delete an existing Security Awareness Training distribution list, select a Security Awareness Training distribution list name and then click **Delete Distribution List** (the dash inside the circle icon).
View available campaigns

To view the available campaigns, click the Security Awareness Training tab. You will see 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.

- **Search**—Text entered in the box will narrow the list displayed to only those rows that contain the search text. The search checks the entire table, not just the visible rows.

- **New Campaign**—Click this button to create a new campaign. See Create a new campaign on page 100 for details.

- **Filters**—Click this button to toggle the filter panel open and closed. Within the filter panel, select one or more filters to apply.

- **Sort**—Click a column heading to sort the table by that column.

- **Campaign name hyperlink**—Click the name of an active or completed campaign to view the summary report for the campaign. See View a campaign summary report on page 105 for details.

- **Site name hyperlink**—Click the name of the site to go to the legacy Security Awareness Training console. This is an older console that will be phased out in the future.

- **Actions, End Campaign**—This menu item immediately ends a campaign. Users who attempt to access a campaign after it has ended will see an error message.

- **Actions, Send Reminder Now**—This menu item immediately sends an email reminder to users who have not completed the training course.

- **Actions, Edit Campaign**—This menu item allows you to edit a campaign. See the campaign settings in Create a new campaign on page 100. This option is only available for draft campaigns.

- **Actions, Archive Campaign**—This menu item keeps a campaign that is completed and no longer active. You can review archived campaigns.
• **Actions, Delete Campaign**—This menu item deletes a draft campaign. You cannot review deleted campaigns.

• **Actions, Copy Campaign**—This menu item create a copy of a campaign. See the campaign settings in *Create a new campaign* on page 100.

• **Rows and paging**—At the bottom of the table are rows and paging controls allowing you to view more or less on a page and move between pages of the table.
View 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 will 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 will narrow 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.
Create a new campaign

Use the following instructions to create a new campaign.

1. Go to the Security Awareness Training tab.
2. Click New Campaign.
3. Build the campaign. The campaign settings are under the first heading.

- **Campaign Name**—Specify a descriptive name for the campaign. This is for your use only, not something the users will see.

- **Campaign Type**—Select the type of campaign to create.
  
  - **Phishing**—This is an email-based phishing simulation. It will test and report on how many users clicked the phishing link.
  
  - **Training**—This is a training course. It will educate and report on how many users completed the training.

- **Select Email Template**—Scroll through the thumbnails that show the phishing 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**—Specify the name of the person, alias, group, or organization you want the email to be from.
- **Sender Address**—Specify the address that you want the email to be from.
- **Email Subject**—Specify the subject line of the email.
- **Email Body**—Specify the body of the email.

After you have customized the email template, you can click **Save As New** to create a new template based on your customizations or click **Apply Edits** to modify the template you are customizing.

- **Landing Page URL**—Select a domain. This is the URL the user will be sent to from the phishing email. You can optionally customize the URL with a subdomain to make it more relevant to the phishing email or your users.

- **Landing Page**—Select what you want to display when the **Landing Page URL** is clicked.
  - **Infographic**—This option will display 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**—Select an infographic that will be displayed. Click **Customize Template** if you want to modify the body of the infographic page.
  - **Broken Link**—This option will display 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**—Select the type of broken link error that will be displayed.
  - **Lure Page**—This option 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**—Select the lure page that will be displayed. Click **Customize Template** if you want to modify the body of the lure page.
    - **Destination Upon Posting Data**—Select an infographic that will be displayed if the user enters information on the lure page. Click **Customize Template** if you want to modify the body of the infographic page.
  - **Select Course**—If you selected a training course, select the course. You can filter the courses displayed by entering search text.

4. Click the second heading to expand it. This section allows you to select the sites to include in the campaign.
• **Select Sites**—This 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.

• **Search for**—Using search, you can narrow either list to only those sites that meet the search criteria. Click the x to clear the search criteria.

• **Show Distribution Lists**—If you have Security Awareness Training distribution lists created, you can enable this option to view the Security Awareness Training distribution lists associated with each site. A selected Security Awareness Training distribution list will only send the campaign to those users in the Security Awareness Training distribution list, rather than all users in a site.

• **Add All**—Click this link to add all of the sites and Security Awareness Training 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 will be added.

• **Sites Selected**—This table lists all of the sites and Security Awareness Training distribution lists that will be included in the campaign. Even if you are using search to narrow the displayed list, all of the sites in the list will be included in the campaign. Click a site in this list to remove an item from the **Sites Selected** list and move it back to the **Select Sites** list.

• **Remove All**—Click this link to remove all items from the **Sites Selected** list and move them back to the **Select Sites** list.

5. Select the third section to expand it. This section allows you to schedule the campaign.
- **Auto-Enrollment**—Select this option to automatically add new users to this campaign when they are added to the site or distribution list selected for the campaign. As long as the campaign is still active, the new users will receive the campaign.
- **Launch Date**—If you are automatically enrolling users, select the date when you want the campaign to start.
- **Duration**—This field is different depending on if you are automatically enrolling users.
  - **Automatic enrollment**—If you are automatically enrolling users, select the length of time enrolled user will remain in the campaign. The campaign will end at 11:59pm on the last day. If you select **Indefinitely**, the user will remain enrolled in the campaign until the campaign is manually ended.
  - **No automatic enrollment**—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 will never expire, unless you manually end the campaign. If you set an end date, the campaign will end at 11:59pm on the last day.

Users who attempt to access a campaign after it has ended will see a message that the campaign is no longer active.

- **Delivery Time**—Select the time when you want the campaign emails to be sent.
  - **Deliver emails at time of launch**—This option sends all of the emails as soon as the campaign starts.
  - **Deliver emails at custom time**—This option sends all of the emails at the specified time.
  - **Spread email delivery out over period of days**—This option spreads the delivery of the emails over the specified number of days.

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.
• **After campaign ends, send Campaign Summary Report automatically**—Select this option 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 will contain 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. See **View a campaign summary report** on page 105 for details.

6. Click the fourth 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 addresses and click **Send Preview**. Repeat for multiple email addresses. Each email address will see a preview of what the campaign will look like and how it will function.

7. Click one of the following buttons.

   - **Cancel**—This button will exit the campaign creation. You will lose the campaign settings you have configured.
   - **Save & Close**—This button will exit the campaign and save the campaign settings you have configured. The campaign will remain in draft status and will not be started, even when the specified launch date is reached.
   - **Launch Campaign**—This button will exit the campaign, save the campaign settings you have configured, and start the campaign when the specified launch date is reached. If the launch date is immediate, the campaign will be started immediately.

---

Make sure your email server will not block the phishing simulation and training emails sent to your users. See **Requirements** on page 7 for details.
View a campaign summary report

To access a campaign summary report, go to the Security Awareness Training tab and click the campaign name hyperlink to view the summary report. The report is divided into sections.

- **Summary**—The top of the report contains high-level information including the launch, duration, and enrolled users.
- **Email used**—The email used for the campaign is displayed below the summary.
- **Type of landing page**—If you are viewing the summary of a phishing campaign, the type of landing page (infographic, broken link, or lure page) is displayed after the email.
- **Training course**—If you are viewing the summary of a training campaign, the training course is displayed after the email.
- **Results**—The high-level results of the campaign are displayed in a table for easy viewing. Below the table are details for each targeted user.

For both phishing and training campaigns, click **Export PDF** or **Export CSV** to create and download the summary report in that file format.
Chapter 11 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. See Report types on page 116 for details on the different reports available.

The following tasks are available for reports.

- Run an on-demand report on page 107
- View available scheduled reports on page 110
- Add a scheduled report on page 111
- View available scheduled report templates on page 113
- Add a scheduled report template on page 114
- View scheduled report history on page 115

In addition to the on-demand and scheduled reports, if you are using the service provider view, you will find information on the Universal Reporter under the API Reporting tab. Review the videos and links to the Knowledge Base and Community Page to learn about this tool.
Run an on-demand report

Use the following instructions to create and run an on-demand report.

You can also run an existing, scheduled report on-demand. See View available scheduled reports on page 110 for details.

1. Click Reports and select the On-Demand tab.
2. Specify the Site you want the report to be run against. You can also run reports against all sites.
4. For some report types, you can also specify a time Period for the report data.
5. Click Submit to generate the report.
6. The report will be displayed on screen. Depending on the report type, you may have one or more of the following tasks and controls available for the report.

- **Chart data**—For report results returned in chart format, click on chart data, for example a bar in a bar chart, to see details for that subset of data. You can continue to drill-down through the chart data. For example, in the Endpoint Status report, if you click on the bar for infected devices, you will see a list of the devices that are infected. You can then click on a device in the list and see details for that device.
- **View details, table row**—For report results returned in table format, click on a table row to see details for that table row entry.
• **View details, file name**—For threats displayed by file name, click on a file name to see details on the threat.

• **Export to CSV**—For some reports, you can to click this button to download the report data to a comma-separated file (.csv).

• **Actions, Add this File to Allow list**—For threats, you can select this action to specify the file as an allowed file.

• **Actions, Restore this File from Quarantine**—For threats, you can select this action to remove the file from quarantine and restore it to its original location.

• **Actions, Initiate Cleanup on this Device**—For devices, you can select this action to start a scan immediately and quarantine any malicious files.

• **Actions, Create Override**—For URLs, you can create an override for the URL.
  
  • **Domain(s)**—Enter a comma-separated list of domains that you want to create a rule for. The protocol (for example, https or www) is not needed. For example, you can specify domain.com. Wildcards are supported. For example, you can specify *.domain.com.

  • **Scope**—If you are using the service provider view, select if the rule should apply to all sites that are configured to include global settings or just the selected site. Specific site rules take precedence over global rules.

  • **Policy**—If you want to associate this rule with a policy, enable this option and specify the policy. If you do not specify a policy, the override will be associated with the site.

  • **Block/Allow**—Select if the domain should be blocked or allowed.

  • **Block Malicious URLs**—Select if you want malicious URLs, for example, domains with known malware, to be blocked regardless of a rule.
Scheduled reports

Scheduled reports allow you to get in-depth information on your sites at recurring intervals. You have the following tasks available when working with scheduled reports:

- View available scheduled reports on page 110
- Add a scheduled report on page 111
- View available scheduled report templates on page 113
- Add a scheduled report template on page 114
- View scheduled report history on page 115

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.
View available scheduled reports

To view your available scheduled reports, click Reports and select the Scheduled Reports tab.

The following controls are available on the reports table.

- **Add**—Click this button to add a new scheduled report. See Add a scheduled report on page 111 for details.
- **Copy**—Click this button to make a copy of an existing scheduled report. Provide a unique name for the new report and click Copy. You can then select the table row for the new report and make any desired modifications.
- **Delete**—Click this button to delete a scheduled report.
- **Suspend**—Click this button to suspend a report. The report will not be generated or emailed until it is resumed.
- **Resume**—Click this button to resume a suspended report. The report will begin being generated and emailed at the interval specified in the scheduled report settings.
- **Run Report Now**—Click this button to immediately generate and send a scheduled report. You do have the option of changing the Creation Method and Recipients for this immediate run, however those changes will not apply to the regularly scheduled report.
- **Edit**—Click on a table row to see and edit details for that table row entry. You can modify any of the report settings as needed.

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.
Add a scheduled report

Use the following instructions to add a scheduled report.

You must have an existing scheduled report template before you can create a scheduled report. See Add a scheduled report template on page 114 for details.

1. Click Reports and select the Scheduled Reports tab.
2. Click Add.
3. Configure the scheduled report.

CREATE REPORT

Report Name

Threat History

Delivery Schedule

Daily \text{ 09:00} \text{ UTC +00:00}

Creation Method

One report created per site

Recipients

Email to the report distribution list of each site

Template

Template for threat detection history

Sites

All selected (4)

Languages

1 of 13 selected

• Report Name—Specify a unique name for the report.
• Delivery Schedule—Select when you want the report to be generated. When selecting a time, specify the time zone according to UTC for the selected time.
• Creation Method—Select how you want the report to be generated.
  • One report created per site—If you have selected multiple sites, you will get multiple reports, one for each site. If you have one selected one site, you will get one report.
One single report created, containing data for all selected sites—You will get one report, regardless of the number of sites you have selected.

**Recipients**—If you have selected one single report, specify a comma-separated list of up to 25 email addresses. Each address will receive the report when it is generated. If you have selected one report per site, select one of the following options.

- **Email to the report distribution list of each site**—Select this option to use the report distribution list associated with each site. (For the business view, this is the report distribution list specified on the **Settings** tab. For the service provider view, go to the **Sites List** tab, click the site name hyperlink, and then go to the **Details** tab.)

- **Email to the email addresses provided below**—Select this option to specify the email addresses that should receive the report. Specify a comma-separated list of up to 25 email addresses. Each address will receive the report when it is generated.

- **Email to both the report distribution list & email addresses provided below**—Select this option if you want to use both of the options above.

**Template**—Select the type of template you want to use for the report. See View available scheduled report templates on page 113 for details.

**Sites**—Select the sites you want to generate the report for. Use the Select all and Select none buttons as needed.

**Languages**—Select the languages you want the default text (chart titles, graph axes, and so on) of the report to be generated in. Use the Select all and Select none buttons as needed. One report per selected language will be created.

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

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.
View available scheduled report templates

When creating a scheduled report, you need to select a template for the report to use. Two default templates are available, and 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 controls are available on the templates table.

- **Add**—Click this button to add a new scheduled report template. See Add a scheduled report template on page 114 for details.
- **Copy**—Click this button to make a copy of an existing scheduled report template. Provide a unique name for the new template and click Copy. You can then select the table row for the new template and make any desired modifications.
- **Delete**—Click this button to delete a scheduled report template.
- **Edit**—Click on a table row to see and edit details for that table row entry. You can modify any of the template details as needed and click Save. See Add a scheduled report template on page 114 for details on the template settings.
**Add a scheduled report template**

Use the following instructions to add a scheduled report template.

1. Click **Reports** and select the **Scheduled Templates** tab.
2. Click **Add**.
3. Configure the scheduled report template.

```
CREATE TEMPLATE

Name
 Template for device activations

Title Page Text
 Device Activation, Last 7 Days

File Format
 PDF

Add Page  Delete Page

<table>
<thead>
<tr>
<th>PAGE</th>
<th>DATA FIELD</th>
<th>CHART TYPE</th>
<th>TIME PERIOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Report Summary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Device Activations</td>
<td>Line</td>
<td>7 days</td>
</tr>
</tbody>
</table>

Cancel  Create
```

- **Name**—Specify a unique name for the template.
- **Title Page Text**—Specify text that will be used for the title of the report generated by this template.
- **File Format**—Select the type of report this template will create: PDF or CSV (comma-separated file).
- **Add Page**—Click this button to add a page to the template.
  - **Data Field**—Select the data to include. See Report types on page 116 for information on the data available.
  - **Chart Type**—If applicable to the Data Field you selected, select the type of chart.
  - **Time Period**—If applicable to the Data Field you selected, select the time frame.
- **Delete Page**—Click this button to delete the selected page from the template.
- **Edit**—Click on a table row to see and edit details for that table row entry.
- **Reorder Pages**—Click the up down arrows next to the page numbers to sort the pages in your desired order.

4. Once the template is configured, click **Create**.
View scheduled report history

To view scheduled reports that were generated within the last 90 days, click **Reports** and select the **Scheduled History** tab. If needed, click **Refresh History** to update the table.

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 and you will see the list of sites included in the report. If the report was successfully created, you can click **Download** to download a copy of the report to your local machine. Keep in mind, if you selected one report per site and selected multiple sites, then you need to specify which site's report to download.
Report types

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

**Device Reports**

These reports are listed by device.

- **Agent Version Spread**—Installed agent versions
- **Device Activations**—Activations within specified time period
- **Device Type**—Windows or MacOS
- **Endpoint Status**—Clean devices and infected devices
- **Expired Status**—Active devices and expired devices
- **Installation Status**—Active devices and uninstalled devices
- **Managed by Policy**—Policy-managed devices and unmanaged devices
- **Operating System Firewall Status**—Enabled, disabled, and unsupported operating system firewalls
- **Operating System Language**—Operating system languages
- **Operating System Platform**—32-bit, 64-bit, or unknown operating system architectures
- **Primary Browser**—Default browsers
- **Remediation Status**—Enabled and disabled remediation status
- **Scheduled Scans Status**—Enabled and disabled scheduled scans
- **Silent Mode**—Enabled, disabled, and unsupported silent scans
- **Virtual Machine**—Virtual machine classified devices

**DNS Protection Reports**

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

- **DNS: Active Hosts**—Complete browsing history and Internet usage
- **DNS: Botnet Command & Control Blocked**—Sites categorized as a botnet using command and control software and have been blocked
- **DNS: Top Blocked Category**—Most often blocked sites by category
- **DNS: Top Blocked Domain**—Most often blocked domains (limited to top 12)
- **DNS: Top Requested Category**—Most often requested sites by category
- **DNS: Top Sites by Number of Requests**—Number of requests by day for the top requested sites

**File Threat Reports**

These reports are listed by file name, device, site, or count.

- **All Threats Seen**—Identified threats by file name
- **All Undetermined Software Seen**—Undetermined threats by file name
- **Attention Required**—Sites that require attention
- **Devices Needing Attention**—Devices that require attention
• **Devices with Threats Seen on Last Scan**—Identified threats by device
• **Devices with Undetermined Software on Last Scan**—Undetermined threats by device
• **Threat Detection History**—Identified threats by count

### Shield Reports

These reports are listed by threat name or device.

• **Evasion Shield - Script Protection Status**—Detect and report, detect and remediate, disabled, and unsupported Evasion Shield protection
• **Evasion Shield - Script Detections**—Detected threats
• **Firewall Status**—Enabled, disabled, and unsupported Endpoint Protection firewalls
• **Identity Shield Status**—Enabled and disabled Identity Shield protection
• **Infrared Status**—Enabled, disabled, and unsupported infrared setting
• **Offline Shield Status**—Enabled, disabled, and unsupported Offline Shield protection
• **Phishing Shield Status**—Enabled and disabled Phishing Shield protection
• **Realtime Shield Status**—Enabled and disabled Realtime Shield protection
• **Rootkit Shield Status**—Enabled, disabled, and unsupported Rootkit Shield protection
• **USB Shield Status**—Enabled, disabled, and unsupported USB Shield protection
• **Web Threat Shield Blocked URL History**—Blocked URLs by date
• **Web Threat Shield Blocked URLs**—Blocked URLs
• **Web Threat Shield Status**—Enabled and disabled Web Threat Shield protection

### Security Awareness Training Reports

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

• **SAT: Phishing Clicks**—Click rates by site
• **SAT: Training Progress**—Training rates by site
• **SAT: Usage Report**—Usage statistics
Chapter 12 Alerts and alert distribution lists

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

The following tasks are available for alerts and alert distribution lists.

- View and manage alerts and alert distribution lists on page 119
- Add an alert on page 120
- Add an alert distribution list on page 124
View and manage 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.

The following controls are available.

- **Add**—Click this button to add an alert or an alert distribution list, depending on the tab you are on. See *Add an alert* on page 120 and *Add an alert distribution list* on page 124 for details.
- **Delete**—Click this button to delete the selected alert or the alert distribution list.
- **Suspend**—Click this button to suspend the selected alert. No emails will be sent to the alert distribution list when the alert criteria is met.
- **Resume**—Click this button to resume the selected alert. Emails will be sent to the alert distribution list when the alert criteria is met.
- **Edit**—Click on a table row to see and edit details for that table row entry. See *Add an alert* on page 120 for details on the alert settings.
Add an alert

Use the following instructions to add an alert.

1. Click Alerts and on the Alert List tab, click Add.
2. In the first step of the Create Alert wizard, configure the basic settings of the alert.

   ![Create Alert Wizard](image)

   - **Name**—Specify a unique name for the alert.
   - **Alert type**—Select the type of alert you want to create.

3. Click Next to continue.
4. In the second step of the Create Alert wizard, identify who will receive the alert.
- **Use Existing List**—Select this option to use an existing alert distribution list and **Select a distribution list** from the drop-down.

- **Create New List**—Select this option to create a new alert distribution list.
  - **Distribution List Name**—Specify a unique name for the new alert distribution list.
  - **Email Addresses**—Specify a comma-separated list of up to 25 email addresses. Each address will receive the alert notification email when it is generated.

5. Click **Next** to continue.

6. In the third step of the **Create Alert** wizard, select the sites that should use this alert.
- **All sites**—Select this option to configure all sites for this alert.
- **Selected sites**—Select this option to configure specific sites for this alert. Select the specific sites you want to use this alert. Use the **Select all** and **Select none** buttons as needed.

7. Click **Next** to continue.

8. In the fourth step of the **Create Alert** wizard, configure the email that will be sent when the alert is generated.
Email Title—Specify the title of the email message that will be sent.

Email Message Body—Specify the body of the email message that will be sent.

Data Inputs—These are variables that will be populated with specific data when an alert is generated. When you cursor is in either the title or body fields, the data input buttons will be enabled (blue). Click on 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 pop-up list to identify which threats you want to include.

The Workgroup and Active Directory data inputs are not applicable to MacOS.

9. Click Finish to create the alert.
Add an alert distribution list

Use the following instructions to add an alert distribution list.

1. Click Alerts and on the Distribution Lists tab, click Add.
2. Configure the alert distribution list.

   - **Name**—Specify a unique name for the new alert distribution list.
   - **Email Addresses**—Specify a comma-separated list of up to 25 email addresses. Each address will receive the alert notification email when it is generated.

3. Click Create to create the alert distribution list.
Chapter 13 Administrators

Each user account is called an Admin and is assigned two types of permissions.

Sites are only applicable if you are using the service provider view. Sites are not applicable to the business view.

- **Account type**—These permissions determine access to the Management Console. You can have full access (super) or limited access.

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

- **Site permissions**—These permissions determine access to a site.
  - **Admin**—This permission has full access to the site.
  - **View Only**—This permission has view-only access to the site.
  - **No Access**—This permission denies access to the site. You will not see the site listed on the Sites List page.

The following tasks are available for administrators.

- **View available administrators** on page 126
- **Add an administrator** on page 127
- **Edit an administrator** on page 129
- **Delete an administrator** on page 130
View available administrators

To view your available administrators, click **Admins**. The page is divided into two tabs. Super administrators and limited administrators (decides access to the Management Console) are listed on the **Admins** tab. Site-only administrators (access to sites) are listed on the **Site Only Admins** tab. To review the permission types, see *Administrators* on page 125.

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

- **Add Admin**—Click this button to add a new administrator. See *Add an administrator* on page 127 for details.
- **Sort**—Click a column heading to sort the table by that column.
- **Admin name hyperlink**—Click the name of an administrator to view or edit the account information. See *Edit an administrator* on page 129 for details.
- **Actions, Resend Confirmation Email**—Use this menu item to send another confirmation email to the email address for the account.
- **Actions, Edit**—Use this menu item to view or edit the account information. See *Edit an administrator* on page 129 for details.
- **Actions, Delete**—Use this menu item to delete an administrator. See *Delete an administrator* on page 130 for details.
Add an administrator

Use the following instructions to add an administrator.

1. Click **Admins** and then click **Add Admin**.
2. In the first step of the **Add Admin** wizard, configure your administrator details.

![ADD ADMIN wizard](image)

- **First Name**—Specify the user’s first name.
- **Last Name**—Specify the user’s last name.
- **Email**—Specify the user’s email address. This is what the user will use to log in.
- **Phone**—Optionally specify the user's phone number.
- **Time Zone**—Specify the user’s time zone.
- **Account Type**—Select 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>Sites Lists</td>
<td>Based on site permissions</td>
<td>Based on site permissions</td>
</tr>
<tr>
<td>Dashboard</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Manage, Entities</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Manage, Policies</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
3. Click **Next** to continue.

4. In the second step of the **Add Admin** wizard, select the sites this administrator should have access to.

   - **Admin**—This permission has full access to the site.
   - **View Only**—This permission has view-only access to the site.
   - **No Access**—This permission denies access to the site. You will not see the site listed on the **Sites List** page.

5. Click **Save** to add the administrator.
Edit an administrator

Use the following instructions to edit an administrator.

1. Click **Admins**.
2. Click the name hyperlink or use the **Actions** menu at the right side of a table row and select **Edit**.

3. Modify the settings on the **Details** or **Site Permissions** tabs as needed. See *Add an administrator* on page 127 for details on each setting.
4. When you have finished editing the administrator, click **Save**.
Delete an administrator

There must be at least one administrator per console. Therefore, you cannot delete the last administrator. A deleted administrator can be added again. To delete an administrator, use the following instructions.

1. Click **Admins**.
2. Click the name hyperlink or use the **Actions** menu at the right side of a table row and select **Delete**.
3. Confirm you want to delete the user by clicking **Delete Admin**.
Chapter 14  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**

- **Endpoint**—This tab includes general site or company information.
  - **Site / Company Name**—Specify a unique name for the site or company.
  - **Keycode**—This field is read-only and displays the keycode assigned to the site or company. If the keycode is a trial, the number of days remaining in the trial period will also be displayed. This is the keycode that will be used in Endpoint Protection installations. You will also see this keycode on the Downloads tab.
  - **Company Size**—Select the range that represents the size of the company.
  - **Company Industry**—Select the industry that represents the company.
  - **Comments**—Optionally enter any comments describing the site or company.
  - **Site Seats**—Specify the number of seats (endpoints or devices) for the site or company you are configuring. This setting is for your internal reference. It is not used for billing.
  - **Default Endpoint Policy**—Select a default policy. The selected policy will be used for all new devices that are installed for this site or company, unless the policy is assigned using inheritance from the group, site, or company for the device. (You can modify the policy the device uses after installation.)
    - **Recommended Defaults**—This policy is intended for desktops and laptops. User interface and PUAs (possibly unwanted applications) are disabled. The setting to install DNS Protection is disabled in this policy.
    - **Recommended DNS Enabled**—This policy is identical to Recommended Defaults, except the setting to install DNS Protection is enabled.
    - **Recommended Server Defaults**—This policy is intended for server environments. It focuses on resource utilization and minimal impact on the server.
    - **Silent Audit**—This policy is based on the Recommended Defaults policy, however, it has the remediation function disabled to minimize production impact. This means it will catch known threats, but not undetermined threats. Use the undetermined threats reports to help you identify items to add to your block and allow overrides. Generally, this policy should only be used for a short duration, for example during initial setup to identify potential production false positives.
    - **Unmanaged**—This policy is intended for technical support, troubleshooting, and when no policy management is needed. This policy cannot be managed, but it turns the agent into a local, unmanaged application that can be controlled directly by the end-user. You should not use this policy in production.
    - **Report Distribution List**—Specify a comma-separated list of up to ten email addresses. Each address will receive the generated reports that are configured to be sent to the report distribution list.
• **Subscriptions**—This 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.

• **Account Information**—This tab provides information on the primary account holder.
  - **Site / Company Name**—This is the company name that is used to define the console. If you need to rename the site or company, click **Rename**. This will also rename the console.
  - **Company Address**—The company address is specified for you when your account is created. If you need to modify the address, contact Webroot.
  - **Contact Email**—This is the email of the primary account for the selected console. If you need to modify the email, contact Webroot.
  - **Contact Phone**—The phone number is specified for you when your account is created. If you need to modify the phone number, contact Webroot.
  - **Parent Keycode**—This 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. When needed, click **Renew/Upgrade** to update your subscription.
  - **View Usage**—Click **My Usage** to see reports about your security usage. Log in when prompted, select **My Usage**, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.

  The report is a rolling 30 day total from the date selected on the usage page. You can export the usage data by clicking the **Download CSV** link. You can also drill down to see site usage by clicking the **Site Usage** button, and you can export the usage data for that site.

  • **Pay Invoices**—Click **My Billing** to access your billing information. Log in when prompted, select **My Billing**, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.

  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 verifying 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 **wr-AccountsReceivable@opentext.com** or your sales representative.

  • **Downloads**—This 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 **Agents** on page 140 for details on other deployment options.

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

  • **Logo**—If you want your own logo to appear on the notification page, drag and drop a logo to the dotted box or click the dotted box and select the logo. The logo file must be .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 will change 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 will change back to the standard Webroot logo.

- **Website not allowed**—The text and graphics below the logo and above the formatting toolbar will automatically appear on the notification page. The text and graphics cannot be modified or deleted.
- **Additional information**—Below the formatting toolbar is a free form field with additional information. You can modify or delete this text to suit your needs. You can enter a maximum of 500 characters in this field.
- **Reset to Default Settings**—Click this button to reset the logo and additional information back to the default settings.

- **API Access**—You can access the Unity API, which is a REST API if you want to automate access to Webroot services and information, such as billing, reporting, and so on. When you create credentials, you will provide a **Client ID** and **Client Secret** which you will need to use to authenticate with the API to access information or take action. You can review the client secret as needed. See the links in this section for details on using the Unite API.

- **Advanced Settings**—This tab contains two advanced settings.
  - **Data Filter**—If you want to limit the data is that is displayed in the console, you can apply data filters. These filters will show or hide data depending on your filter. For example, if you select **2 Months**, all devices that have not connected for two months will be excluded from the data shown for this site. This option 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.

  From the **Advanced Settings** tab, click **Edit** to set or remove a filter. The edit page also allows you to see the history of data filter changes.

  - **Convert to Managed Service Provider Console**—Click **Convert** if you want to change to the service provider view. This allows you to have multiple sites (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**

- **Subscriptions**—This 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.

- **Account Information**—This tab provides information on the primary account holder for the selected console. (Consoles are limited to 1000 sites, so you may have multiple consoles if you have more sites than that.)
  - **Site / Company Name**—This is the company name that is used to define the console. If you need to rename the site or company, click **Rename**. This will also rename the console.
• **Company Address**—The company address is specified for you when your account is created. If you need to modify the address, contact Webroot.

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

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

• **Parent Keycode**—This is the keycode assigned to the selected console. Do not use this keycode for installations. You should use the keycode assigned to a site for installations. When needed, click Renew/Upgrade to update your subscription.

• **View Usage**—Click My Usage to see reports about your security usage. Log in when prompted, select My Usage, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.

  The report is a rolling 30 day total from the date selected on the usage page. You can export the usage data by clicking the Download CSV link. You can also drill down to see site usage by click the Site Usage button, and you can export the usage data for that site.

• **Pay Invoices**—Click My Billing to access your billing information. Log in when prompted, select My Billing, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.

  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 verifying 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 wr-AccountsReceivable@opentext.com or your sales representative.

• **Data Filter**—If you want to limit the data that is that is displayed in the console, you can apply data filters. These filters will show or hide data depending on your filter. For example, if you select 2 Months, all devices that have not connected for two months will be excluded from the data shown for this site. This option 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.

  From the Settings tab, you can set a filter that applies to all sites. You can override this setting from within an individual site. See Manage a site on page 42 for details. From this tab, you can also see the history of data filter changes.

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

  • **Logo**—If you want your own logo to appear on the notification page, drag and drop a logo to the dotted box or click the dotted box and select the logo. The logo file must be .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 will change 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 will change back to the standard Webroot logo.

- **Website not allowed**—The text and graphics below the logo and above the formatting toolbar will automatically appear on the notification page. The text and graphics cannot be modified or deleted.
- **Additional information**—Below the formatting toolbar is a free form field with additional information. You can modify or delete this text to suit your needs. You can enter a maximum of 500 characters in this field.
- **Reset to Default Settings**—Click this button to reset the logo and additional information back to the default settings.

- **API Access**—You can access the Unity API, which is a REST API if you want to automate access to Webroot services and information, such as billing, reporting, and so on. When you create credentials, you will provided a **Client ID** and **Client Secret** which you will need to use to authenticate with the API to access information or take action. You can review the client secret as needed. See the links in this section for details on using the Unite API.
Chapter 15 DNS Protection

If you followed the process to Get started on page 10 for DNS Protection, you should have DNS Protection enabled and installed on at least one device using an Endpoint Protection policy. However, you are not limited to the DNS Protection agent, nor are you limited to running the agent on devices with Endpoint Protection. See the DNS Protection tasks below for more information.

- **Assign the default DNS Protection policy** on page 137—You can select the default DNS Protection policy. The selected policy will be used for all new devices that are installed for this site or company, unless the policy is assigned using inheritance from the group, site, or company for the device. (You can modify the policy the device uses after installation.) The policy defines which types of web sites are blocked and allowed.

- **Configure the network** on page 138—DNS Protection protects your servers by registering the IP address or domain associated with the network, so that all devices on the network, even those not running the DNS Protection agent, will have Active Directory DNS requests handled by Webroot DNS Protection. This also allows you to control content on WiFi and guest networks as well as limit content available over different circuit types. The networks you specify will forward DNS requests to specified Webroot DNS Protection servers for resolution.

- **Install DNS Protection using an Endpoint Protection policy** on page 23—If your DNS Protection devices are already running Endpoint Protection, you do not need to install the agent separately. The agent installation is controlled by the **Install DNS Protection policy** setting in your Endpoint Protection policies.

- **Agents** on page 140—If your DNS Protection devices are not running Endpoint Protection, you can deploy the agent separately. There are multiple deployment options available.
Assign the default DNS Protection policy

You can select the default DNS Protection policy. The selected policy will be used for all new devices that are installed for this site or company, unless the policy is assigned using inheritance from the group, site, or company for the device. (You can modify the policy the device uses after installation.) The policy defines which types of web sites are blocked and allowed. See Policies on page 54 for details on adding, editing, and other policy tasks.

1. If you are using the business view, go to the DNS Protection tab. If you are using the service provider view, go to the Sites List tab, and then for the site that you want to assign the default DNS Protection policy, click the gear icon in the Actions menu for DNS Protection to automatically go to the DNS Protection tab for the selected site.

2. Select a Default DNS Site Policy. There are two default policies, or you may have created your own. See Policies on page 54 for details on adding, editing, and other policy tasks.

3. If you also want to configure the network settings, see Configure the network on page 138 for details.

4. Click Save.
Configure the network

DNS Protection protects your servers by registering the IP address or domain associated with the network, so that all devices on the network, even those not running the DNS Protection agent, will have Active Directory DNS requests handled by Webroot DNS Protection. This also allows you to control content on WiFi and guest networks as well as limit content available over different circuit types. The networks you specify will forward DNS requests to specified Webroot DNS Protection servers for resolution.

Use the following instructions to configure your network for DNS Protection.

1. If you are using the business view, go to the DNS Protection tab. If you are using the service provider view, go to the Sites List tab, and then for the site that you want to configure the network, click the gear icon in the Actions menu for DNS Protection to automatically go to the DNS Protection tab for the selected site.

2. In the Agent Settings section, select the default policy. See Assign the default DNS Protection policy on page 137 for details.

3. In the Domain Bypass List section, you can enter a domain, if desired, so that it is never blocked by the Webroot DNS Protection servers. Enter a Domain and click Add Domain. Keep in mind the following.
   - 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 menu at the right side of the table row.

4. In the Network Settings section, enter the Domain/IP Address for a network that you want to register to use the Webroot DNS Protection servers, select a Policy to use for this network, and click Add Network. All devices using this network will have Active Directory DNS requests handled by the Webroot DNS Protection servers. Keep in mind the following.
   - You should be using a WAN IP address. If you are uncertain what your WAN IP address is, you can search "my IP" on the Internet to see it.
   - There are two default policies, or you may have created your own. See Policies on page 54 for details on adding, editing, and other policy tasks.
   - Add more networks by adding additional rows. For example, you can add guest network and WiFi networks separately.
   - You can add up to 500 entries.
   - If you need to edit or delete a row, use the Actions menu at the right side of the table row.

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

6. If you need to filter DNS requests on servers, select Enable Agent Install on Servers. You will have visibility by server name of all Internet requests that have been made from your servers. However, do not use this option on a DNS server or you will have resolution issues.

7. Click Save.
8. Use the following steps to test the network configuration.
   a. From a device on the network, open a command prompt.
   b. Query the domain by entering the following command.
      \n      NSLookup
   c. Set the lookup server by entering the following command.
      server 45.54.55.54
   d. Check several sites to confirm valid responses. Keep in mind that 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 45.54.55.54
Default Server: 54.55.54.45.wsadns.webroot.com
Address: 45.54.55.54

Server: 54.55.54.45.wsadns.webroot.com
Address: 45.54.55.54

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

>
```

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

---

If you are only using network protection and are not using the DNS Protection agent (which installs certificates when it is installed on a device), Windows users will receive browser certificate errors when secure (https) web sites are blocked. To avoid certificate errors, download certificates from [http://45.54.55.55/download](http://45.54.55.55/download) and install them to Trusted Root Certification Authorities on each device. See Microsoft documentation for details on installing certificates manually or pushing them out automatically.

In the event you discontinue protecting your network using DNS Protection or your trial period expires, you will need to revert your routers or DNS forwarders to their original settings because the Webroot DNS Protection servers will only respond to accounts that have active trials or that have purchased.
Chapter 16 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.

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

- **DNS Protection**—If you will be using DNS Protection on devices to filter DNS requests when the devices are off the network, you will use the same agent that is used with Endpoint Protection.

The agent installation files are .exe for Windows and .dmg for Apple.

You have many choices when deploying 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 the method you choose, 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.

- *Install on Windows or MacOS using the installation wizard* on page 142
- *Install on Windows or MacOS from the command line* on page 143
- *Install on Windows using Msiexec* on page 145
- *Install on Windows using group policy* on page 146

If your DNS Protection devices are already running Endpoint Protection, you do not need to install the agent separately. The agent installation is controlled by the **Install DNS Protection policy** setting in your Endpoint Protection policies. See *Endpoint Protection policy settings* on page 63 for details.

Regardless of how the DNS Protection installation was completed (using Endpoint Protection policy or deployment), the installation includes a service that inspects and saves (at startup and when the connection status of a network adapter changes) the settings for the active network adapters. 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.

Keep in mind the following caveats for the DNS Protection agent installation.
• If you are using a trial of DNS Protection and it expires, 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 Endpoint Protection policy configuration is changed to no longer install DNS Protection, 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 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.
Install on Windows or MacOS using the installation wizard

Use the following instructions to install on Windows or MacOS using the installation wizard.

1. Locate the installation file download links in the Management Console.
   - **Business view**—If you are using the business view, go to the **Settings** tab and then the **Downloads** tab to find the installation file download links.
   - **Service provider view**—If you are using the service provider view, use the following steps to locate the installation file download links.
     a. In the Management Console, click **Sites List**.
     b. Locate your site in the list and click the site name hyperlink.
     c. Click the **Endpoint Protection** tab.

2. Select the Windows or Apple download link as appropriate to download the file.

3. Copy the **Keycode** for your company or for the site.

4. Copy, post, email, or use another method to get the installation file to the device you want to install on.

5. Install the agent.
   - For Windows, run the .exe file.
   - For Apple, run the .dmg file and then open the **Applications** folder and double-click the Webroot icon to launch the installer.
     Follow the on-screen prompts to complete the installation.

Once the installation is complete and the agents check in with the Management Console, you will see the **Devices** column populate. The agent should complete the first scan for threats in seconds or minutes and report back to the Management Console. If DNS Protection is enabled, filtering will begin immediately.
Install on Windows or MacOS from the command line

Use the following instructions to install on Windows or MacOS from the command line.

1. Locate the installation file download links in the Management Console.
   - **Business view**—If you are using the business view, go to the Settings tab and then the Downloads tab to find the installation file download links.
   - **Service provider view**—If you are using the service provider view, use the following steps to locate the installation file download links.
     a. In the Management Console, click Sites List.
     b. Locate your site in the list and click the site name hyperlink.
     c. Click the Endpoint Protection tab.

2. Select the Windows or Apple download link as appropriate to download the file.

3. Install the agent using any of the command options that correspond to your operating system. Some options are only relevant to Windows installations.
   - `/key=keycode`—Install the agent software using the specified keycode, with or without hyphens.
   - `/silent`—Install the agent in the background with no on-screen interaction.
   - `/nostart`—On a Windows device, install the agent, but do not start it.
   - `/lockautouninstall=password`—On a Windows device, install the agent without adding it to the Windows Control Panel programs list. This allows you to silently uninstall later using the specified password.
   - `/autouninstall=password`—On a Windows device, uninstall the agent using the password specified with /lockautouninstall.
   - `-clone`—On a Windows device that does not have a unique host name due to cloning, assign a unique ID to the machine when the agent is installed. The unique ID will be included in the host name to better identify this machine.
   - `-uniquedevice`—On a Windows device that does not have a unique machine ID (but does have a unique host name), assign a unique ID to the machine where the agent is installed. The host name will be used to identify this machine.
   - `/exeshowaddremove`—On a Windows device, include 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`—On a Windows device, assign 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`—Use the specified proxy server during the agent installation.

   Endpoint Protection will automatically detect 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`—Use the specified port number for the proxy server.
   - `/proxyuser=name`—Use the specified user name for the proxy server.
• `/proxypass=password`—Use the specified password for the proxy server.
• `/proxyauth=authtype`—Use one of the following authentication types 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.

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

• `/lang=languagecode`—Install the agent using one of the following language codes.
  • de—German
  • en—English
  • es—Spanish
  • fr—French
  • it—Italian
  • ja—Japanese
  • ko—Korean
  • nl—Dutch
  • pt—Brazilian Portuguese
  • ru—Russian
  • tr—Turkish
  • zh-cn—Simplified Chinese
  • zh-tw—Traditional Chinese

Once the installation is complete and the agents check in with the Management Console, you will see the **Devices** column populate. The agent should complete the first scan for threats in seconds or minutes and report back to the Management Console. If DNS Protection is enabled, filtering will begin immediately.
Install 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. In most cases, you will use this method of installation when you are pushing the software using a remote deployment tool.

1. Locate the installation file download links in the Management Console.
   - **Business view**—If you are using the business view, go to the **Settings** tab and then the **Downloads** tab to find the installation file download links.
   - **Service provider view**—If you are using the service provider view, use the following steps to locate the installation file download links.
     a. In the Management Console, click **Sites List**.
     b. Locate your site in the list and click the site name hyperlink.
     c. Click 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.

Once the installation is complete and the agents check in with the Management Console, you will see the **Devices** column populate. The agent should complete the first scan for threats in seconds or minutes and report back to the Management Console. If DNS Protection is enabled, filtering will begin immediately.
Install 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.

1. Locate the installation file download links in the Management Console.
   - **Business view**—If you are using the business view, go to the Settings tab and then the Downloads tab to find the installation file download links.
   - **Service provider view**—If you are using the service provider view, use the following steps to locate the installation file download links.
     a. In the Management Console, click Sites List.
     b. Locate your site in the list and click the site name hyperlink.
     c. Click 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, and Endpoint Protection will be installed on the devices in the group when they restart.

Once the installation is complete and the agents check in with the Management Console, you will see the **Devices** column populate. The agent should complete the first scan for threats in seconds or minutes and report back to the Management Console. If DNS Protection is enabled, filtering will begin immediately.